Horizon 制御プレーン next-gen の使用 - Horizon Cloud Service およびクラウド接続された Horizon 8

2024 年 4 月以降のサービスに対して更新

VMware Horizon Cloud Service - next-gen

VMware by Broadcom の Web サイトで最新の技術ドキュメントを確認できます

https://docs.vmware.com/jp/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

目次

Horizon 制御プレーン next-gen の使用 - Horizon Cloud Service およびクラウド接続された Horizon 8

1

Horizon 制御プレーンはクラウドホスト型の制御プレーンで、クラウド接続された Horizon 環境で使用される SaaS サービスを提供します。

Horizon 制御プレーンには、主に次の 2 つのユースケースがあります。

- Horizon Cloud Service (DaaS) をデプロイするためのプラットフォーム。現在、Horizon Cloud Service on Azure のみが使用可能です。
- Horizon 8 ポッドに接続して、オプションの共通 SaaS サービスを提供する制御プレーン。オンプレミスおよびパブリック クラウド SDDC にデプロイされた Horizon 8 ポッドは、Horizon 制御プレーンに接続し、追加の SaaS サービスを使用できます。

この出版物は、仮想デスクトップとアプリケーションを組織内のエンド ユーザーに大規模に提供し、Horizon 制御プレーンと Horizon Universal Console を使用してそれらの仮想デスクトップとアプリケーションを効率的に管理する管理者を対象としています。

Horizon 制御プレーンのメリット - ネイティブ Microsoft Azure デプロイ

このセクションでは、ネイティブ Microsoft Azure でのデプロイに対する次世代の Horizon 制御プレーンのメリットを示します。

これらは、追加の SaaS サービスを使用して Horizon 制御プレーンに接続する Horizon 8 ポッドの他のユースケースには適用されません。

注： その他の利用可能な機能については、『Horizon Cloud Service - next-gen リリース ノート』の「新機能」セクションを参照してください。

低コスト

シン Edge インフラストラクチャとポッドレス デプロイを備えた Horizon Edge により、運用コストの削減、価値の提供までの時間の短縮、および Horizon インフラストラクチャ コンポーネントの排除によるメンテナンスの削減が実現します。

可視性とトラブルシューティングの向上

すべてのプラットフォームで同じモデルを使用することで、Workspace ONE Intelligence との統合によるプロアクティブなアラート機能と高度なレポート機能を使用し、可視性とトラブルシューティング機能を向上させています。

環境間にわたるシームレスな操作性と機能性

環境間での管理者およびエンドユーザーの操作性と機能性を共通化することで、管理を効率化し、エンドユーザーの生産性を向上させることができます。

高度な自動化

API ベースのプラットフォームでは、高度な自動化と、Day 1 および Day 2 プロセスのためのサードパーティのアプリケーションとサービスとの統合をサポートします。

これまでにないスケーラビリティ

シン Edge アーキテクチャとクラウド ネイティブ アーキテクチャを備えた Horizon Edge は、あらゆるプラットフォームでスケーラビリティを高めます。

関連するソリューションの Horizon 8 ファミリのドキュメントを確認する場合は、Horizon ドキュメント - Horizon 8、Horizon Cloud Service、および Horizon Clients を参照してください。

次のトピックを参照してください。

- Horizon 制御プレーン のアーキテクチャ特性 - ネイティブ Microsoft Azure デプロイ

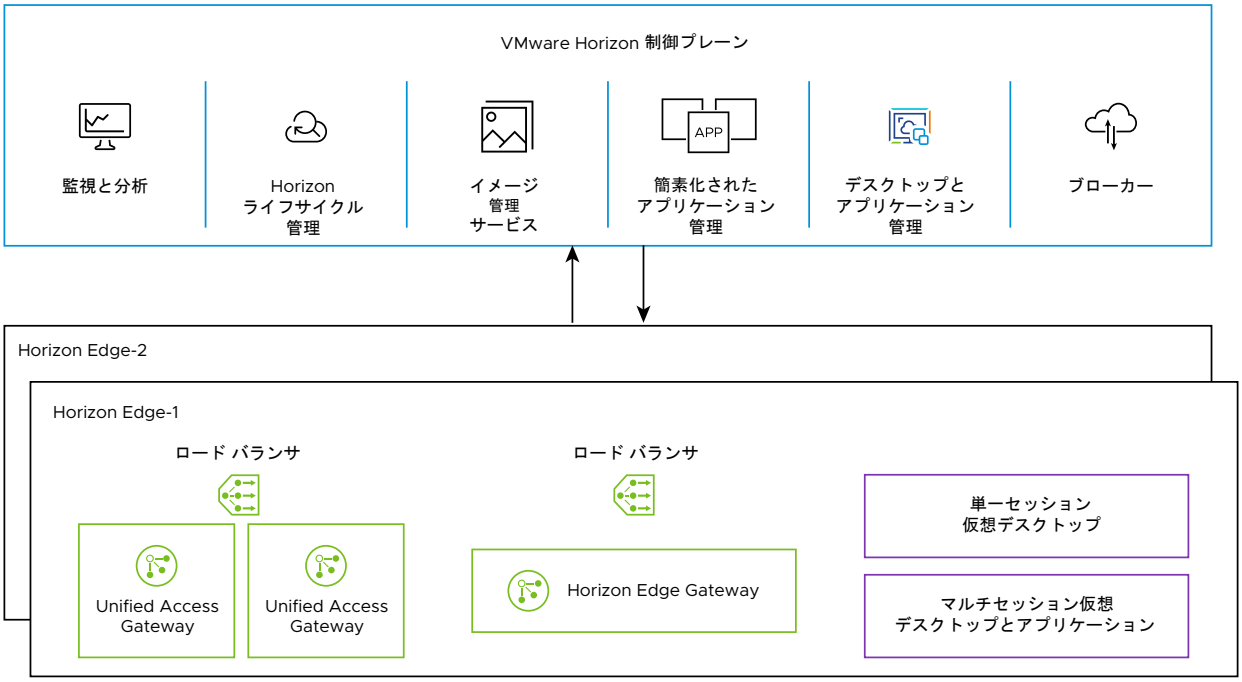
Horizon 制御プレーン のアーキテクチャ特性 - ネイティブ Microsoft Azure デプロイ

いくつかのアーキテクチャ特性は、Horizon Cloud Service - next-gen サービスがどのように動作するか、またこのサービスが前世代の Horizon Cloud Service - first-gen サービスをどのように改善するかを定義します。

このセクションでは、現在ネイティブ Microsoft Azure で使用可能な Horizon Cloud Service - next-gen に固有の特性について説明します。Horizon 8 ポッドが Horizon 制御プレーン に接続し、追加の SaaS サービスを使用する場合のユースケースには対応していません。

このアーキテクチャは、構成、運用、および管理が容易なクラウドベースのデプロイを提供します。

次の図は、Horizon 制御プレーン と、Microsoft Azure Cloud (`Horizon Edge-1`) にデプロイされた最初の Horizon Edge の関係を示しています。この例では、デプロイ ウィザードでの作業中に、管理者は 2 つの Horizon Edge Gateway インスタンスを使用することを選択しました。



次のコア インフラストラクチャ要素は、これらのサービスを提供します。

- Horizon 制御プレーンを参照してください。
- Horizon Edge Gateway インスタンス。プロバイダとしての Microsoft Azure Cloud の場合、デプロイヤはこのインスタンスを使用して Microsoft Azure ロード バランサをデプロイします。
- Unified Access Gateway のインスタンス、およびそれらのインスタンスのロード バランサ。

アーキテクチャの詳細については、「Horizon Cloud Service next-gen アーキテクチャ」を参照してください。

第 1 世代との違い

Horizon Cloud Service - next-gen は、その大幅な改善と動作により、以前の Horizon Cloud Service - first-gen と区別されます。Horizon Cloud Service - next-gen の主なメリットは、以前は組織の環境にデプロイされていたインフラストラクチャ コンポーネントの多くが、現在は Horizon 制御プレーン のサービスとして配置されていることです。

Horizon Cloud Service - first-gen から Horizon Cloud Service - next-gen に移行した場合のユーザー エクスペリエンスの違いは、「第 1 世代 Horizon Cloud on Microsoft Azure デプロイから Horizon Cloud Service - next-gen へのセルフサービスの移行」で概説されています。Horizon Cloud Service - next-gen への現在の追加については、『Horizon Cloud Service - next-gen リリース ノート』の「新機能」セクションを参照してください。

Horizon 制御プレーンの使用開始 - Microsoft Azure および Horizon 8 のデプロイ

2

Horizon Cloud Service - next-gen または Horizon 制御プレーンを使用するための最初の手順として、サービスにオンボーディングします。

オンボーディング プロセスを開始するときに、次のシステム要件とサブスクリプションの前提条件を参照してください。

1 環境に対応するチェックリストを確認し、要件を満たします。

- Microsoft Azure Edge をデプロイするための要件チェックリスト
- Horizon 8 Edge をデプロイするための要件チェックリスト

2 デプロイ タイプに対応する環境の準備手順を完了します。

- Microsoft Azure Edge のデプロイ
- Horizon 8 Edge デプロイ

3 「4 章 Horizon Cloud Service - next-gen 管理者のオンボーディング」で説明されているデプロイとオンボーディングの手順を開始します。

次のトピックを参照してください。

- Horizon 8 Edge をデプロイするための要件チェックリスト
- Microsoft Azure Edge をデプロイするための要件チェックリスト

Horizon 8 Edge をデプロイするための要件チェックリスト

次のタスクを完了して、Horizon 制御プレーン にオンボーディングするために Horizon 8 のコンポーネントを準備します。オンボーディングを正常に完了するために、以下のセクションの説明に従って、要件を満たしていることを確認します。

チェックリスト対象者

以降のセクションにリストされている要件の一部は、Horizon Edge 環境でサブスクリプション ライセンスを使用する目的で Horizon コンポーネントを正常にオンボーディングするために必要です。一部の要件は、Horizon コンポーネントでの Horizon 制御プレーン サービスの使用を有効にするために最初のオンボーディング後に実行する主要なタスクに必要なものです。

Horizon Edge Gateway および Horizon Connection Server の要件

☐	Horizon Edge Gateway と Horizon 間の相互運用性を実現するには、Horizon Connection Server が 7.13.2 以降である必要があります。次に、クラウド接続された Horizon Edge で最新のクラウド サービスと機能を使用するには、Horizon Connection Server が現在のバージョンの Horizon Edge サービスを実行する必要があります。
☐	新しいデプロイの場合は、最新の Horizon Edge Gateway バージョンを使用することを強くお勧めします。 Horizon Edge Gateway アプライアンスのデプロイ手順では、次を使用します。 ■ 固定 IP アドレス ■ DNS 正引きおよび逆引き参照レコード
☐	Horizon Edge Gateway 仮想アプライアンスのリソース要件。リソース要件は、デプロイされた Horizon Edge アーキテクチャによって異なります。以下のリストは、各設計の新しいデプロイで現在サポートされているバージョンを反映しています。 **バージョン 2.2.0** vCPU x 8、16 GB メモリ (RAM)、40 GB データストア

DNS、ポートおよびプロトコルの要件

☐	特定のポートとプロトコルは、Horizon ポッドを Horizon Cloud にオンボーディングするため、およびポッド、そのポッドとペアリングされた Horizon Edge Gateway、Horizon 制御プレーン を使用する Horizon Edge Gateway での継続的な運用のために必要です。Horizon 8 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にするを参照してください。

Microsoft Windows オペレーティング システムのライセンス

Horizon Cloud は、Horizon Cloud ワークフローを使用する過程で使用する Microsoft Windows オペレーティング システムの使用に必要なゲスト OS ライセンスを提供しません。ユーザーは、Horizon Cloud テナント環境で使用するために選択した Windows ベースのデスクトップ仮想マシンおよび RDSH 仮想マシンの作成、ワークフローの実行、および操作を行う資格が付与される有効で適格な Microsoft ライセンスを所有している責任があります。必要なライセンスは、使用目的によって異なります。

☐	次のいずれかのタイプのライセンス：Microsoft Windows 7、Microsoft Windows 10
☐	次のいずれかのタイプのライセンス：Microsoft Windows Server 2012 R2、Microsoft Windows 2016、Microsoft Server 2019
☐	Microsoft Windows RDS ライセンス サーバ — 高可用性のために冗長ライセンス サーバを推奨
☐	Microsoft RDS ユーザーまたはデバイス CAL（またはその両方）

Horizon 8 Edge をデプロイするためのポートとプロトコルの要件

このページは、一般的な Horizon Edge と Horizon Connection Server との通信に使用されるすべてのポートとプロトコルのリファレンスです。以下の表を使用して、ネットワーク構成とファイアウォールで正常なデプロイと日常操作に必要な通信トラフィックが可能になるようにします。

特定のデプロイに必要な特定のポートとプロトコルは、Horizon Edge 環境で使用する機能によって多少異なります。Splunk Enterprise を監視に使用する予定がない場合は、Splunk Enterprise に関連付けられているポートを無視できます。

重要： ここで説明するポートとプロトコルに加えて、Horizon Edge 環境と対応する日常の操作には、特定の DNS 要件があります。詳細については、Horizon 8 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にするを参照してください。

Horizon Edge で必要なポートおよびプロトコル

Horizon インフラストラクチャの監視 を有効にすると、Horizon Edge がデプロイされ、関連付けられたサブスクリプションで構成されます。以下の表には、有効化プロセスの実行中に必要となるポートとプロトコルが記載されています。このプロセスでは、アプライアンスをデプロイし、アプライアンスがそれらのコンポーネントから設計に従って収集する監視データを収集できるようにマネージャ仮想マシンを構成します。またこの表には、設計に従って収集すべきデータを収集する定常状態の運用中に必要なポートとプロトコルも記載されています。

表 2-1.

ソース	ターゲット	ポート	プロトコル	目的
Horizon Edge	Horizon Connection Server	443	HTTPS	ライセンスの構成
Horizon Edge	Splunk Enterprise	8000 および 8088	HTTP HTTPS	監視データの収集
Horizon Edge	DNS サーバ	53 および 853	TCP UDP	DNS サービス
Horizon Edge	*.blob.core.windows.net	443	TCP	Azure Blob Storage へのプログラム アクセス、および必要に応じて Horizon Edge ログをアップロードするために使用されます。 Docker イメージをダウンロードして、監視、SSO、UAG の更新などに役立つ必要な Horizon Edge モジュールを作成するために使用されます。
Horizon Edge	horizonedgeprod.azurecr.io	443	TCP	Docker イメージをダウンロードして、監視、SSO、UAG の更新などに役立つ必要な Horizon Edge モジュールを作成する際の認証に使用されます。

表 2-1. （続き）

ソース	ターゲット	ポート	プロトコル	目的
Horizon Edge	*.azure-devices.net	443	TCP	クラウド制御プレーンとの通信、アプライアンスのモジュールの構成のダウンロード、アプライアンスのモジュールのランタイム ステータスの更新に使用されるアプライアンス。現在の具体的なエンドポイントは次のとおりです。 北米： ■ edgehubprodna.azure-devices.net ヨーロッパ： ■ edgehubprodeu.azure-devices.net 日本： ■ edgehubprodjp.azure-devices.net
Horizon Edge	vmwareprod.wavefront.com	443	TCP	VMware Tanzu® Observability™ by Wavefront に操作メトリックを送信するために使用されます。VMware のオペレータは、お客様をサポートするためのデータを受け取ります。 Tanzu Observability はストリーミング分析プラットフォームです。データを Tanzu Observability に送信し、カスタム ダッシュボードでデータを表示および操作できます。VMware Tanzu Observability by Waveftont のドキュメントを参照してください。

表 2-1. （続き）

ソース	ターゲット	ポート	プロトコル	目的
Horizon Edge	*.data.vmwservices.com	443	TCP	イベントまたはメトリックを Workspace ONE Intelligence に送信してデータを監視します。 Workspace ONE Intelligence を参照してください。 現在の具体的なエンドポイントは次のとおりです。 ■ eventproxy.na1.data.vmwservices.com ■ eventproxy.eu1.data.vmwservices.com ■ eventproxy.eu2.data.vmwservices.com ■ eventproxy.uk1.data.vmwservices.com ■ eventproxy.ca1.data.vmwservices.com ■ eventproxy.ap1.data.vmwservices.com ■ eventproxy.au1.data.vmwservices.com ■ eventproxy.in1.data.vmwservices.com
Horizon Edge	login.microsoftonline.com	443	TCP	一般的に Microsoft Azure サービスに対して認証を行うためにアプリケーションによって使用されます。

表 2-1. （続き）

ソース	ターゲット	ポート	プロトコル	目的
Horizon Edge	management.azure.com	443	TCP	Microsoft Azure Resource Manager エンドポイントへの Edge API リクエストで、Microsoft Azure Resource Manager サービスを使用するために使用されます。Microsoft Azure Resource Manager は、Azure PowerShell、Azure CLI、Azure ポータル、REST API、およびクライアント SDK を通じてタスクを実行するための一貫した管理レイヤーを提供します。
Horizon Edge	NTP サーバ	123	UDP	NTP サービス
Horizon Agent	Horizon Edge	31883	TCP MQTT UDP	仮想マシンで実行されている Horizon Agent から Edge で実行されている MQTT へ。
Horizon Edge	Horizon Connection Server	4002	TCP	Java Messaging Service (JMS) 経由で Horizon Edge から Horizon Connection Server へ。

Horizon 8 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にする

Horizon Edge 環境を作成し、アプライアンス モジュールをインストールまたは更新するには、それぞれのポートで適切な URL を許可する必要があります。

次の表に記載された目的は、Horizon Connection Server を備えた Horizon Edge Gateway のコンテキストを想定しています。

管理サブネットの URL の許可

サイトの場所とニーズに応じて適切な URL およびワイルドカード サブドメインを許可します。具体的には、次のタスクを実行します。

- 次の表の URL およびワイルドカード サブドメインを許可します。たとえば、ファイアウォールの許可リストに URL とワイルドカード サブドメインを追加します。
- 次のように SSL ディープ パケット インスペクションをバイパスします。
  - 次の表の URL およびワイルドカード サブドメインのファイアウォール。

- プロキシ サーバ（該当する場合）。

  したがって、Horizon Edge Gateway がプロキシ サーバを介して Horizon Cloud 制御プレーンに接続されている場合は、次の表の URL とワイルドカード サブドメインに対してプロキシ サーバの SSL ディープ パケット インスペクションをバイパスします。

ターゲット (DNS 名)	ポート	プロトコル	目的
*.blob.core.windows.net	443	TCP	Azure Blob Storage へのプログラム アクセス、および必要に応じて Horizon Edge ログをアップロードするために使用されます。 Docker イメージをダウンロードして、監視、SSO、UAG の更新などに役立つ必要な Horizon Edge モジュールを作成するために使用されます。
horizonedgeprod.azurecr.io	443	TCP	Docker イメージをダウンロードして、監視、SSO、UAG の更新などに役立つ必要な Horizon Edge モジュールを作成する際の認証に使用されます。
*.azure-devices.net、またはテナント アカウントに適用されるリージョン別制御プレーンに対応した、以下のリージョン固有の名前のいずれか。 北米： ■ edgehubprodna.azure-devices.net ヨーロッパ： ■ edgehubprodeu.azure-devices.net 日本： ■ edgehubprodjp.azure-devices.net	443	TCP（要件は HTTP、HTTPS、および WSS を意味します）	アプライアンスを Horizon Cloud 制御プレーンに接続し、アプライアンスのモジュールの構成をダウンロードし、アプライアンスのモジュールのランタイム ステータスを更新するために使用されます。
*.data.vmwservices.com、またはテナント アカウントに適用されるリージョン別 Workspace ONE Intelligence ターゲットに対応した、以下のリージョン固有の名前のいずれか。 ■ eventproxy.na1.data.vmwservices.com ■ eventproxy.eu1.data.vmwservices.com ■ eventproxy.eu2.data.vmwservices.com ■ eventproxy.uk1.data.vmwservices.com ■ eventproxy.ca1.data.vmwservices.com ■ eventproxy.ap1.data.vmwservices.com ■ eventproxy.au1.data.vmwservices.com ■ eventproxy.in1.data.vmwservices.com	443	TCP	イベントまたはメトリックを Workspace ONE Intelligence に送信するために使用されます。 Workspace ONE Intelligence を参照してください。

Microsoft Azure Edge をデプロイするための要件チェックリスト

このチェックリストの目的は、Horizon 制御プレーン を使用してネイティブの Microsoft Azure デプロイを実行するために必要な要素をユーザーに通知することです。

重要： Horizon Cloud on Microsoft Azure デプロイとは、ネイティブの Microsoft Azure インフラストラクチャを指します。

チェックリスト対象者

このチェックリストは、テナント環境に Horizon Cloud on Microsoft Azure をデプロイしたことがない Horizon Cloud 顧客アカウントを対象としています。クリーンスレート環境またはグリーンフィールド環境と呼ばれるこのようなテナントについて聞いたことがあるかもしれません。

Horizon Cloud をデプロイする前に、以降のいくつかの項目を実行する必要があります。一部の項目は、デプロイが完了して実行状態になるまで延期できます。

Microsoft Azure サブスクリプションの要件

構成の制限については、「Horizon Cloud Service - next-gen デプロイのサイジング」を参照してください。これには、VMware 構成の上限ツールの使用に関する情報が含まれています。[構成の上限] ページから、[制限の表示]、[VMware Horizon Cloud Service - next-gen]、最新バージョン、および表示するカテゴリを選択します。

☐	サポートされている Microsoft Azure 環境 (Azure Commercial) で有効な Microsoft Azure サブスクリプション。Horizon Edge Gateway および Unified Access Gateway インスタンスを含む Horizon Edge アプライアンスを独自の専用プロバイダ（Microsoft Azure サブスクリプション）にデプロイする場合は、プールをデプロイするために別の有効な Microsoft Azure サブスクリプションを取得します。 **注：** Horizon Cloud は、ほとんどの Microsoft Azure リージョンをサポートします。
☐	Microsoft Azure ポータルを使用して、Microsoft Azure Edge のデプロイを実行するための各 Microsoft Azure サブスクリプションで有効な Microsoft Azure 管理者権限。
☐	各 Microsoft Azure サブスクリプションに 1 つ以上のサービス プリンシパルを作成し、サブスクリプション ID、ディレクトリ ID、アプリケーション ID を確認して、サブスクリプションの各サービス プリンシパルに適切なロールを割り当てます。 ■ Microsoft Azure サブスクリプションのサービス プリンシパルの作成を参照してください。 ■ サービス プリンシパルにカスタム ロールを使用するには、Horizon Cloud アプリケーション登録にカスタム ロールを使用するを参照してください。 **注：** 複数のサービス プリンシパルを作成すると、サブスクリプション ID とディレクトリ ID が共有されますが、各サービス プリンシパルには独自のアプリケーション ID があります。
☐	デプロイする Microsoft Azure Edge 形式のタイプを決定します。次のオプションを使用できます。 ■ Edge Gateway (VM) = Edge Gateway 仮想マシン Edge Gateway (VM) は、高可用性を使用しない小規模なデプロイ向けです。 ■ Edge Gateway (AKS) = Edge Gateway Azure Kubernetes サービス Edge Gateway (AKS) は高可用性を提供します。

☐	Edge Gateway (AKS) をデプロイするには、Microsoft Azure ユーザー管理 ID を作成します。 AKS クラスタを使用する Horizon Edge には、管理 VNet のリソース グループ スコープでのネットワーク コントリビュータ ロール、および Microsoft Azure サブスクリプション スコープでの管理対象 ID オペレータ ロールを持つユーザー管理 ID が必要です。ユーザー割り当ての管理対象 ID の管理に関する Microsoft のドキュメントを参照してください。 管理サブネットにルート テーブルがあり、そのルート テーブルのリソース グループが VNet のリソース グループと異なる場合は、ネットワーク コントリビュータ ロールもルート テーブルのリソース グループに割り当てる必要があります。
☐	Microsoft Azure サブスクリプションに必要なリソース プロバイダを登録します。必要なリソース プロバイダが Microsoft Azure サブスクリプションに登録されていることの確認を参照してください。
☐	サブスクリプション内の Azure Compute Gallery に読み取り権限を付与するカスタム ロールを作成し、そのカスタム ロールを特定の Horizon Edge 用に構成されたすべてのサービス プリンシパルに割り当てます。
☐	サブスクリプションでは、タグのないリソース グループの作成を許可する必要があります。

Microsoft Azure のキャパシティの要件

次の表で Microsoft Azure のキャパシティを参照している場合、手動インストールは必要ありません。指定されたキャパシティがサブスクリプションで使用可能である限り、デプロイヤは説明された仮想マシンを自動的にインスタンス化します。

☐	コアの Horizon Edge リソースをそのサブスクリプションにデプロイするための Microsoft Azure キャパシティ。 キャパシティ要件は、デプロイする Microsoft Azure Edge の形式（Edge Gateway (AKS) または Edge Gateway (VM)）によって異なります。 ■ [Edge Gateway (AKS)]：アップグレード中の 4 ノード AKS クラスタと追加ノードに十分な割り当て。 ■ Edge Gateway (AKS) デプロイでは、Azure Kubernetes サービス (AKS) クラスタを使用します。これには、キャパシティ用にサポートされている仮想マシン サイズの 1 つを使用する 4 つのノードが必要です。 Edge Gateway (AKS) デプロイでサポートされている仮想マシン SKU サイズのリストを優先順位の降順で次に示します。Microsoft Azure サブスクリプションに、次の仮想マシン SKU サイズの少なくとも 1 つに対するキャパシティがある場合、Edge のデプロイは受け入れられます。それ以外の場合、Edge のデプロイは拒否されます。 ■ Standard_D2s_v3 - vCPU x 2、8 GB メモリ ■ Standard_D2ds_v5 - vCPU x 2、8 GB メモリ ■ Standard_D2a_v4 - vCPU x 2、8 GB メモリ AKS クラスタの通常の動作中は、4 つの仮想マシン ノードが必要です。追加のノードが 1 つ必要で、アップグレード中に使用されます。 ■ [Edge Gateway (VM)]：単一の仮想マシンに十分な割り当て。 Edge Gateway (VM) デプロイでサポートされている仮想マシン SKU サイズのリストを優先順位の降順で次に示します。Microsoft Azure サブスクリプションに、次の仮想マシン SKU サイズの少なくとも 1 つに対するキャパシティがある場合、Edge のデプロイは受け入れられます。それ以外の場合、Edge のデプロイは拒否されます。 ■ Standard_D4s_v3 - vCPU x 4、16 GB メモリ ■ Standard_D4s_v4 - vCPU x 4、16 GB メモリ ■ Standard_D4s_v5 - vCPU x 4、16 GB メモリ ■ コマンドを実行して、Microsoft Azure 仮想マシン モデルの可用性を確認し、リージョン CPU 出力を確認します。Microsoft Azure 仮想マシン モデルの可用性の確認を参照してください。 ■ Unified Access Gateway インスタンス – 次のサポートされるサイズの 2 倍以上。デフォルトおよび推奨サイズは Standard_F8s_v2 です。 ■ Standard_A4_v2 ■ Standard_D8s_v4 ■ Standard_D16s_v4 ■ Standard_D8s_v5 ■ Standard_D16s_v5 ■ Standard_F8s_v2 ■ Standard_F16s_v2 **注：** `A4_v2` 仮想マシン モデルが十分に機能するのは、Horizon Edge でのアクティブなセッション数が 1,000 を超えないことが分かっている PoC（事前検証）環境、パイロット環境、または小規模な環境のみとなります。 Horizon Edge インスタンスを使用する準備ができたら、Microsoft Azure クラウドのキャパシティは、インポートされた仮想マシン、イメージ、プール仮想マシン、およびその Horizon Edge インスタンスで作成する App Volumes アプリキャプチャ仮想マシンにも対応する必要があります。Image Management System Requirements セクションを参照してください。

ネットワーク要件

次のネットワーク要件には、Horizon Edge を正常にデプロイして運用するために必要な詳細が含まれます。次の 2 つの表は似ていますが、異なります。デプロイを計画している Microsoft Azure Edge 形式のタイプ（Edge Gateway (VM) または Edge Gateway (AKS)）に適用される表を使用してください。

Edge Gateway (VM)

Edge Gateway (VM) のデプロイには、次の表を使用します。

表 2-2. Edge Gateway (VM) のネットワーク要件

☐	必要なサブネットをカバーする適切なアドレス空間を使用して、ターゲットの Microsoft Azure リージョンに Microsoft Azure 仮想ネットワーク (VNet) が作成済みであること。Microsoft Azure リージョンのネットワーク設定の構成を参照してください。
☐	次のサブネット要件が最小です。大規模な環境では、より大きなサブネットが必要になる場合があります。 ■ 管理サブネット - /26 以上 ■ デスクトップ（テナント）サブネット - プライマリ - /27 以上。ただしデスクトップと RDS サーバの数に基づいて適切なサイズを設定します。必要に応じてサブネットを追加できます。 ■ DMZ サブネット - Unified Access Gateway インスタンスのクラスタの /27 以上(内部 Unified Access Gateway アクセス タイプには不要)。 前提条件として、VNet でサブネットを手動で作成する必要があります。Microsoft Azure リージョンのネットワーク設定の構成を参照してください。ベスト プラクティスとして、他のリソースをサブネットに接続しないでください。 専用プロバイダを使用して Horizon Gateway アプライアンス（Horizon Edge Gateway および Unified Access Gateway）をデプロイする場合は、デスクトップのデプロイ元となるプロバイダにバックエンド サブネットを作成する必要があります。
☐	内部マシン名と外部名の両方を解決できる有効な DNS サーバを参照するように VNet (仮想ネットワーク) DNS サーバを構成していること。Horizon Edge Gateway および Unified Access Gateway のデプロイ後に必要な DNS レコードを構成するを参照してください。 内部エンドポイントの場合、Active Directory サーバは 1 つの例です。 外部エンドポイントの場合、ゲートウェイのデプロイに対して使用している VNet 上のアウトバウンド インターネット アクセスでは、特定のポートとプロトコルを使用して特定の DNS 名を解決し、その名前にアクセスする必要があります。これは、デプロイおよび継続的な運用に必要です。
☐	Horizon Edge デプロイに対して使用している VNet 上のアウトバウンド インターネット アクセスでは、特定のポートとプロトコルを使用して特定の DNS 名を解決し到達する必要があります。これは、デプロイおよび継続的な運用に必要です。DNS 名とポートのリストについては、Microsoft Azure 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にするを参照してください。
☐	任意。プロキシ サーバ情報（VNet での外部へのインターネット アクセスに必要な場合)。Horizon Cloud 環境のデプロイおよび継続的な運用で使用されます。
☐	任意。VNet とオンプレミスの企業のネットワーク間のネットワークが必要な場合は、Microsoft Azure VPN/Express Route を構成します。

Edge Gateway (AKS)

Edge Gateway (AKS) のデプロイには、次の表を使用します。これらの要件には、AKS クラスタを使用した Horizon Edge Gateway の構成のサポートが含まれています。AKS クラスタを使用して Horizon Edge Gateway を構成すると、より簡単に拡張可能なソリューションが提供されます。

表 2-3. Edge Gateway (AKS) のネットワーク要件

☐	必要なサブネットをカバーする適切なアドレス空間を使用して、ターゲットの Microsoft Azure リージョンに Microsoft Azure 仮想ネットワーク (VNet) が作成済みであること。Microsoft Azure リージョンのネットワーク設定の構成を参照してください。
☐	次のサブネット要件が最小です。大規模な環境では、より大きなサブネットが必要になる場合があります。 ■ 管理サブネット - /26 以上 Edge Gateway (AKS) をデプロイする場合は、AKS クラスタを使用する Horizon Edge は送信接続用の NAT ゲートウェイを必要とするため、管理サブネットの NAT ゲートウェイを構成します。 ■ デスクトップ（テナント）サブネット - プライマリ - /27 以上。ただしデスクトップと RDS サーバの数に基づいて適切なサイズを設定します。必要に応じてサブネットを追加できます。 ■ DMZ サブネット - Unified Access Gateway インスタンスのクラスタの /27 以上(内部 Unified Access Gateway アクセス タイプには不要)。 前提条件として、VNet でサブネットを手動で作成する必要があります。Microsoft Azure リージョンのネットワーク設定の構成を参照してください。ベスト プラクティスとして、他のリソースをサブネットに接続しないでください。 専用プロバイダを使用して Horizon Gateway アプライアンス（Horizon Edge Gateway および Unified Access Gateway）をデプロイする場合は、デスクトップのデプロイ元となるプロバイダにバックエンド サブネットを作成する必要があります。
☐	Edge Gateway (AKS) をデプロイし、Edge の作成時にクラスタ送信タイプの値として NAT ゲートウェイを選択する場合は、管理サブネットで NAT ゲートウェイを構成して、Horizon Edge Gateway の送信接続を有効にします。Edge の作成時にクラスタ送信タイプの値としてユーザー定義ルートを選択した場合は、デフォルト ルート 0.0.0.0/0 がタイプ [VirtualAppliance] または [VirtualNetworkGateway] のネクスト ホップを指しているルート テーブルを管理サブネット上に構成します。
☐	デプロイ時に Horizon Edge Gateway を構成するために必要な、次の CIDR IP アドレス範囲を収集します。 **注：** これらの範囲が環境内で使用されている他の範囲と競合しないようにしてください。 ■ サービス CIDR - /27 以上 ■ ポッド CIDR - /21 以上 Edge Gateway (AKS) をデプロイする場合、AKS クラスタを正常に展開するには、次の Microsoft Azure 要件に準拠する必要があります。Horizon Universal Console を使用して Horizon Edge をデプロイするときは、管理サブネットの VNet のサービス CIDR、ポッド CIDR、およびアドレス空間が次の IP アドレス範囲と競合していないことを確認します。 ■ 169.254.0.0/16 ■ 172.30.0.0/16 ■ 172.31.0.0/16 ■ 192.0.2.0/24
☐	内部マシン名と外部名の両方を解決できる有効な DNS サーバを参照するように VNet (仮想ネットワーク) DNS サーバを構成していること。Horizon Edge Gateway および Unified Access Gateway のデプロイ後に必要な DNS レコードを構成するを参照してください。 内部エンドポイントの場合、Active Directory サーバは 1 つの例です。 外部エンドポイントの場合、ゲートウェイのデプロイに対して使用している VNet 上のアウトバウンド インターネット アクセスでは、特定のポートとプロトコルを使用して特定の DNS 名を解決し、その名前にアクセスする必要があります。これは、デプロイおよび継続的な運用に必要です。

表 2-3. Edge Gateway (AKS) のネットワーク要件 （続き）

☐	Horizon Edge デプロイに対して使用している VNet 上のアウトバウンド インターネット アクセスでは、特定のポートとプロトコルを使用して特定の DNS 名を解決し到達する必要があります。これは、デプロイおよび継続的な運用に必要です。DNS 名とポートのリストについては、Microsoft Azure 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にするを参照してください。
☐	任意。プロキシ サーバ情報（VNet での外部へのインターネット アクセスに必要な場合）。Horizon Cloud 環境のデプロイおよび継続的な運用で使用されます。
☐	任意。VNet とオンプレミスの企業のネットワーク間のネットワークが必要な場合は、Microsoft Azure VPN/Express Route を構成します。
☐	Edge Gateway (AKS) をデプロイする場合、AKS クラスタを使用する Horizon Edge に関して、Horizon Edge のデプロイに使用している VNet にカスタム DNS サーバがある場合は、Microsoft Azure DNS IP アドレス 168.63.129.16 を、外部名解決用の DNS フォワーダとして追加できます。

ポートとプロトコルの要件

☐	デプロイと Horizon Cloud 環境の継続的な運用には特定のポートとプロトコルが必要です。Microsoft Azure での Horizon Cloud 環境のポートとプロトコルの要件を参照してください。

Unified Access Gateway の要件

Unified Access Gateway 仮想マシンのクラスタがプールに関連付けられているため、クライアントはそのプール内の仮想マシンへの信頼された HTML Access 接続を確立できます。

Horizon Universal Console を使用して Horizon Cloud に Unified Access Gateway を構成します。以下の項目は、そのタイプの構成に必要です。

☐	*.horizon.vmware.com への送信インターネット アクセスはすべての構成タイプで必要です。 [企業のネットワーク経由の内部アクセスの許可] が [Unified Access Gateway アクセス タイプ] である場合、ユーザー定義のルーティングまたは NAT ゲートウェイのいずれかを管理サブネットに適用して、送信トラフィックを許可できます。 [Unified Access Gateway アクセス タイプ] が DMZ ネットワークを使用して外部に構成されている場合は、DMZ ネットワーク上で *.horizon.vmware.com への外部アクセスを構成する必要があります。
☐	Unified Access Gateway の構成には FQDN が必要です。
☐	FQDN に一致する PEM 形式の Unified Access Gateway の証明書。 **注：** この目的で提供する 1 つまたは複数の証明書が、特定の DNS 名を参照する CRL（証明書失効リスト）または OCSP（オンライン証明書ステータス プロトコル）の設定を使用する場合、次に、それらの DNS 名への VNet 上のアウトバウンド インターネット アクセスが解決可能で到達可能であることを確認する必要があります。Unified Access Gateway 構成で提供された証明書を構成するときに、Unified Access Gateway ソフトウェアはこれらの DNS 名にアクセスして、証明書の失効ステータスを確認します。これらの DNS 名にアクセスできない場合、デプロイは失敗します。これらの名前は、証明書の取得に使用した CA に大きく依存し、VMware のコントロールには含まれません。

ユーザー ID とマシン ID について

Horizon Cloud Service - next-gen は、ID の処理方法が他の環境とは異なります。Horizon Cloud Service - next-gen では、サービスはユーザー ID とマシン ID を区別し、クライアントとリモート デスクトップまたはアプリケーション間の安全な接続を確立するときに両方のタイプの ID に依存します。

注： 第 1 世代の Horizon Cloud 環境や Horizon 8 オンプレミス環境など、単一の ID プロバイダを使用してユーザーとマシンの両方の ID を認証する環境に慣れている場合は、ユーザー ID とマシン ID の区別を行うのは初めてかもしれません。

Horizon Cloud Service - next-gen では、ユーザー ID を認証するための ID プロバイダとマシン ID を認証するための ID プロバイダで構成される ID 構成を設定する必要があります。

ユーザー ID

Horizon Cloud Service - next-gen では、ユーザー ID プロバイダを登録する必要があります。サービスは、この ID プロバイダを使用して、リモート デスクトップおよびアプリケーションにアクセスしようとするクライアント ユーザーを認証します。

マシン ID

Horizon Cloud Service - next-gen では、マシン ID プロバイダも登録する必要があります。サービスは、この ID プロバイダを使用して、リモート デスクトップとアプリケーションを提供する仮想マシンのマシン ID を確立します。

マシン ID プロバイダを介して、サービスはリモート デスクトップとリモート アプリケーションの仮想マシン ソースを、クライアント ユーザーがアクセスする資格が付与されている信頼できるネットワーク ドメインに参加させます。

サポートされている ID 構成

Horizon Cloud Service - next-gen では、ユーザー ID プロバイダとマシン ID プロバイダで構成される ID 構成を登録する必要があります。機能は、構成に含まれる特定の ID プロバイダによって異なる場合があります。

Horizon Cloud Service - next-gen は、次の ID 構成をサポートしています。

表 2-4. Horizon Cloud Service - next-gen でサポートされる ID 構成

ID 構成	ユーザー ID プロバイダ	マシン ID プロバイダ	機能に関する注意事項
A	Microsoft Entra ID	Active Directory	■ リモート デスクトップおよびアプリケーションへの SSO をサポート
B	Microsoft Entra ID	Microsoft Entra ID	■ リモート デスクトップおよびアプリケーションへのシングル サインオン (SSO) をサポートしない
C	Workspace ONE Access	Active Directory	■ リモート デスクトップおよびアプリケーションへの SSO をサポート ■ Workspace ONE との統合をサポート

このページの次のセクションでは、サポートされている各ユーザー ID プロバイダとマシン ID プロバイダの詳細な要件について説明します。

ユーザー ID の要件

このセクションでは、ID 構成で使用するユーザー ID プロバイダの要件について説明します。Horizon Cloud Service - next-gen は、ユーザー ID のプロバイダとして Microsoft Entra ID と Workspace ONE Access をサポートします。

このセクションで説明する要件に加えて、機能の考慮事項と各ユーザー ID プロバイダで使用できるマシン ID プロバイダについては、「サポートされている ID 構成」を参照してください。Horizon Cloud Service - next-gen が ID を管理する方法の概要については、「ユーザー ID とマシン ID について」を参照してください。

Microsoft Entra ID

☐	Microsoft Entra ID がユーザー ID プロバイダの場合、グローバル管理者権限を持つユーザーは次の操作を行う必要があります。 ■ 要求された権限を承認する。 ■ 組織全体の同意書を提供する。

Workspace ONE Access

☐	Workspace ONE Access Workspace ONE Access がユーザー ID プロバイダの場合、管理者権限を持つユーザーは次の操作を行う必要があります。 ■ 要求された権限を承認する。 ■ 組織全体の同意書を提供する。

マシン ID の要件

このセクションでは、ID 構成で使用するマシン ID プロバイダの要件について説明します。Horizon Cloud Service - next-gen は、マシン ID のプロバイダとして Microsoft Entra ID と Active Directory をサポートします。

このセクションで説明する要件に加えて、機能の考慮事項と各マシン ID プロバイダで使用できるユーザー ID プロバイダについては、「サポートされている ID 構成」を参照してください。Horizon Cloud Service - next-gen が ID を管理する方法の概要については、「ユーザー ID とマシン ID について」を参照してください。

Microsoft Entra ID

☐	プールまたは仮想マシンの削除を可能にする場合、サービス プリンシパルには Microsoft Entra ID からデバイス エントリを削除する権限が必要です。 権限は次のとおりです。 ■ `Scope: https://graph.microsoft.com/` ■ `Permission : Device.ReadWrite.All` ■ `Read and write devices` ■ `Admin Consent : Yes` 権限を付与するには、次の場所に移動します。 [サブスクリプション -> Azure Active Directory -> アプリケーションの登録 -> 権限を付与する必要があるアプリケーションを選択 -> API 権限 -> Microsoft GRAPH -> Device.ReadWriteAll を選択]
☐	Microsoft Entra ID で RBAC を構成します。 この構成により、[仮想マシン管理者ログイン] または [仮想マシン ユーザー ログイン] ロールを持つユーザーまたはユーザーグループのみが資格にログインできるようになります。

Active Directory

☐	Horizon Edge Gateway インスタンスとデスクトップ サブネットを認識できる Active Directory サーバ。次に例を示します。 ■ VPN/ExpressRoute を介して接続されたオンプレミス Active Directory サーバ ■ Microsoft Azure にある Active Directory サーバ
☐	LDAPS を使用して Active Directory に接続する場合は、Active Directory ドメインの PEM でエンコードされたルート CA 証明書と中間 CA 証明書を収集します。 Horizon Universal Console を使用して Active Directory ドメインを設定すると、その時点で、PEM エンコードされたルート CA 証明書と中間 CA 証明書をアップロードするように求められます。
☐	サポートされる Microsoft Windows Active Directory Domain Services (AD DS) のドメイン機能レベル。 ■ Windows Server 2016 ■ Windows Server 2012 R2 ■ Windows Server 2012 サポートされる Microsoft Windows Active Directory Domain Services (AD DS) の OS バージョン。 ■ Windows Server 2019 ■ Windows Server 2016 ■ Windows Server 2012 R

☐	**ドメイン バインド アカウント** sAMAccountName 属性を持つ Active Directory ドメイン バインド アカウント（読み取りアクセス権限を持つ標準ユーザー）。sAMAccountName 属性は 20 文字以下にする必要があります。また、"/ \ [ ] : ; | = , + * ? < > の文字を含めることはできません。 アカウントは、以下の権限を持つ必要があります。 ■ コンテンツの一覧表示 ■ すべてのプロパティの読み取り ■ アクセス許可の読み取り ■ tokenGroupsGlobalAndUniversal の読み取り（すべてのプロパティの読み取り により暗黙に含まれる） また、アカウントのパスワードを 無期限 に設定して、Horizon Cloud 環境にログインするために引き続きアクセスできるようにします。 ■ Horizon オンプレミス サービスに精通している場合、上記の権限は、Horizon オンプレミス サービスの 2 番目の認証情報アカウントに必要なセットと同じです。 ■ ドメイン バインド アカウントには、Microsoft Active Directory デプロイで認証されたユーザーに通常付与される、デフォルトの特別な設定は不要の読み取りアクセス関連の権限が付与されています。ただし、組織の Active Directory 管理者が通常ユーザーの読み取りアクセス権に関連する権限をロックダウンすることを選択した場合は、それらの Active Directory 管理者に、Horizon Cloud に使用するドメイン バインド アカウントの認証済みユーザーの標準デフォルト設定を保持するように要求する必要があります。 参照：Active Directory ドメイン バインドおよびドメイン参加アカウントの作成
☐	**補助ドメイン バインド アカウント** メインのドメイン バインド アカウントとは別にする必要があります。ユーザー インターフェイスでは、両方のフィールドで同じアカウントを再利用しません。 sAMAccountName 属性を持つ Active Directory ドメイン バインド アカウント（読み取りアクセス権限を持つ標準ユーザー）。sAMAccountName 属性は 20 文字以下にする必要があります。また、"/ \ [ ] : ; | = , + * ? < > の文字を含めることはできません。 アカウントは、以下の権限を持つ必要があります。 ■ コンテンツの一覧表示 ■ すべてのプロパティの読み取り ■ アクセス許可の読み取り ■ tokenGroupsGlobalAndUniversal の読み取り（すべてのプロパティの読み取り により暗黙に含まれる） また、アカウントのパスワードを 無期限 に設定して、Horizon Cloud 環境にログインするために引き続きアクセスできるようにします。 ■ Horizon オンプレミス サービスに精通している場合、上記の権限は、Horizon オンプレミス サービスの 2 番目の認証情報アカウントに必要なセットと同じです。 ■ ドメイン バインド アカウントには、Microsoft Active Directory デプロイで認証されたユーザーに通常付与される、デフォルトの特別な設定は不要の読み取りアクセス関連の権限が付与されています。ただし、組織の Active Directory 管理者が通常ユーザーの読み取りアクセス権に関連する権限をロックダウンすることを選択した場合は、それらの Active Directory 管理者に、Horizon Cloud に使用するドメイン バインド アカウントの認証済みユーザーの標準デフォルト設定を保持するように要求する必要があります。

□	**ドメイン参加アカウント** システムが Sysprep 操作を実行し、仮想コンピュータをドメインに参加させるために使用できる Active Directory ドメイン参加アカウント。通常は、この明確な目的のために作成する新しいアカウントです。（ドメイン参加ユーザー アカウント） このアカウントには、sAMAccountName 属性が必須です。sAMAccountName 属性は 20 文字以下にする必要があります。また、`"/ \ [ ] : ; | = , + * ? < >` の文字を含めることはできません。 アカウントのユーザー名に空白を使用することは、現在サポートされていません。 Horizon Cloud が継続して Sysprep 操作を実行し、仮想コンピュータをドメインに参加させるために、アカウントのパスワードを 無期限 に設定します。 このアカウントには、コンピュータ OU、またはコンソールのドメイン参加ユーザー インターフェイスに入力する OU に適用される次の Active Directory 権限が必要です。 ■ すべてのプロパティの読み取り：このオブジェクトのみ ■ コンピュータ オブジェクトの作成：このオブジェクトとすべての子孫オブジェクト ■ コンピュータ オブジェクトの削除：このオブジェクトとすべての子孫オブジェクト ■ すべてのプロパティの書き込み：子孫コンピュータ オブジェクト ■ パスワードのリセット：子孫コンピュータ オブジェクト プールに使用するターゲット組織単位 (OU) については、このアカウントには、そのターゲット組織単位 (OU) のすべての子孫オブジェクトに対する「すべてのプロパティの書き込み」という名前の Active Directory 権限も必要です。 ドメイン参加アカウントの作成と再利用の詳細については、Active Directory ドメイン バインドおよびドメイン参加アカウントの作成を参照してください。 Microsoft Active Directory では、新しい組織単位 (OU) を作成するときに、システムは、新しく作成された OU およびすべての子孫オブジェクトの [すべての子オブジェクトの削除] 権限に `Deny` を適用する `Prevent Accidental Deletion` 属性を自動的に設定する場合があります。その結果、ドメイン参加アカウントに [コンピュータ オブジェクトの削除] 権限を明示的に割り当てた場合、新しく作成された OU の場合、Active Directory は、明示的に割り当てられた [コンピュータ オブジェクトの削除] 権限に上書きを適用した可能性があります。[誤削除の防止] フラグをオフにしても、Active Directory が [すべての子オブジェクトの削除] 権限に適用した `Deny` が自動的にオフにならない場合があるため、新しく追加された OU の場合、Horizon Cloud コンソールでドメイン参加アカウントを使用する前に、OU およびすべての 子 OU の [すべての子オブジェクトの削除] に対して設定した `Deny` 権限を確認して手動でクリアする必要がある場合があります。

☐	**オプションの補助ドメイン参加アカウント** システムが Sysprep 操作を実行し、仮想コンピュータをドメインに参加させるために使用できる Active Directory ドメイン参加アカウント。通常は、この明確な目的のために作成する新しいアカウントです。(ドメイン参加ユーザー アカウント) このアカウントには、sAMAccountName 属性が必須です。sAMAccountName 属性は 20 文字以下にする必要があります。また、`"/ \ [ ] : ; | = , + * ? < >` の文字を含めることはできません。 アカウントのユーザー名に空白を使用することは、現在サポートされていません。 Horizon Cloud が継続して Sysprep 操作を実行し、仮想コンピュータをドメインに参加させるために、アカウントのパスワードを 無期限 に設定します。 このアカウントには、コンピュータ OU、またはコンソールのドメイン参加ユーザー インターフェイスに入力する OU に適用される次の Active Directory 権限が必要です。 ■ すべてのプロパティの読み取り：このオブジェクトのみ ■ コンピュータ オブジェクトの作成：このオブジェクトとすべての子孫オブジェクト ■ コンピュータ オブジェクトの削除：このオブジェクトとすべての子孫オブジェクト ■ すべてのプロパティの書き込み：子孫コンピュータ オブジェクト ■ パスワードのリセット：子孫コンピュータ オブジェクト プールに使用するターゲット組織単位 (OU) については、このアカウントには、そのターゲット組織単位 (OU) のすべての子孫オブジェクトに対する「すべてのプロパティの書き込み」という名前の Active Directory 権限も必要です。 Microsoft Active Directory では、新しい組織単位 (OU) を作成するときに、システムは、新しく作成された OU およびすべての子孫オブジェクトの [すべての子オブジェクトの削除] 権限に `Deny` を適用する `Prevent Accidental Deletion` 属性を自動的に設定する場合があります。その結果、ドメイン参加アカウントに [コンピュータ オブジェクトの削除] 権限を明示的に割り当てた場合、新しく作成された OU の場合、Active Directory は、明示的に割り当てられた [コンピュータ オブジェクトの削除] 権限に上書きを適用した可能性があります。[誤削除の防止] フラグをオフにしても、Active Directory が [すべての子オブジェクトの削除] 権限に適用した `Deny` が自動的にオフにならない場合があるため、新しく追加された OU の場合、Horizon Cloud コンソールでドメイン参加アカウントを使用する前に、OU およびすべての 子 OU の [すべての子オブジェクトの削除] に対して設定した `Deny` 権限を確認して手動でクリアする必要がある場合があります。
☐	仮想デスクトップおよび RDS セッションベースのデスクトップまたは公開アプリケーション、またはその両方の Active Directory 組織単位 (OU)。 Microsoft Active Directory では、新しい組織単位 (OU) を作成するときに、システムは、新しく作成された OU およびすべての子孫オブジェクトの [すべての子オブジェクトの削除] 権限に `Deny` を適用する `Prevent Accidental Deletion` 属性を自動的に設定する場合があります。その結果、ドメイン参加アカウントに [コンピュータ オブジェクトの削除] 権限を明示的に割り当てた場合、新しく作成された OU の場合、Active Directory は、明示的に割り当てられた [コンピュータ オブジェクトの削除] 権限に上書きを適用した可能性があります。[誤削除の防止] フラグをオフにしても、Active Directory が [すべての子オブジェクトの削除] 権限に適用した `Deny` が自動的にオフにならない場合があるため、新しく追加された OU の場合、Horizon Cloud コンソールでドメイン参加アカウントを使用する前に、OU およびすべての 子 OU の [すべての子オブジェクトの削除] に対して設定した `Deny` 権限を確認して手動でクリアする必要がある場合があります。

Image Management System Requirements

Microsoft Azure サブスクリプションは、デプロイされた Horizon Edge からプロビジョニングするイメージの種類に応じて、次の要件を満たす必要があります。

☐	イメージの基本。1 つ以上のサポートされている Microsoft Azure 仮想マシン構成。 ■ Microsoft Azure 第 1 世代および第 2 世代の仮想マシンがサポートされています。 ベース仮想マシンに使用するモデルに十分な割り当てがあることを確認します。次のモデル タイプはデフォルトであり、推奨されます。 [非 GPU：] ■ Standard_DS2_v2 [GPU 対応：] ■ Standard_NV12s_v3 リストされている [非 GPU] および [GPU 対応] タイプ以外のモデル タイプもサポートされていますが、これらは必ずしも検証されているわけではありません。これらのモデルのいずれかを選択する場合は、サブスクリプションに十分な割り当てがあることを確認します。

プール仮想マシンの要件

Microsoft Azure サブスクリプションは、デプロイされた Horizon Edge からプロビジョニングするプール仮想マシンの種類に応じて、次の要件を満たす必要があります。

☐	プールの仮想マシンのモデル選択 - Microsoft Azure リージョンで使用可能な Microsoft Azure 仮想マシン構成のいずれか (Horizon Cloud デスクトップ操作と互換性のないものを除く)。 仮想マシン モデルを選択するときは、次の詳細について考慮します。 ■ GPU 対応モデル タイプと非 GPU モデル タイプの選択は、イメージの作成時に選択した仮想マシンによって決まります。 ■ マルチセッション プールを作成するには、マルチセッション オペレーティング システムを使用して作成されたイメージを選択します。 ■ 本番環境では、スケール テストでは、2 個以上の CPU を搭載したモデルを使用することをお勧めします。 ■ Horizon Cloud Service - next-gen の Microsoft Azure 仮想マシンのタイプとサイズ (89090) を参照し、Microsoft Azure 仮想マシンのさまざまなタイプとサイズと VMware Horizon Cloud Service - next-gen との互換性を確認してください。 ■ Microsoft Azure の第 1 世代および第 2 世代の仮想マシンは、プールでサポートされています。

Horizon Client および Horizon HTML Access（Web クライアント）の要件

☐	Horizon Cloud 環境で使用資格が付与されたリソースへのエンド ユーザー アクセスを有効にするには、次のサポート対象クライアントのいずれかを使用していることを確認します。 **Horizon Client** エンド ユーザーは、次の Horizon Client バージョンを使用できます。 ■ Horizon Client for Windows 2111 以降 ■ Horizon Client for Mac 2111 以降 ■ Horizon Client for Linux 2206 以降 ■ Horizon Client for Android 2303 以降 ■ Horizon Client for iOS 2303 以降 ■ Horizon Client for Chrome 2306 以降 **Horizon HTML Access** エンド ユーザーは、Horizon Cloud 環境に組み込まれている HTML Access のバージョンに接続できます。

Microsoft Azure での Horizon Cloud 環境のポートとプロトコルの要件

このページは、Horizon Cloud Service - next-gen の Microsoft Azure 環境の一般的な Horizon Cloud Service 内の通信に使用されるすべてのポートとプロトコルのリファレンスです。以下の表を使用して、ネットワーク構成とファイアウォールで正常なデプロイと日常操作に必要な通信トラフィックが可能になるようにします。

特定のデプロイに必要な特定のポートとプロトコルは、Microsoft Azure 環境の Horizon Cloud Service に使用する機能によって一部異なります。特定のコンポーネントまたはプロトコルを使用しない場合、その必要な通信トラフィックはユーザーの目的には不要であり、そのコンポーネントに関連付けられているポートは無視してもかまいません。たとえば、エンド ユーザーが Blast Extreme 表示プロトコルのみを使用する場合、PCoIP ポートの許可は必須ではありません。

重要： ここで説明するポートとプロトコルに加えて、Horizon Edge 環境と対応する日常の操作には、特定の DNS 要件があります。詳細については、Microsoft Azure 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にするを参照してください。

Horizon Edge で必要なポートおよびプロトコル

Horizon インフラストラクチャの監視 を有効にすると、Horizon Edge がデプロイされ、関連付けられたサブスクリプションで構成されます。以下の表には、有効化プロセスの実行中に必要となるポートとプロトコルが記載されています。このプロセスでは、アプライアンスをデプロイし、アプライアンスがそれらのコンポーネントから設計に従って収集する監視データを収集できるようにマネージャ仮想マシンを構成します。またこの表には、設計に従って収集すべきデータを収集する定常状態の運用中に必要なポートとプロトコルも記載されています。

表 2-5.

ソース	ターゲット	ポート	プロトコル	目的
Horizon Edge	Unified Access Gateway 台の仮想マシン	9443	HTTPS	このポートは、Edge の Unified Access Gateway 構成の設定を構成するために、管理サブネット上の Edge 仮想マシンによって使用されます。このポート要件は、Unified Access Gateway 構成を最初にデプロイする場合、および Edge を編集して Unified Access Gateway 構成を追加する場合、またはその Unified Access Gateway 構成を更新する場合に適用されます。また、Unified Access Gateway からのセッション統計情報を監視する場合にも適用されます。
Horizon Edge	ドメイン コントローラ	Kerberos：88 LDAP：389、3268 LDAPS：636、3269	TCP UDP	Horizon Cloud NextGen をドメインに登録し、SSO ログインとドメイン コントローラの定期的な検出を行います。 LDAP/LDAPS がそのワークフローで指定される場合、これらのポートは LDAP または LDAPS サービスに必要です。LDAP は、ほとんどのテナントでデフォルトです。 ターゲットは、Active Directory 構成内のドメイン コントローラのロールが含まれているサーバです。

表 2-5. （続き）

ソース	ターゲット	ポート	プロトコル	目的
Horizon Edge	AD 証明書サービス	135 および 49152 ～ 65535 の範囲内のポート	RPC/TCP	Microsoft Enterprise Certificate Authority (AD CS) に接続して、True SSO の一時的な証明書を取得します。Horizon Edge は、最初の RPC 通信に TCP ポート 135 を使用し、次に 49152 ～ 65535 の範囲内のポートを使用して AD CS (Active Directory Certificate Services) と通信します。
Horizon Edge	DNS サーバ	53 および 853	TCP UDP	DNS サービス。
Horizon Edge	*.file.core.windows.net	445	TCP	パッケージをインポートし、ファイル共有間でパッケージをレプリケートする App Volumes ワークフロー用にプロビジョニングされたファイル共有へのアクセス。
Horizon Edge	■ *.blob.core.windows.net ■ *.blob.storage.azure.net	443	TCP	Azure BLOB ストレージへのプログラム アクセス、および必要に応じて Horizon Edge ログをアップロードするために使用されます。 Docker イメージをダウンロードして、監視、SSO、UAG の更新などに役立つ必要な Horizon Edge モジュールを作成するために使用されます。
Horizon Edge	horizonedgeprod.azurecr.io	443	TCP	Docker イメージをダウンロードして、監視、SSO、UAG の更新などに役立つ必要な Horizon Edge モジュールを作成する際の認証に使用されます。

表 2-5. （続き）

ソース	ターゲット	ポート	プロトコル	目的
Horizon Edge	*.azure-devices.net	443	TCP	クラウド制御プレーンとの通信、アプライアンスのモジュールの構成のダウンロード、アプライアンスのモジュールのランタイム ステータスの更新に使用されるアプライアンス。現在の具体的なエンドポイントは次のとおりです。 北米： ■ edgehubprodna.azure-devices.net ヨーロッパ： ■ edgehubprodeu.azure-devices.net 日本： ■ edgehubprodjp.azure-devices.net
Horizon Edge	vmwareprod.wavefront.com	443	TCP	Wavefront による Observability を VMware Tanzu に操作メトリックを送信するために使用されます。VMware のオペレータは、お客様をサポートするためのデータを受け取ります。 Tanzu Observability はストリーミング分析プラットフォームです。データを Tanzu Observability に送信し、カスタム ダッシュボードでデータを表示および操作できます。VMware Tanzu Observability by Wavefront のドキュメントを参照してください。

表 2-5. （続き）

ソース	ターゲット	ポート	プロトコル	目的
Horizon Edge	*.data.vmwservices.com	443	TCP	イベントまたはメトリックを Workspace ONE Intelligence に送信してデータを監視します。 Workspace ONE Intelligence を参照してください。 現在の具体的なエンドポイントは次のとおりです。 ■ eventproxy.na1.data.vmwservices.com ■ eventproxy.eu1.data.vmwservices.com ■ eventproxy.eu2.data.vmwservices.com ■ eventproxy.uk1.data.vmwservices.com ■ eventproxy.ca1.data.vmwservices.com ■ eventproxy.ap1.data.vmwservices.com ■ eventproxy.au1.data.vmwservices.com ■ eventproxy.in1.data.vmwservices.com
Horizon Edge	login.microsoftonline.com	443	TCP	一般的に Microsoft Azure サービスに対して認証を行うためにアプリケーションによって使用されます。

表 2-5. （続き）

ソース	ターゲット	ポート	プロトコル	目的
Horizon Edge	management.azure.com	443	TCP	Microsoft Azure Resource Manager エンドポイントへの Edge API リクエストで、Microsoft Azure Resource Manager サービスを使用するために使用されます。Microsoft Azure Resource Manager は、Azure PowerShell、Azure CLI、Azure ポータル、REST API、およびクライアント SDK を通じてタスクを実行するための一貫した管理レイヤーを提供します。

表 2-5. （続き）

ソース	ターゲット	ポート	プロトコル	目的
Horizon Edge	*.horizon.vmware.com リージョン固有 US ■ cloud-sg-us-r-westus2.horizon.vmware.com ■ cloud-sg-us-r-eastus2.horizon.vmware.com ■ cloud-sg-us.horizon.vmware.com EU ■ cloud-sg-eu-r-northeurope.horizon.vmware.com ■ cloud-sg-eu-r-germanywestcentral.horizon.vmware.com ■ cloud-sg-eu.horizon.vmware.com JP ■ cloud-sg-jp-r-japaneast.horizon.vmware.com ■ cloud-sg-jp.horizon.vmware.com	443	TCP	クラウド制御プレーンとの通信および Day 2 運用に使用されるアプライアンス。
Horizon Edge	NTP サーバ	123	UDP	NTP サービス

Unified Access Gateway 仮想マシンのポートとプロトコルの要件

上記の表に記載されたプライマリ ポートとプロトコルの要件に加え、以下の表のポートとプロトコルは、デプロイ後の継続的な運用のために動作するように構成したゲートウェイに関連しています。

Unified Access Gateway インスタンスで構成されている接続では、Unified Access Gateway インスタンスから以下の表に記載されているターゲットへのトラフィックを許可する必要があります。

表 2-6. Unified Access Gateway インスタンスからのトラフィックのポート要件

ソース	ターゲット	ポート	プロトコル	目的
Unified Access Gateway	*.horizon.vmware.com	DMZ ネットワーク上の 53 または 443	TCP UDP	Unified Access Gateway は、これらのアドレスをいつでも解決できる必要があります。解決できない場合、ユーザーはセッションを起動できません。これは、Unified Access Gateway が次の場所から JWK セットを取得するためです。 cloud-sg-<region>-r-<DC>.horizon.vmware.com 現在の具体的なエンドポイントは次のとおりです。 ■ US ■ cloud.horizon.vmware.com cloud-sg-us-r-westus2.horizon.vmware.com cloud-sg-us-r-eastus2.horizon.vmware.com ■ cloud.horizon.vmware.com cloud-sg-us-r-westus2.horizon.vmware.com cloud-sg-us-r-eastus2.horizon.vmware.com ■ EU ■ cloud.horizon.vmware.com cloud-sg-eu-r-northeurope.horizon.vmware.com cloud-sg-eu-r-germanywestcentral.horizon.vmware.com ■ JP ■ cloud.horizon.vmware.com cloud-sg-jp-r-japaneast.horizon.vmware.com
Unified Access Gateway	デスクトップまたはファーム RDSH 仮想マシン内の Horizon Agent	22443	TCP UDP	Blast Extreme デフォルトでは、Blast Extreme を使用する場合、クライアント ドライブ リダイレクト (CDR) トラフィックおよび USB トラフィックはこのポート内でサイド チャネルされます。好みに応じて、CDR トラフィックは TCP 9427 ポート上で、USB リダイレクト トラフィックは TCP 32111 ポート上で分離できます。
Unified Access Gateway	デスクトップまたはファーム RDSH 仮想マシン内の Horizon Agent	9427	TCP	CDR とマルチ メディア リダイレクト (MMR) トラフィックでは省略できます。
Unified Access Gateway	デスクトップまたはファーム RDSH 仮想マシン内の Horizon Agent	32111	TCP	USB リダイレクト トラフィックでは省略できます。
Unified Access Gateway	time.google.com	123	UDP	NTP サービス
Unified Access Gateway	*.blob.core.windows.net *.blob.storage.azure.net	443	TCP	Azure BLOB ストレージへのプログラム アクセス、および必要に応じて Unified Access Gateway ログをアップロードするために使用されます。

App Volumes のポートとプロトコル

Microsoft Azure の Horizon Cloud Service で使用する App Volumes 機能をサポートするには、テナント（デスクトップ）サブネットへの TCP プロトコル トラフィック用にポート 445 を構成する必要があります。ポート 445 は、Microsoft Windows の SMB ファイル共有にアクセスするための標準の SMB ポートです。AppStack は、ポッド マネージャ仮想マシンと同じリソース グループにある SMB ファイル共有に保存されます。

表 2-7. App Volumes のポート要件

ソース	ターゲット	ポート	プロトコル	目的
ベースのインポートされた仮想マシン、ゴールド イメージ、デスクトップ仮想マシン、ファーム RDSH 仮想マシンの App Volumes Agent	*.file.core.windows.net	445	TCP	VDI マシン上の App Volumes アプリケーションの仮想化と VDI マシン上のアプリケーション パッケージのキャプチャは、ファイル共有へのアクセスに依存します。

VDI ポートおよびプロトコルの要件

次の表に、環境で構成されたデスクトップ（VDI またはテナント）サブネットに必要なポートとプロトコルを示します。

表 2-8. VDI ポートおよびプロトコルの要件

ソース	ターゲット	ポート	プロトコル	目的
デスクトップ（テナント）サブネット	*.horizon.vmware.com	443	TCP MQTT	エージェント関連の操作（たとえば、仮想マシン ハブを使用した証明書の署名や更新など）用。現在の具体的なエンドポイントは次のとおりです。 US： ■ cloud-sg-us-r-westus2.horizon.vmware.com ■ cloud-sg-us-r-westus2-mqtt.horizon.vmware.com ■ cloud-sg-us-r-eastus2.horizon.vmware.com ■ cloud-sg-us-r-eastus2-mqtt.horizon.vmware.com EU： ■ cloud-sg-eu-r-northeurope.horizon.vmware.com ■ cloud-sg-eu-r-northeurope-mqtt.horizon.vmware.com ■ cloud-sg-eu-r-germanywestcentral.horizon.vmware.com ■ cloud-sg-eu-r-germanywestcentral-mqtt.horizon.vmware.com JP： ■ cloud-sg-jp-r-japaneast.horizon.vmware.com ■ cloud-sg-jp-r-japaneast-mqtt.horizon.vmware.com
デスクトップ（テナント）サブネット	ドメイン コントローラ	88	TCP UDP	Kerberos サービス。ターゲットは、Active Directory 構成内のドメイン コントローラのロールが含まれているサーバです。Active Directory への Edge の登録が必要です。

表 2-8. VDI ポートおよびプロトコルの要件 （続き）

ソース	ターゲット	ポート	プロトコル	目的
デスクトップ（テナント）サブネット	ドメイン コントローラ	Kerberos：88 LDAP：389、3268 LDAPS：636、3269	TCP UDP	これらのポートは、仮想マシンからドメイン コントローラへの接続のための LDAP または LDAPS サービスに必要です。VDI がドメイン コントローラにアクセスできない場合、セッションを起動できません。
デスクトップ（テナント）サブネット	DNS サーバ	53 および 853	TCP UDP	DNS サービス
デスクトップ（テナント）サブネット	NTP サーバ	123	UDP	NTP サービス
デスクトップ（テナント）サブネット	*.blob.core.windows.net	443	TCP	DCT ログ バンドルのアップロード。顧客管理者が要求の処理後に任意の仮想マシンの DCT ログ収集をクリックすると、バンドルが VDI から BLOB にアップロードされ、そのバンドルが Horizon Universal Console からダウンロードできるようになります。
デスクトップ（テナント）サブネット	Horizon Edge	31883	TCP MQTT UDP	仮想マシンで実行されている Horizon Agent から Edge で実行されている MQTT へ。
デスクトップ（テナント）サブネット	Horizon Edge	32443	TCP	Microsoft Azure Edge の形式が Edge Gateway (VM) の場合のシングル サインオン。
デスクトップ（テナント）サブネット	Horizon Edge	443	TCP	Microsoft Azure Edge の形式が Edge Gateway (AKS) の場合のシングル サインオン。
デスクトップ（テナント）サブネットと管理サブネット	softwareupdate.vmware.com	443	TCP	VMware ソフトウェア パッケージ サーバ。システムのイメージに関連する操作および自動化されたエージェント更新プロセスで使用されているエージェントに関連するソフトウェアの更新をダウンロードするために使用します。
デスクトップ（テナント）サブネット	プライベート リンク エンドポイント	443	TCP	クラウド制御プレーンの接続サービスへのデスクトップ接続。
デスクトップ（テナント）サブネットと管理サブネット	AD 証明書サービス	135、445 および 49152 ～ 65535 の範囲内のポート	RPC/TCP	デスクトップをドメインに追加する。

エンドユーザーの接続トラフィックのポートとプロトコルの要件

エンド ユーザーが Horizon Edge 仮想アプライアンス で使用する可能性のあるさまざまな Horizon Client の詳細については、https://docs.vmware.com/jp/VMware-Horizon-Client/index.html にある Horizon Client のドキュメント ページを参照してください。エンド ユーザーの接続によるトラフィックで、仮想デスクトップおよびリモート アプリケーションにアクセスするためにどのポートが開かれていなければならないかは、エンド ユーザーが接続する方法に関する選択内容によって異なります。

表 2-9. エンドユーザーの接続トラフィックのポートとプロトコル

ソース	ターゲット	ポート	プロトコル	目的
Horizon Client	これらの Unified Access Gateway インスタンスの Microsoft Azure ロード バランサ	443	TCP	CDR、MMR、USB リダイレクト、およびトンネリングされた RDP トラフィックを伝送します。 SSL（HTTPS アクセス）は、デフォルトでクライアント接続に対して有効にされています。ポート 80（HTTP アクセス）は、いくつかの場合に使用できます。
Horizon Client	これらの Unified Access Gateway インスタンスの Microsoft Azure ロード バランサ	8443 または 443	TCP	Horizon Client からのデータ トラフィック用の Unified Access Gateway 上の Blast Secure Gateway 経由の Blast Extreme。
Horizon Client	これらの Unified Access Gateway インスタンスの Microsoft Azure ロード バランサ	443	UDP	データ トラフィック用の Unified Access Gateway 経由の Blast Extreme。
Horizon Client	これらの Unified Access Gateway インスタンスの Microsoft Azure ロード バランサ	8443	UDP	データ トラフィック用の Unified Access Gateway 上の Blast Secure Gateway 経由の Blast Extreme（アダプティブ トランスポート）。
ブラウザ	これらの Unified Access Gateway インスタンスの Microsoft Azure ロード バランサ	443	TCP	CDR、MMR、USB リダイレクト、およびトンネリングされた RDP トラフィックを伝送します。 SSL（HTTPS アクセス）は、デフォルトでクライアント接続に対して有効にされています。ポート 80（HTTP アクセス）は、いくつかの場合に使用できます。

表 2-9. エンドユーザーの接続トラフィックのポートとプロトコル （続き）

ソース	ターゲット	ポート	プロトコル	目的
ブラウザ	これらの Unified Access Gateway インスタンスの Microsoft Azure ロード バランサ	8443 または 443	TCP	Horizon HTML Access クライアント（Web クライアント）からのデータ トラフィック用の Unified Access Gateway 上の Blast Secure Gateway 経由の Blast Extreme。
Horizon Client/ブラウザ	*.horizon.vmware.com	443	TCP	ログインして起動アイテムを一覧表示した後、ユーザーがクリックしてデスクトップを起動すると、Unified Access Gateway へのプロトコル トラフィックのリダイレクトは、オンボーディング時に選択したユーザーの組織の場所に基づいて、これらの URL のいずれかから実行されます。現在の具体的なエンドポイントは次のとおりです。 ■ cloud-sg-us-r-westus2.horizon.vmware.com ■ cloud-sg-us-r-eastus2.horizon.vmware.com ■ cloud-sg-eu-r-northeurope.horizon.vmware.com ■ cloud-sg-eu-r-germanywestcentral.horizon.vmware.com ■ cloud-sg-jp-r-japaneast.horizon.vmware.com

Microsoft Windows オペレーティング システムのライセンスの取得

Microsoft Azure へのデプロイの場合は、Horizon Cloud Service - next-gen 環境で使用する Windows ベースのデスクトップ仮想マシンとリモート デスクトップ セッション ホスト (RDSH) 仮想マシンを作成、ワークフロー実行、および操作する資格を付与する有効な Microsoft ライセンスを取得します。

Horizon Cloud は、Horizon Cloud ワークフローで使用する Microsoft Windows オペレーティング システムのゲスト OS ライセンスを必要としません。

Microsoft ライセンスを取得するには、Windows Server の Microsoft Azure Hybrid Benefit ライセンスに関する Microsoft のドキュメントを参照してください。

VMware は、ソフトウェア アシュアランスを備えた RDS Client Access License (CAL) を適用します。

Microsoft Azure 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にする

Horizon Edge 環境を作成し、Horizon Cloud Service - next-gen 環境にアプライアンス モジュールをインストールまたは更新するには、それぞれのポートで適切な URL を許可する必要があります。

次の表に記載された目的は、Horizon Edge 環境のコンテキストを想定しています。

管理サブネットの URL を許可し、URL アクセスを確認する

サイトの場所とニーズに応じて適切な URL およびワイルドカード サブドメインを許可するには、次のタスクを実行します。

- 次の表の URL およびワイルドカード サブドメインを許可します。たとえば、ファイアウォールおよびネットワーク セキュリティ グループの許可リストに URL とワイルドカード サブドメインを追加します。

- 次のように SSL ディープ パケット インスペクションをバイパスします。
  - 次の表の URL およびワイルドカード サブドメインのファイアウォール。
  - プロキシ サーバ（該当する場合）。

    Horizon Edge Gateway がプロキシ サーバを介して Horizon Agent に接続されている場合は、次の表の URL とワイルドカード サブドメインに対してプロキシ サーバの SSL ディープ パケット インスペクションをバイパスします。

ターゲット (DNS 名)	ポート	プロトコル	プロキシ トラフィック（デプロイで構成されている場合）	目的
*.blob.core.windows.net	443	TCP	はい	Azure Blob Storage へのプログラム アクセス、および必要に応じて Horizon Edge ログをアップロードするために使用されます。 Docker イメージをダウンロードして、監視、SSO、UAG の更新などに役立つ必要な Horizon Edge モジュールを作成するために使用されます。
horizonedgeprod.azurecr.io	443	TCP	はい	Docker イメージをダウンロードして、監視、SSO、UAG の更新などに役立つ必要な Horizon Edge モジュールを作成する際の認証に使用されます。
*.azure-devices.net、またはテナント アカウントに適用されるリージョン別制御プレーンに対応した、以下のリージョン固有の名前のいずれか。 北米： ■ edgehubprodna.azure-devices.net ヨーロッパ： ■ edgehubprodeu.azure-devices.net 日本： ■ edgehubprodjp.azure-devices.net	443 / TCP	TCP	はい	アプライアンスを Horizon Cloud 制御プレーンに接続し、アプライアンスのモジュールの構成をダウンロードし、アプライアンスのモジュールのランタイム ステータスを更新するために使用されます。
vmwareprod.wavefront.com	443	TCP	はい	Tanzu Observability by Wavefront に操作メトリックを送信するために使用されます。VMware のオペレータは、お客様をサポートするためのデータを受け取ります。 Tanzu Observability はストリーミング分析プラットフォームです。データを Tanzu Observability に送信し、カスタム ダッシュボードでデータを表示および操作できます。Tanzu Observability by Wavefront のドキュメントを参照してください。

ターゲット (DNS 名)	ポート	プロトコル	プロキシ トラフィック（デプロイで構成されている場合）	目的
*.data.vmwservices.com、またはテナント アカウントに適用されるリージョン別 Workspace ONE Intelligence ターゲットに対応した、以下のリージョン固有の名前のいずれか。 ■ eventproxy.na1.data.vmwservices.com ■ eventproxy.eu1.data.vmwservices.com ■ eventproxy.eu2.data.vmwservices.com ■ eventproxy.uk1.data.vmwservices.com ■ eventproxy.ca1.data.vmwservices.com ■ eventproxy.ap1.data.vmwservices.com ■ eventproxy.au1.data.vmwservices.com ■ eventproxy.in1.data.vmwservices.com	443	TCP	はい	イベントまたはメトリックを Workspace ONE Intelligence に送信するために使用されます。 Workspace ONE Intelligence を参照してください。
ファイアウォールまたはネットワーク セキュリティ グループ (NSG) でサービス タグの使用がサポートされている場合は、Azure サービス タグ `AzureCloud` を適用します。ファイアウォールまたは NSG がサービス タグの使用をサポートしていない場合は、ホスト名 `monitor.horizon.vmware.com` を使用します。	1514 および 1515	TCP	いいえ	システム監視に使用されます。
azcopyvnext.azureedge.net	443	TCP	はい	トラブルシューティングの目的で Azure Blob Storage にデプロイ ログをアップロードするために使用されます。
■ management.azure.com ■ login.microsoftonline.com ■ mcr.microsoft.com ■ *.data.mcr.microsoft.com ■ packages.microsoft.com ■ acs-mirror.azureedge.net	443	HTTPS	はい	Horizon Edge Gateway の Microsoft コンポーネントにパッチを適用するために使用されます。
time.google.com	123	UDP	はい	時間の同期のために使用されます。
■ security.ubuntu.com ■ azure.archive.ubuntu.com ■ changelogs.ubuntu.com ■ motd.ubuntu.com	80	HTTP	はい	Ubuntu コンポーネントのパッチ適用に使用されます。

ターゲット (DNS 名)	ポート	プロトコル	プロキシ トラフィック（デプロイで構成されている場合）	目的
*.file.core.windows.net	445	TCP	いいえ	パッケージをインポートし、ファイル共有間でパッケージをレプリケートするワークフロー用にプロビジョニングされたファイル共有へのアクセス。
softwareupdate.vmware.com	443	TCP	はい	ソフトウェア パッケージ サーバ。システムのイメージに関連する操作および自動化されたエージェント更新プロセスで使用されているエージェントに関連するソフトウェアの更新をダウンロードするために使用します。

管理サブネットの URL がアクセス可能であるかを判断する

Horizon Cloud Service - next-gen Edge サブネット URL チェッカー ツールは、「[ユーティリティ] ページ」の TechZone で使用できます。関連情報は、Techzone ページ「Horizon 8 環境向け Horizon Edge Gateway のデプロイ」で確認できます。

このツールは、`.exe` ファイルとして提供されます。Horizon Edge が存在するネットワーク上の Windows 10 ベース以降の仮想マシンで Horizon Cloud Service - next-gen の Edge サブネット URL チェッカー ツールをダウンロードして使用するには、次の手順を実行します。

1 Horizon Cloud Service - next-gen Edge サブネット URL チェッカーを、Horizon Edge ネットワークにデプロイされた Windows 仮想マシンにダウンロードします。

2 ファイルをダブルクリックして実行ファイルを実行します。

ダイアログ ボックスが表示されます。

3 [はい] をクリックします。

4 出力フォルダを `C:/VMwareURLCheckerOutput/` で開きます。

このフォルダには、各リージョン別の制御プレーンの出力ファイルが含まれています。

5 Horizon Edge をデプロイするリージョンの出力ファイルを開き、必要な URL にアクセスできるかどうかを判断します。

次の詳細が当てはまります。

- ファイルには、管理サブネットのために必要な URL のステータスが表示されます。
- 各 URL の想定されるステータスは、アクセス可能です。
- URL のステータスが「到達不能」の場合は、エラー メッセージを確認し、問題のブロックを解除するために必要な変更を加えます。

6 目的のリージョン内の全ドメインのステータスがアクセス可能になるまで、必要に応じて実行ファイルを再実行します。

テナント（デスクトップ）サブネットの URL の許可 - グローバル 仮想マシン ハブ DNS ホスト名

グローバル 仮想マシン ハブ インスタンスを使用することがサイトのニーズに合っている場合、Horizon Edge Gateway をデプロイするときに、次の URL とその設定を許可します。

ターゲット (DNS 名)	ポート	プロトコル	目的
*.horizon.vmware.com	443	TCP	エージェント関連の操作（たとえば、仮想マシン ハブ を使用した証明書の署名や更新など）用。

テナント（デスクトップ）サブネットの URL の許可 - リージョン別の 仮想マシン ハブ DNS ホスト名

リージョン別の 仮想マシン ハブ インスタンスを使用することがサイトのニーズに合っている場合、指定されたリージョンに Horizon Edge Gateway をデプロイするときに、指定された 2 つの対応する URL を使用します。

各リージョンの 仮想マシン ハブ インスタンスのポート、プロトコル、および目的は、グローバル 仮想マシン ハブ インスタンスと一致します。

ポート	443
プロトコル	TCP
目的	エージェント関連の操作（たとえば、仮想マシン ハブ を使用した証明書の署名や更新など）用。

次の Azure リージョンの場合	次のターゲット（DNS 名）URL を許可
■ westus2 ■ westus ■ westus3 ■ westcentralus ■ centralus	■ cloud-sg-us-r-westus2.horizon.vmware.com ■ cloud-sg-us-r-westus2-mqtt.horizon.vmware.com
■ eastus2 ■ eastus ■ southcentralus ■ northcentralus ■ canadacentral ■ canadaeast ■ brazilsouth ■ brazilsoutheast ■ usgovvirginia	■ cloud-sg-us-r-eastus2.horizon.vmware.com ■ cloud-sg-us-r-eastus2-mqtt.horizon.vmware.com

次の Azure リージョンの場合	次のターゲット（DNS 名）URL を許可
■ northeurope ■ norwaywest ■ norwayeast ■ uaecentral ■ uaenorth ■ uksouth ■ ukwest ■ westeurope	■ cloud-sg-eu-r-northeurope.horizon.vmware.com ■ cloud-sg-eu-r-northeurope-mqtt.horizon.vmware.com
■ germanywestcentral ■ germanynorth ■ swedencentral ■ swedensouth ■ francecentral ■ francesouth ■ switzerlandnorth ■ switzerlandwest	■ cloud-sg-eu-r-germanywestcentral.horizon.vmware.com ■ cloud-sg-eu-r-germanywestcentral-mqtt.horizon.vmware.com
■ japanwest ■ japaneast	■ cloud-sg-jp-r-japaneast.horizon.vmware.com ■ cloud-sg-jp-r-japaneast-mqtt.horizon.vmware.com
■ australiaeast ■ australiacentral ■ australiacentral2 ■ australiasoutheast	■ cloud-sg-jp-r-australiaeast.horizon.vmware.com ■ cloud-sg-jp-r-australiaeast-mqtt.horizon.vmware.com
■ centralindia ■ jioindiawest ■ jioindiacentral ■ southindia ■ westindia	■ cloud-sg-jp-r-centralindia.horizon.vmware.com ■ cloud-sg-jp-r-centralindia-mqtt.horizon.vmware.com

プロキシの有効化の URL を許可する

プロキシ サーバを使用して環境からのトラフィック フローを制御する場合は、必要なポートを開き、Horizon Edge Gateway がプロキシ サーバにアクセスできるようにします。Microsoft Azure Edge の形式が Edge Gateway (AKS) の場合は、「Azure Kubernetes サービス (AKS) クラスタの送信ネットワークと FQDN ルール」を参照してください。

Microsoft Azure 仮想マシン モデルの可用性の確認

Microsoft Azure Edge に十分な Microsoft Azure キャパシティがあることを確認するには、Microsoft Azure 仮想マシン モデルの可用性をテストし、リージョンの CPU 出力を確認します。

次の手順は、Microsoft Azure のキャパシティの要件で推奨されます。この手順には、コマンドと出力の例が含まれています。コマンドは、特定のリージョンのすべてのアベイラビリティ ゾーン (1、2、3) にわたる Horizon Edge Gateway に使用される Microsoft Azure 仮想マシン モデルの可用性をテストします。

手順

1 次の一般的な例とその後の特定の例に示すように、コマンドを実行して、マシン タイプ（Standard_D2 など）のリージョン SKU 制限を取得します。

```
az vm list-skus --location <azure_region_where_edge_is_being_deployed> --size Standard_D2
--all --output table
```

次のコード例は、location westeurope のリージョン制限に対する特定のテストです。

```
az vm list-skus --location westeurope --size Standard_D2 --all --output table
```

上記のコマンドの出力例を次に示します。最初の例は、制限がないことを示す成功した結果です。2 番目の例は、既存の制限を示す失敗した結果です。

成功した結果の出力 - 制限はありません

```
ResourceType     Locations    Name                 Zones    Restrictions
---------------  -----------  -------------------  -------  --------------
virtualMachines  westeurope   Standard_D2_v3       1,2,3    None
```

失敗した結果の出力 - 制限があります

```
ResourceType     Locations    Name                 Zones    Restrictions
---------------  -----------  -------------------  -------  --------------
virtualMachines  westeurope   Standard_D2          1,2,3    'NotAvailableForSubscription,
type: Zone, locations: westeurope, zones: 1,2,3']
```

2 次の一般的な例とその後の特定の例に示すように、コマンドを実行して、リージョン CPU 制限の合計を取得します。

```
az vm list-usage --location <azure_region_where_edge_is_being_deployed> -o table
```

次のコード例は、location westeurope の CPU リージョン制限の合計に対する特定のテストです。

```
az vm list-usage --location westeurope -o table
```

上記のコマンドの出力例を次に示します。最初の例は、Total Regional vCPUs の CurrentValue が 25 以上（この場合は 26）であり、制限がないことを示す成功した結果です。2 番目の例は、Total Regional vCPUs の Limit が 25 未満（この場合は 10）であり、制限があることを示す失敗した結果です。

成功した結果の出力 - 制限はありません

```
Name                                  CurrentValue    Limit
------------------------------------  --------------  -------
Availability Sets                     1               2500
Total Regional vCPUs                  26              310
```

```
Virtual Machines                          11              25000
Virtual Machine Scale Sets                1               2500
Dedicated vCPUs                           0               3000
Cloud Services                            0               2500
```

失敗した結果の出力 - 制限があります

```
Name                                      CurrentValue    Limit
----------------------------------------  --------------  -------
Availability Sets                         0               2500
Total Regional vCPUs                      0               10
Virtual Machines                          0               25000
Virtual Machine Scale Sets                0               2500
Dedicated vCPUs                           0               3000
Cloud Services                            0               2500
```

次のステップ

- ベスト プラクティスとして、Horizon Edge Gateway をデプロイする予定のリージョンで、Microsoft Azure が SKU を使用可能にするよう要求します。
- Microsoft Azure のキャパシティの要件に戻ります。

。

Microsoft Azure サブスクリプションのサービス プリンシパルの作成

Horizon Cloud Service on Microsoft Azure のデプロイの場合、サービスは API 呼び出しを使用してリソースを Microsoft Azure サブスクリプションにデプロイし、それらのリソースを管理します。Microsoft Azure サブスクリプションで API 呼び出しを使用する機能を Horizon Cloud に提供するには、Microsoft Entra ID にアプリケーション登録と呼ばれるサービス プリンシパルを作成します。

プロバイダに対して最大 4 つの一意のサービス プリンシパルを作成します。合計 5,000 台の仮想マシンをサポートするには、4 つのサービス プリンシパルを追加します。複数のサービス プリンシパルがある場合、それらはサブスクリプション ID とディレクトリ ID を共有しますが、各サービス プリンシパルには独自のアプリケーション ID があります。

重要： 各サービス プリンシパルに同じロールを使用します。

Horizon Cloud のために Microsoft Azure サブスクリプションのキャパシティにアクセスして使用するには、サービス プリンシパルを作成します。Microsoft Azure サブスクリプション ID、ディレクトリ ID、およびアプリケーション ID とキーは、Horizon Cloud で使用されます。

注： Microsoft Azure ポータルでこのセクションのタスクを実行します。構成の詳細については、Microsoft のドキュメントのリソースにアクセスできる Azure AD アプリケーションとサービス プリンシパルをポータルで作成するを参照してください。Microsoft はサービス プリンシパルに証明書ベースの認証を使用することを推奨していますが、VMware はサービス プリンシパルにキー/シークレット ベースの認証を要求します。

Horizon Cloud サービス プリンシパルには、サブスクリプションに割り当てられたロールが必要です。通常、Horizon Cloud はサブスクリプションに組み込みの `Contributor` ロールを使用します。

`Contributor` ロールを使用するのは、Horizon Cloud がサブスクリプション内で実行する必要があるすべての API 呼び出しをカバーするためです。ロールの割り当ては直接割り当てである必要があります。ロールのグループベースの割り当ての使用（ロールがグループに割り当てられ、サービス プリンシパルがそのグループのメンバーとなる）は、サポートされていません。

組織がサブスクリプションで `Contributor` ロールの使用を避けたい場合は、Horizon Cloud は代わりにカスタム ロールの使用をサポートします。使用する場合、カスタム ロールは、Horizon Cloud が使用する必要がある特定の API 呼び出しを提供する必要があります。詳細については、Horizon Cloud アプリケーション登録にカスタム ロールを使用するを参照してください。

注： Microsoft Entra ID に参加しているプールまたは仮想マシンを削除する場合、サービス プリンシパルには Microsoft Entra ID からデバイス エントリを削除する権限が必要です。

権限は次のとおりです。

範囲：`https://graph.microsoft.com/`

権限：`Device.ReadWrite.All Read and write devices`

管理者の同意：`Yes`

権限を付与するには、次の場所に移動します。

[サブスクリプション] - [Azure Active Directory] - [アプリケーションの登録] - [権限を付与する必要があるアプリケーションを選択] - [API 権限] - [Microsoft GRAPH を選択] - [Device.ReadWriteAll を選択]

次の手順では、Horizon Cloud 環境で使用する設定を示します。

手順

- サブスクリプションに最大 4 つのサービス プリンシパルとクライアント シークレットを構成します。
  a クライアント シークレットの有効期間を、`24 Months` など適切な長さに設定します。
  b 後で参照できるように、クライアント シークレットのコピーを保存します。
  c 各サービス プリンシパルに適切なロールを割り当て、サービス プリンシパルがサブスクリプション内のリソースを管理できるようにします。

次のステップ

必要なリソース プロバイダを登録します。必要なリソース プロバイダが Microsoft Azure サブスクリプションに登録されていることの確認を参照してください。

必要なリソース プロバイダが Microsoft Azure サブスクリプションに登録されていることの確認

Horizon Cloud Service - next-gen の Microsoft Azure サブスクリプションでは、いくつかのリソース プロバイダのステータスが登録済みである必要があります。

Horizon Edge をデプロイする前に、リストされたリソース プロバイダのステータスが登録済みであることを確認してください。Horizon Edge デプロイの最後の手順では、これらのリソース プロバイダのステータスが登録済みであることを検証し、登録解除されている場合は Horizon Edge のデプロイを開始できないようにします。

リソース プロバイダには、ステータスが登録済みのものとそうでないものがあることに注意してください。ステータスにそのような違いがあるのは、標準の Microsoft Azure の動作の結果であり、リソース プロバイダのセットがすべての Microsoft Azure サブスクリプションに対して登録されます。

次の必須リソース プロバイダが Microsoft Azure サブスクリプションに登録されている必要があります。

- Microsoft.Authorization
- Microsoft.Compute
- Microsoft.ContainerService
- Microsoft.KeyVault
- Microsoft.MarketplaceOrdering
- Microsoft.ResourceGraph
- Microsoft.Network
- Microsoft.Resources
- Microsoft.Security
- Microsoft.Storage
- Microsoft.ManagedIdentity

次の手順を使用して、上記のリソース プロバイダが Microsoft Azure サブスクリプションに登録されていることを確認します。

1 Microsoft Azure ポータルにログインし、Horizon Edge インスタンスのデプロイ先となるサブスクリプションを検索します。

2 サブスクリプション名をクリックし、[リソース プロバイダ] メニュー項目が表示されるまで下にスクロールします。

3 上記のリソース プロバイダを探し、それぞれ [登録済み] ステータスにチェック マークが付いていることを確認します。

   Microsoft Azure ポータルを使用して、上記のリストから、ステータスが [未登録] のリソース プロバイダを登録します。

Horizon Cloud アプリケーション登録にカスタム ロールを使用する

`Contributor` ロールは通常、Horizon Cloud アプリケーション登録プロセスを有効にして Microsoft Azure サブスクリプションで API 呼び出しを行うために使用されます。`Contributor` ロールの使用を回避する場合は、その目的のためにカスタム ロールを作成できます。カスタム ロールには必須の権限とオプションの権限があり、サービス プリンシパルを作成するときに認識しておく必要があるます。

カスタム ロールを作成するには、Azure PowerShell や Azure CLI などのツールを使用し、少なくともこのトピックに記載されている必須の権限を含むカスタム ロール定義を作成します。以降の JSON の例を参照してください。このページに記載されている特定の Microsoft Azure 権限の詳細については、Azure リソース プロバイダの操作を参照してください。

必須の権限

表 2-10. サブスクリプション レベルで権限を割り当てるときに、カスタム ロールで許可する必要がある Microsoft Azure リソースの操作

操作
Microsoft.Authorization/*/read
Microsoft.Compute/*/read
Microsoft.Compute/availabilitySets/*
Microsoft.Compute/disks/*
Microsoft.Compute/galleries/read Microsoft.Compute/galleries/write Microsoft.Compute/galleries/delete Microsoft.Compute/galleries/images/* Microsoft.Compute/galleries/images/versions/*
Microsoft.Compute/images/*
Microsoft.Compute/locations/*
Microsoft.Compute/snapshots/*
Microsoft.Compute/virtualMachines/*
Microsoft.Compute/virtualMachineScaleSets/*
Microsoft.ContainerService/managedClusters/delete
Microsoft.ContainerService/managedClusters/read
Microsoft.ContainerService/managedClusters/write
Microsoft.ContainerService/managedClusters/commandResults/read
Microsoft.ContainerService/managedClusters/runcommand/action
Microsoft.ContainerService/managedClusters/upgradeProfiles/read
Microsoft.ManagedIdentity/userAssignedIdentities/*/assign/action
Microsoft.ManagedIdentity/userAssignedIdentities/*/read
Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write
Microsoft.Network/loadBalancers/*
Microsoft.Network/networkInterfaces/*
Microsoft.Network/networkSecurityGroups/*
Microsoft.Network/virtualNetworks/read

表 2-10. サブスクリプション レベルで権限を割り当てるときに、カスタム ロールで許可する必要がある Microsoft Azure リソースの操作（続き）

操作
Microsoft.Network/virtualNetworks/write
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read
Microsoft.Network/virtualNetworks/subnets/*
Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read
Microsoft.ResourceGraph/*
Microsoft.Resources/deployments/*
Microsoft.Resources/subscriptions/read
Microsoft.Resources/subscriptions/resourceGroups/*
Microsoft.ResourceHealth/availabilityStatuses/read
Microsoft.Storage/*/read
Microsoft.Storage/storageAccounts/*

App Volumes を使用する場合は、表に記載されている権限がサブスクリプション レベルで構成されていることを確認します。これらの権限の詳細については、「App Volumes アプリケーション ストレージ アカウントの Azure プライベート エンドポイント」を参照してください。

操作
Microsoft.Network/locations/availablePrivateEndpointTypes/read
Microsoft.Network/privateEndpoints/read
Microsoft.Network/privateEndpoints/write
Microsoft.Network/privateEndpoints/delete
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/subnets/read
Microsoft.Network/virtualNetworks/subnets/write
Microsoft.Network/virtualNetworks/subnets/join/action
Microsoft.Resources/deployments/*
Microsoft.Resources/subscriptions/read
Microsoft.Resources/subscriptions/resourceGroups/read

オプションの権限

Microsoft Azure に Horizon Edge をデプロイする場合、次の権限は必須ではありません。ただし、これらのオプションの権限を含めない場合、それらに依存する Horizon Universal Console の機能は機能しません。

表 2-11. サブスクリプション レベルで権限を割り当てるときに、カスタム ロールでオプションで実行できる Microsoft Azure リソースの操作

操作	

`Microsoft.KeyVault/*/read`
`Microsoft.KeyVault/vaults/*`
`Microsoft.KeyVault/vaults/secrets/*`
	プール仮想マシンのディスク暗号化には、キー コンテナの権限が必要です。

`Microsoft.Network/natGateways/join/action`	この権限は、Horizon Edge の作成時に [Azure Private Link] 接続タイプが選択され、管理サブネットに NAT ゲートウェイが関連付けられている場合に必要です。この権限は、プライベート エンドポイント リソースを作成するために必要です。
`Microsoft.Network/natGateways/read`	この権限は、クラスタ送信タイプが Horizon Edge の NAT ゲートウェイとして選択されているときに、管理サブネットの NAT ゲートウェイが存在している場合に正しく構成されていることを検証するために必要です。
`Microsoft.Network/privateEndpoints/write` `Microsoft.Network/privateEndpoints/read`	Azure Private Link を使用して Horizon Edge をデプロイするには、プライベート エンドポイント権限が必要です。

表 2-11. サブスクリプション レベルで権限を割り当てるときに、カスタム ロールでオプションで実行できる Microsoft Azure リソースの操作（続き）

操作	
Microsoft.Network/publicIPAddresses/*	パブリック IP アドレスを持つロード バランサの背後に Unified Access Gateway インスタンスを含む Horizon Edge インスタンスをデプロイするには、パブリック IP アドレスの権限が必要です。また、イメージをデプロイし、イメージにパブリック IP アドレス追加するには、この権限は必須です。
Microsoft.Network/routeTables/join/action	この権限は、Horizon Edge の作成時に [Azure Private Link] 接続タイプが選択され、管理サブネットにルート テーブルが接続されている場合に必要です。この権限は、プライベート エンドポイント リソースを作成するために必要です。
Microsoft.Network/routeTables/read	この権限は、Horizon Edge のために選択されたクラスタ送信タイプがユーザー定義ルートの場合に必要です。デフォルト ルートが正しく構成されていることを確認するには、管理サブネットの関連付けられたルート テーブルを検証することが必要です。

注： Microsoft Entra ID に参加しているプールまたは仮想マシンを削除する場合、サービス プリンシパルには Microsoft Entra ID からデバイス エントリを削除する権限が必要です。

権限は次のとおりです。

範囲：`https://graph.microsoft.com/`

権限：`Device.ReadWrite.All Read and write devices`

管理者の同意：`Yes`

権限を付与するには、次の場所に移動します。

[サブスクリプション] - [Azure Active Directory] - [アプリケーションの登録] - [権限を付与する必要があるアプリケーションを選択] - [API 権限] - [Microsoft GRAPH] - [Device.ReadWriteAll を選択]

Microsoft Azure カスタム ロールの JSON の例

次の JSON コード ブロックは、`Horizon Cloud カスタム ロール – Titan` という名前のカスタム ロール定義に、前述の一連の必須およびオプションの操作がある場合にどのような状態になるかを示す例です。ID は、カスタム ロールの一意の ID です。Azure PowerShell または Azure CLI を使用してカスタム ロールを作成すると、プロセスによってこの ID が自動的に生成されます。変数 *my_subscription_ID* の場合は、カスタム ロールが使用されるサブスクリプションの ID を置き換えます。

`assignableScopes` セクションでは、複数のサブスクリプション ID、「*/subscriptions/my_subscription_ID*」を使用して、複数のサブスクリプションにわたってカスタム ロールを使用できます。

表 2-12. サブスクリプション レベルで権限を割り当てるときに Horizon Cloud が必要とする操作を許可するロールの JSON の例

```
{
    “id”: “uuid”,
    “properties”: {
        “roleName”: “Horizon Cloud Custom Role - Titan”,
        “description”: “All permissions required for deployment and operation of a Horizon
Edge in Azure”,
        “assignableScopes”: [
              “/subscriptions/my_subscription_ID”
        ],
        “permissions”: [
            {
                “actions”: [
                    “Microsoft.Authorization/*/read”,
                    “Microsoft.Compute/*/read”,
                    “Microsoft.Compute/availabilitySets/*“,
                    “Microsoft.Compute/disks/*“,
                    “Microsoft.Compute/galleries/read”,
                    “Microsoft.Compute/galleries/write”,
                    “Microsoft.Compute/galleries/delete”,
                    “Microsoft.Compute/galleries/images/*”,
                    “Microsoft.Compute/galleries/images/versions/*”,
                    “Microsoft.Compute/images/*”,
                    “Microsoft.Compute/locations/*”,
                    “Microsoft.Compute/snapshots/*”,
                    “Microsoft.ContainerService/managedClusters/delete”,
                    “Microsoft.ContainerService/managedClusters/read”,
                    “Microsoft.ContainerService/managedClusters/write”,
                    “Microsoft.ContainerService/managedClusters/commandResults/read”,
                    “Microsoft.ContainerService/managedClusters/runcommand/action”,
                    “Microsoft.ContainerService/managedClusters/upgradeProfiles/read”,
                    “Microsoft.ManagedIdentity/userAssignedIdentities/*/assign/action”,
                    “Microsoft.ManagedIdentity/userAssignedIdentities/*/read”,
                    “Microsoft.Compute/virtualMachines/*”,
                    “Microsoft.Compute/virtualMachineScaleSets/*”,
                    “Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/
agreements/read”,
                    “Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/
agreements/write”,
                    “Microsoft.Network/loadBalancers/*”,
                    “Microsoft.Network/networkInterfaces/*”,
                    “Microsoft.Network/networkSecurityGroups/*”,
                    “Microsoft.Network/virtualNetworks/read”,
                    “Microsoft.Network/virtualNetworks/write”,
                    “Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read”,
                    “Microsoft.Network/virtualNetworks/subnets/*”,
                    “Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read”,
                    “Microsoft.ResourceGraph/*”,
                    “Microsoft.Resources/deployments/*”,
                    “Microsoft.Resources/subscriptions/read”,
                    “Microsoft.Resources/subscriptions/resourceGroups/*”,
                    “Microsoft.ResourceHealth/availabilityStatuses/read”,
                    “Microsoft.Storage/*/read”,
                    “Microsoft.Storage/storageAccounts/*”,
                    “Microsoft.KeyVault/*/read”,
                    “Microsoft.KeyVault/vaults/*”,
                    “Microsoft.KeyVault/vaults/secrets/*”,
                    “Microsoft.Network/natGateways/join/action”,
                    “Microsoft.Network/natGateways/read”,
                    “Microsoft.Network/privateEndpoints/write”,
                    “Microsoft.Network/privateEndpoints/read”,
                    “Microsoft.Network/publicIPAddresses/*”,
                    “Microsoft.Network/routeTables/join/action",
```

表 2-12. サブスクリプション レベルで権限を割り当てるときに Horizon Cloud が必要とする操作を許可するロールの JSON の例

```
                    "Microsoft.Network/routeTables/read"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

Horizon 制御プレーン および Horizon Cloud Service - next-gen での一般的なユースケースとシナリオのプランニング

3

ユーザーを Horizon 制御プレーン および Horizon Cloud Service - next-gen にオンボーディングする準備をするときには、予想されるユースケースとシナリオをサポートするために必要なサイジングを検討してください。

次のトピックを参照してください。

- Horizon Cloud Service - next-gen デプロイのサイジング

Horizon Cloud Service - next-gen デプロイのサイジング

Horizon Cloud Service - next-gen にオンボーディングした後は、構成の上限オンライン ツールを使用して、プロバイダおよび Horizon Edge Gateway ごとにサポートされる仮想マシン、ユーザー、サービス プリンシパルなどの数に基づいて環境のサイズを設定することができます。

Horizon Cloud Service - next-gen 構成の上限ツールの情報は、リストされている各制限の意味を説明します。ただし、次の背景情報は、これらの制限がデプロイのパフォーマンスに与える影響を説明するのに役立ちます。

構成の上限ツールで提供されている適切な Horizon Cloud Service - next-gen 構成の制限に以降の情報を適用します。

- サービス プリンシパルの数がプロビジョニング時間に与える影響

  仮想マシンのライフサイクル管理ワークフローの実行中にデスクトップをプロビジョニングするため、Horizon Cloud Service - next-gen ではいくつかの Microsoft Azure API 呼び出しを発行します。Microsoft Azure API のスロットルは、サービス プリンシパルに基づいています。したがって、サービス プリンシパルの数を増やすと、より多くの API を同時に発行できます。これにより、仮想マシンのライフサイクル管理ワークフローのパフォーマンスが向上します。ワークフローの例には、プールの作成と削除、仮想マシンの一括電源操作などがあります。

- App Volumes 配信ファイル共有がアプリケーションのロード時間に与える影響

  App Volumes アプリケーションは、配信ファイル共有に存在する VHD ファイルをマウントすることによってデスクトップに配信されます。ファイル共有内の同時マウント数が多いほど、セッションまたはデスクトップ内でアプリケーションのプロビジョニングが完了するまでにかかる時間が長くなります。配信ファイル共有の数を増やすと、アプリケーションのプロビジョニング プロセスが向上し、アプリケーションがより早く準備できるようになります。

Horizon Cloud Service - next-gen 管理者のオンボーディング

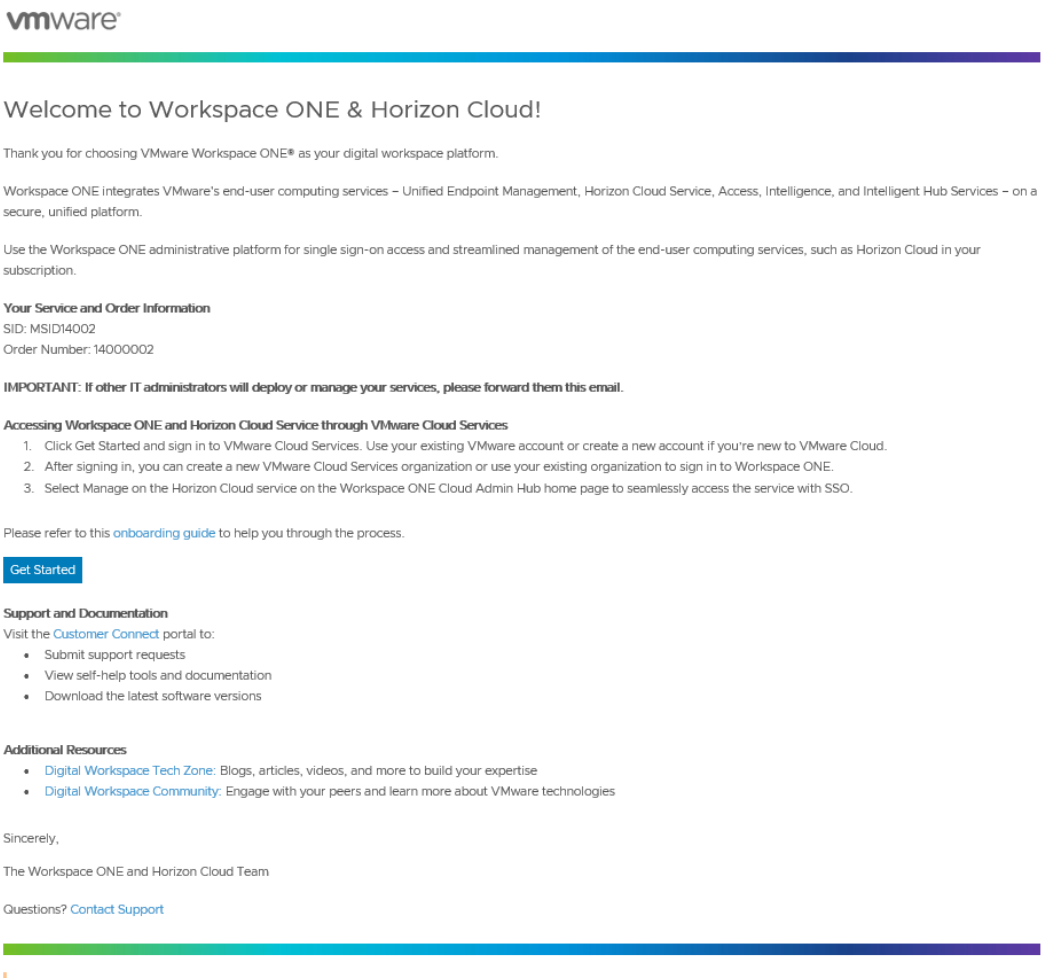
4

管理者は、Horizon Cloud Service - next-gen オンボーディング プロセスを開始および完了するために次の情報を確認してください。

ウェルカム メール

VMware は、管理者アカウントにウェルカム メールを送信して、製品ライセンスの評価または購入を確認します。この E メールは、登録を確認するものであり、Horizon Cloud Service - next-gen へのアクセスと引き換える「[使用開始]」リンクが含まれています。

注： この段階では、Workspace ONE のスタート ガイドの情報が役立ちます。Workspace ONE 製品ドキュメントの『スタート ガイド』を参照してください。



vmware

Welcome to Workspace ONE & Horizon Cloud!

Thank you for choosing VMware Workspace ONE® as your digital workspace platform.

Workspace ONE integrates VMware's end-user computing services – Unified Endpoint Management, Horizon Cloud Service, Access, Intelligence, and Intelligent Hub Services – on a secure, unified platform.

Use the Workspace ONE administrative platform for single sign-on access and streamlined management of the end-user computing services, such as Horizon Cloud in your subscription.

Your Service and Order Information
SID: MSID14002
Order Number: 14000002

IMPORTANT: If other IT administrators will deploy or manage your services, please forward them this email.

Accessing Workspace ONE and Horizon Cloud Service through VMware Cloud Services

1. Click Get Started and sign in to VMware Cloud Services. Use your existing VMware account or create a new account if you're new to VMware Cloud.
2. After signing in, you can create a new VMware Cloud Services organization or use your existing organization to sign in to Workspace ONE.
3. Select Manage on the Horizon Cloud service on the Workspace ONE Cloud Admin Hub home page to seamlessly access the service with SSO.

Please refer to this onboarding guide to help you through the process.

Get Started

Support and Documentation
Visit the Customer Connect portal to:

- Submit support requests
- View self-help tools and documentation
- Download the latest software versions

Additional Resources

- Digital Workspace Tech Zone: Blogs, articles, videos, and more to build your expertise
- Digital Workspace Community: Engage with your peers and learn more about VMware technologies

Sincerely,

The Workspace ONE and Horizon Cloud Team

Questions? Contact Support

Horizon Cloud Service - next-gen は、Anywhere Workspace ソリューション全体の一部です。

Horizon Cloud Service - next-gen の Horizon Cloud ライセンス サービスは、IT 管理者が購入したライセンス タイプに基づいて機能にアクセスして利用できるようにします。

Horizon サブスクリプションのライセンス機能の比較については、「Horizon サブスクリプション比較マトリックス」を参照してください。これは、ライセンスを期間と SaaS に大別します。現在リストされているすべての機能が Horizon Cloud Service - next-gen に適用されるわけではありません。

注： ウェルカム メールには、購入したライセンスのタイプに関する情報は含まれません。このような情報は、自分の Customer Connect アカウントから取得できます。Customer Connect ユーザーになるには、ナレッジベースの記事 KB2007005 を参照してください。

オンボーディング プロセスが完了したら、Horizon のライセンスを Horizon Universal Console から追跡できます。Horizon Universal Console を使用した Horizon ライセンスの追跡を参照してください。

Cloud Services コンソール にログインします。

注： Cloud Services コンソール の詳細については、Cloud Services 製品ドキュメントを参照してください。Cloud Services Platform (CSP) や Cloud Services エンゲージメント プラットフォーム など、VMware Cloud services の他の名前が表示されることがあります。

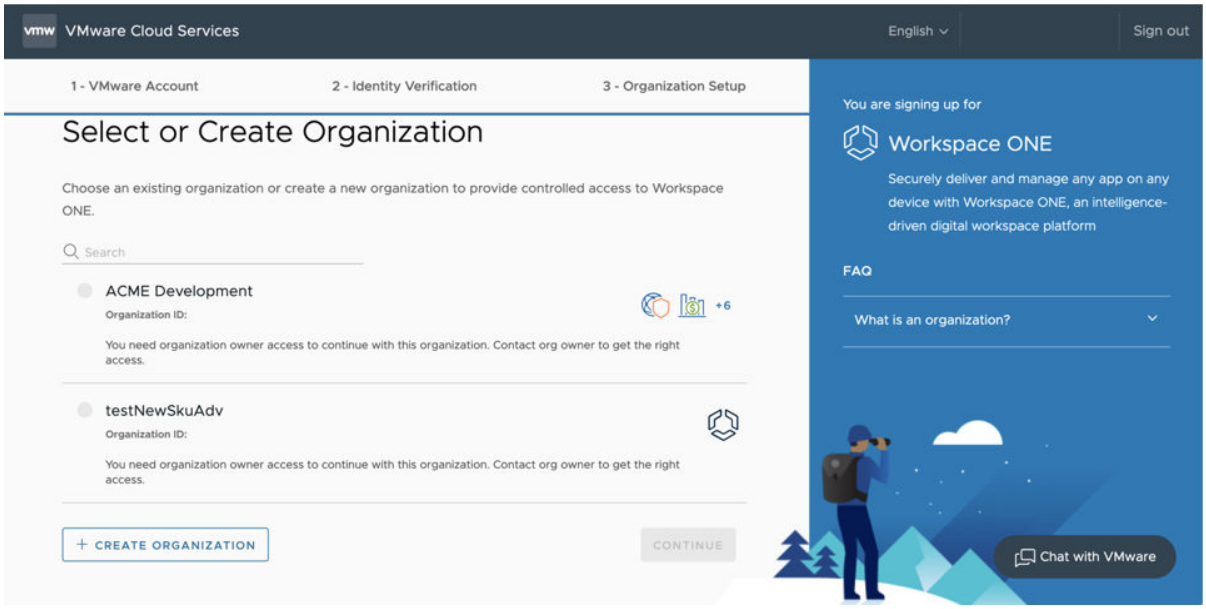
1 新しい Cloud Services コンソール アカウントを作成するか、既存のアカウントを使用します。

新しいアカウントを作成するには、ウェルカム E メール内のリンクをクリックし、VMware Cloud services アカウントを作成し、VMware ID を使用して VMware Cloud services にログインします。

注：

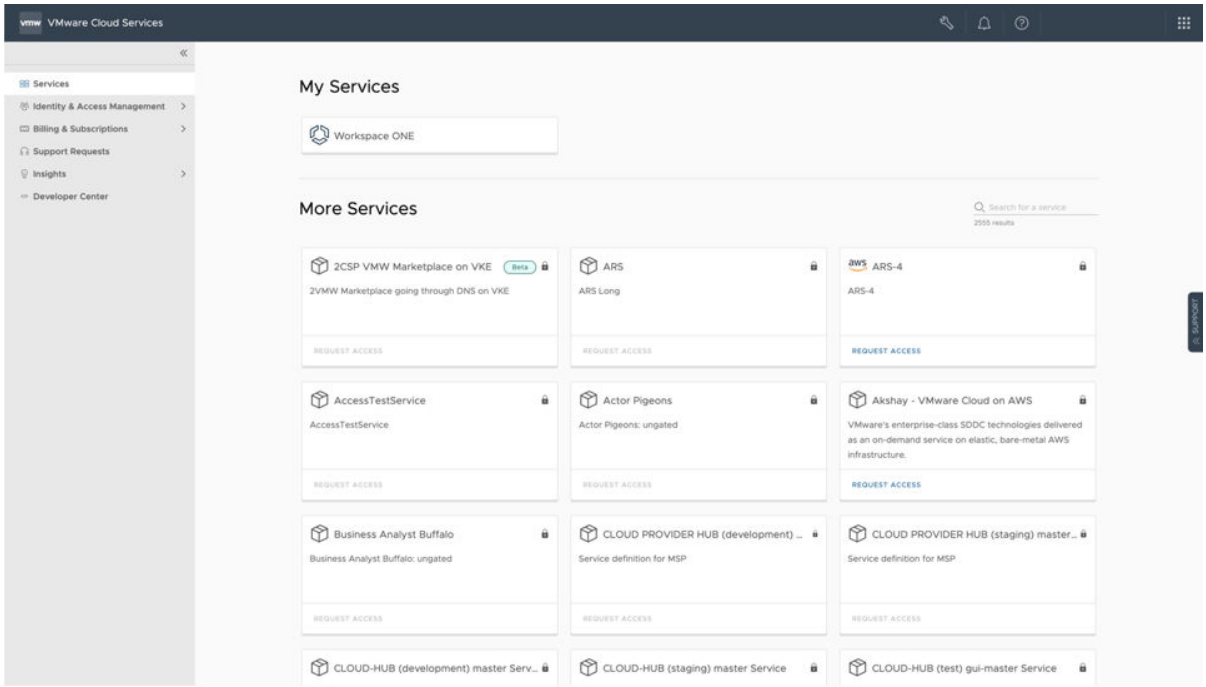
- ウェルカム E メールのリンクを使用して招待を引き換えると、自動的に管理者ロールが割り当てられます。
- 同じ管理者に Horizon Cloud を管理させるときに、Cloud Services で提供されている別の製品にも CSP 組織を使用している場合は、同じ CSP 組織を選択します。
- 既存の CSP 組織があり、同じ管理者に Horizon Cloud でサブスクリプションを管理させないようにする場合は、新しい CSP 組織を作成します。ただし、そうした場合は、今後 CSP 組織を組み合わせることができなくなります。
- すでに Horizon Cloud を管理している既存の CSP 組織があり、新しい地理的リージョンのサブスクリプションを追加している場合は、新しい組織を作成します。

Cloud Services コンソール で [組織のセットアップ] ページが開きます。



2 選択した組織名を入力し、[組織を作成してサインアップを完了する] をクリックします。

Cloud Services コンソール ページが表示され、アクセス権を持つすべてのサービスが表示されます。



3 右上隅の名前をクリックし、[組織を表示] をクリックします。

Cloud Services コンソール に戻り、必要なロールを割り当てることができます。

ユーザーの追加とロールの割り当ての概要

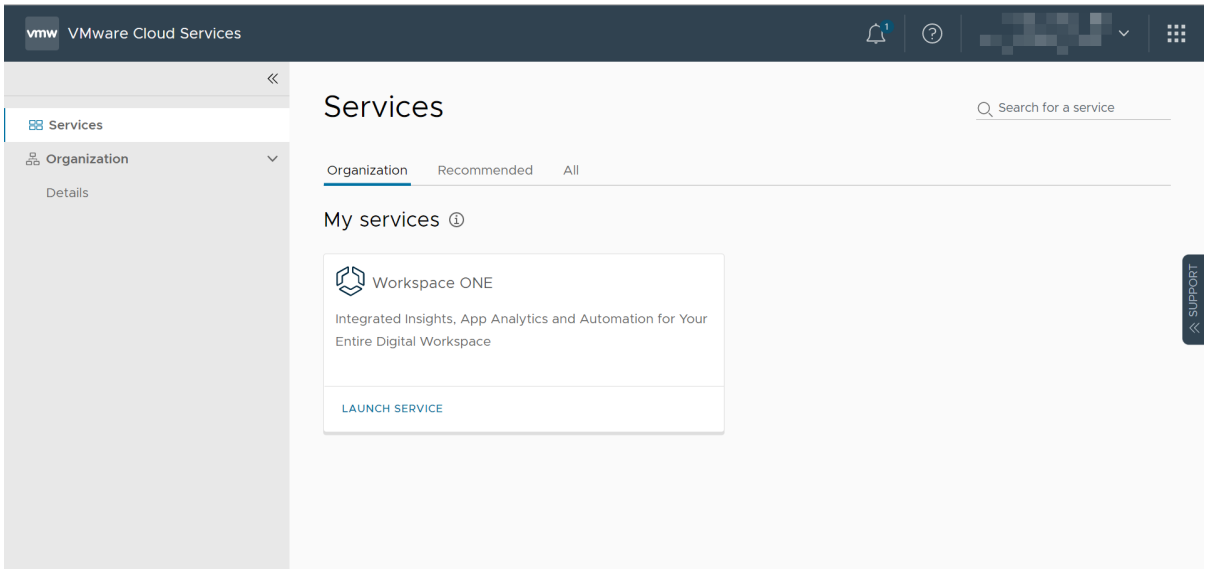
ウェルカム E メールのリンクを使用して招待を引き換えると、自動的に管理者ロールが割り当てられます。管理者ロールにより、オンボーディングする必要がある Horizon Universal Console のユーザー インターフェイスと API に対する完全な権限が付与されます。Horizon Universal Console へのアクセス権を他の管理者ユーザーに付与することができます。詳細については、Horizon Universal Console ユーザーへの管理ロールの割り当てを参照してください。

Cloud Services コンソール を使用して Workspace ONE を起動する

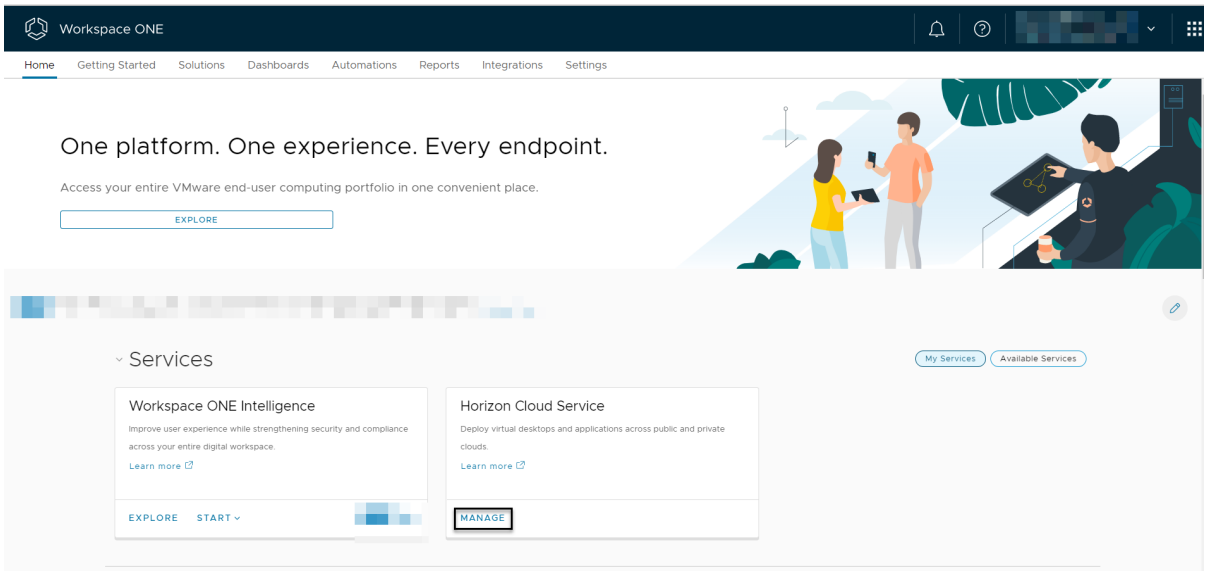
Horizon Cloud を起動するには、次の手順を実行します。

1 左側のペインで、[サービス] をクリックします。

2 Workspace ONE に対して [サービスの起動] をクリックします。

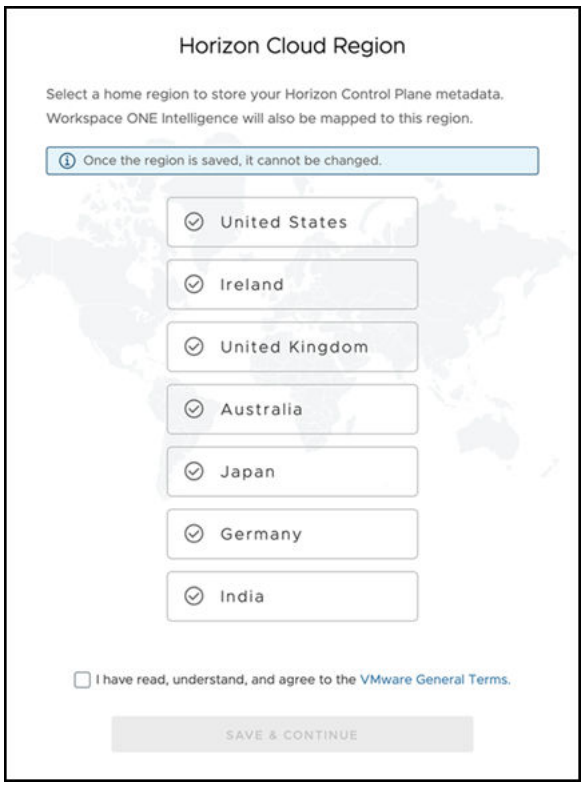


3 [Horizon Cloud Service] タイルで [管理] をクリックして、Horizon Universal Console を起動します。



Horizon Universal Console を使用して Horizon Cloud リージョンを選択する

コンソールを起動すると、リージョンを選択するように求められます。データ主権の原則に準拠するには、リソースとそのメタデータを配置するリージョンを選択する必要があります。一度選択したリージョンは変更できません。



1 Horizon Cloud リージョンを選択します。

2 サービスの利用条件に同意するチェックボックスを選択します。

3 [保存して続行] をクリックします。

Horizon Cloud Service - next-gen の Horizon Universal Console へようこそ

コンソールに [ようこそ] 画面が表示されたら、画面上のガイダンスに従って、テナントの最初のデプロイの画面上の選択を行います。

注： この時点で、Horizon Universal Console に、ライセンスの同期が進行中であることを示すバナーが画面の上部に表示されることがあります。この場合、同期が完了してブラウザを更新するまで、コンソールには特定のライセンスによって有効になるすべての機能が表示されません。同期が完了すると、ユーザーのライセンスに該当する要素が Horizon Universal Console に表示されます。

画面上のガイダンスをサポートするドキュメントについては、デプロイのタイプに応じて、次を参照してください。

- Horizon Plus の使用開始とデプロイ
- Microsoft Azure のデプロイ、Horizon Edge - デプロイするための準備
- Horizon 8 のデプロイ、Horizon Edge - デプロイするための準備
- Horizon Cloud Service - next-gen を使用した Horizon 8 フェデレーション デプロイの構成

Horizon 制御プレーン および Horizon Cloud Service - next-gen のセットアップとデプロイ

5

セットアップ チェックリストを使用し、ネットワーク、キャパシティ、および統合設定を構成し、Horizon 制御プレーン および Horizon Cloud Service - next-gen に Edge を作成してデプロイする準備を行います。

次のトピックを参照してください。

- Edge デプロイの ID およびアクセス プロバイダ情報の設定
- リソース キャパシティ プロバイダへの Horizon Edge のデプロイ
- 統合の構成

Edge デプロイの ID およびアクセス プロバイダ情報の設定

Horizon Cloud Service - next-gen では、Edge の構成とデプロイ プロセスの一環として、Active Directory ドメインと ID プロバイダ (IdP) を構成します。

2 章 Horizon 制御プレーンの使用開始 - Microsoft Azure および Horizon 8 のデプロイ 要件チェックリストの作成に加えて、Active Directory ドメインと ID プロバイダを構成します。関連情報については、次のトピックを参照してください。

- Active Directory ドメインの設定
- ID プロバイダの設定
- ID プロバイダの接続

目的のデプロイのユースケースに適用可能なドメインと ID プロバイダの構成を完了したら、「リソース キャパシティ プロバイダへの Horizon Edge のデプロイ」の手順を使用して適切な Horizon Edge をデプロイします。

リソース キャパシティ プロバイダへの Horizon Edge のデプロイ

ID プロバイダに接続したら、プロバイダ、サイト、およびネットワークにシン Edge クラウド インフラストラクチャをデプロイできます。

Horizon 8 Edge デプロイ

Horizon Cloud Service - next-gen をオンボーディングするには、次のセクションの説明に従って Horizon Connection Server を使用して Horizon Edge を設定し、管理者アカウントに送信された Horizon Cloud Service - next-gen ウェルカム メールを利用する必要があります。

Horizon Cloud Service - next-gen ウェルカム メールの利用方法については、「4 章 Horizon Cloud Service - next-gen 管理者のオンボーディング」を参照してください。

Active Directory ドメインと ID プロバイダを構成するには、「Edge デプロイの ID およびアクセス プロバイダ情報の設定」を参照してください。

Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイ

このページでは、Horizon 8 ポッドをリソース プロバイダとして使用し、そのポッドが vSphere 環境（オンプレミスまたはオールイン SDDC デプロイ）にある Horizon Edge を作成する場合の Horizon Universal Console の [Horizon Edge を追加] ワークフローの手順について説明します。また、目的の仮想化プラットフォームへのフェデレーションデプロイに対して、さまざまなキャパシティ タイプを構成することもできます。Horizon Edge では、1 つの Horizon Connection Server ポッドのみがサポートされます。

Horizon Edge のデプロイには、Horizon Edge Gateway アプライアンスの vSphere インフラストラクチャへのデプロイ、そのアプライアンスと Horizon 制御プレーン のペアリング、Horizon Edge 用の Horizon 8 ポッドの Horizon Connection Server の詳細の構成が含まれます。

重要： Horizon Edge Gateway アプライアンスを vSphere インフラストラクチャにデプロイする場合は、vSphere Client または vSphere Web Client を使用してデプロイする必要があります。アプライアンスを ESXi ホストに直接デプロイしないでください。

このエンドツーエンドのプロセスには、複数の手順があります。

1 このプロセスは、Horizon Universal Console を使用して開始します。[使用開始] ページで、[][Horizon 8] を選択して、[デプロイと構成] ページに移動します。Horizon 8 を Horizon Universal Console に接続するには、最初の Horizon Edge をデプロイし、ID プロバイダに接続して、Horizon 8 ユーザー カード、ユーザー検索、およびヘルプ デスク機能を有効にします。ID プロバイダに接続しない場合、コンソールの [ユーザーを検索] フィールドは無効になります。

2 OVA アプライアンスを vSphere 環境にデプロイします。OVA のデプロイ時に、プロセスの最初の部分で作成されるペアリング コード情報を OVF テンプレートのデプロイ ユーザー インターフェイス フィールドで使用する必要があります。

   注： Horizon Edge Gateway OVA/OVF デプロイは、オールイン SDDC アーキテクチャまたはキャパシティ タイプのプライベート データセンターを使用する Horizon 8 プロバイダのみが使用できます。フェデレーション アーキテクチャを使用する Horizon 8 プロバイダの場合は、「Horizon Cloud Service - next-gen を使用した Horizon 8 フェデレーション デプロイの構成」で説明されている特定のキャパシティ タイプの手順を参照してください。

3 Horizon Universal Console に戻り、ペアリング ステータスが成功したことを確認し、このコンソールの残りの手順を完了して Horizon 8 ポッドの詳細を追加します。

注： 「Horizon 8 ポッド」という語は、Horizon Cloud Service - next-gen での使用がサポートされているバージョンの 1 つである Horizon Connection Server ソフトウェア バージョンを実行しているポッドを指します。たとえば、Horizon 7 バージョン 7.13 がサポートされているバージョンの 1 つである場合、このフレーズはそのバージョンを実行しているポッドにも適用されます。Horizon バージョンと Horizon Cloud Service - next-gen の製品バージョンの相互運用性については、「VMware 製品の相互運用性マトリックス」を参照してください。Horizon Edge ごとにサポートされる Horizon 8 は 1 つのみです。

Horizon Edge は、シン Edge クラウド インフラストラクチャです。Horizon 8 デプロイの場合、Horizon 8 ポッドは Horizon Edge のキャパシティ プロバイダです。

環境が少なくとも 1 つの Active Directory ドメインと ID プロバイダで構成されると、コンソールによってこの [Horizon Edge を追加] ワークフローが使用可能になります。

前提条件

- Horizon 8 Edge をデプロイするための要件チェックリストの要件を確認し、これらの要件を満たします。
- 「Horizon 8 Edge デプロイ」ページにある、リンク付きのページで説明されている準備項目を確認し、実行します。
- デプロイされた Horizon Edge Gateway アプライアンスに使用する完全修飾ドメイン名 (FQDN) を判断します。ユーザー インターフェイス ウィザードで、その FQDN を入力するように求められます。
- この Horizon Edge に含まれる Horizon Connection Server に自己署名証明書がある場合は、ウィザードの検証手順の証明書のフィンガープリントを確認してください。
- Horizon Cloud Service - next-gen によってレンダリングされたデフォルトの証明書がプロキシまたはその他の手段でカスタム証明書に置き換えられると、Horizon Edge Gateway から Horizon Cloud Service - next-gen への送信 TLS 接続が失敗する場合があります。デフォルトの証明書をカスタム証明書に置き換えることはサポートされていません。
- **注：** Horizon Edge Gateway OVA/OVF デプロイは、オールイン SDDC アーキテクチャまたはキャパシティ タイプのプライベート データセンターを使用する Horizon 8 プロバイダのみが使用できます。フェデレーション アーキテクチャを使用する Horizon 8 プロバイダの場合は、「Horizon Cloud Service - next-gen を使用した Horizon 8 フェデレーション デプロイの構成」で説明されている特定のキャパシティ タイプの手順を参照してください。
- ここに記載された手順を実行する前に、次の TechZone ビデオをご覧ください。
  - Horizon Edge Gateway アプライアンスのデプロイ - https://via.vmw.com/tchzmno5209 での DNS 構成
  - Horizon Edge Gateway アプライアンスのデプロイ - https://via.vmw.com/tchzmno5210 での URL チェッカー
  - Horizon Edge Gateway アプライアンスのデプロイ - https://via.vmw.com/tchzmno5211 でのプロバイダとアプライアンスの構成
  - https://via.vmw.com/tchzmno5212 での OVA からの Horizon Edge Gateway のデプロイ

手順

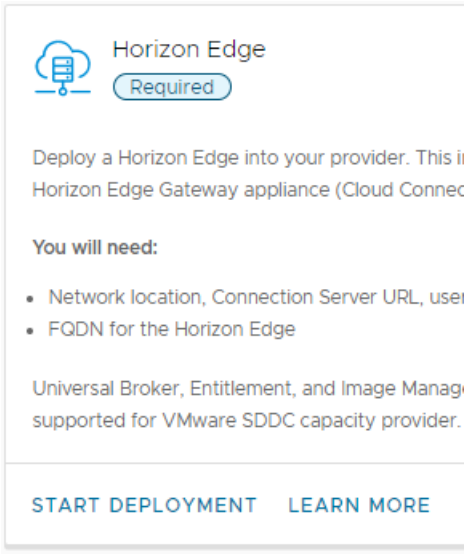
1 コンソールの [Horizon Edge を追加] ウィザードを起動します。

コンソールでは、[Horizon Edge を追加] ウィザードをさまざまなエントリ ポイントから使用できます。コンソールでのこの手順の開始点は通常、環境が新規であるか、Horizon 8 または Microsoft Azure 向けの Horizon Edge の既存のデプロイがあるかによって異なります。

Horizon Edge はまだありません - コンソールの Horizon Edge カードから開始します

環境に Horizon Edge がない場合、通常は [デプロイの開始] をクリックしてウィザードを開始します。

次のスクリーンショットは、この [Horizon Edge] カードを示しています。



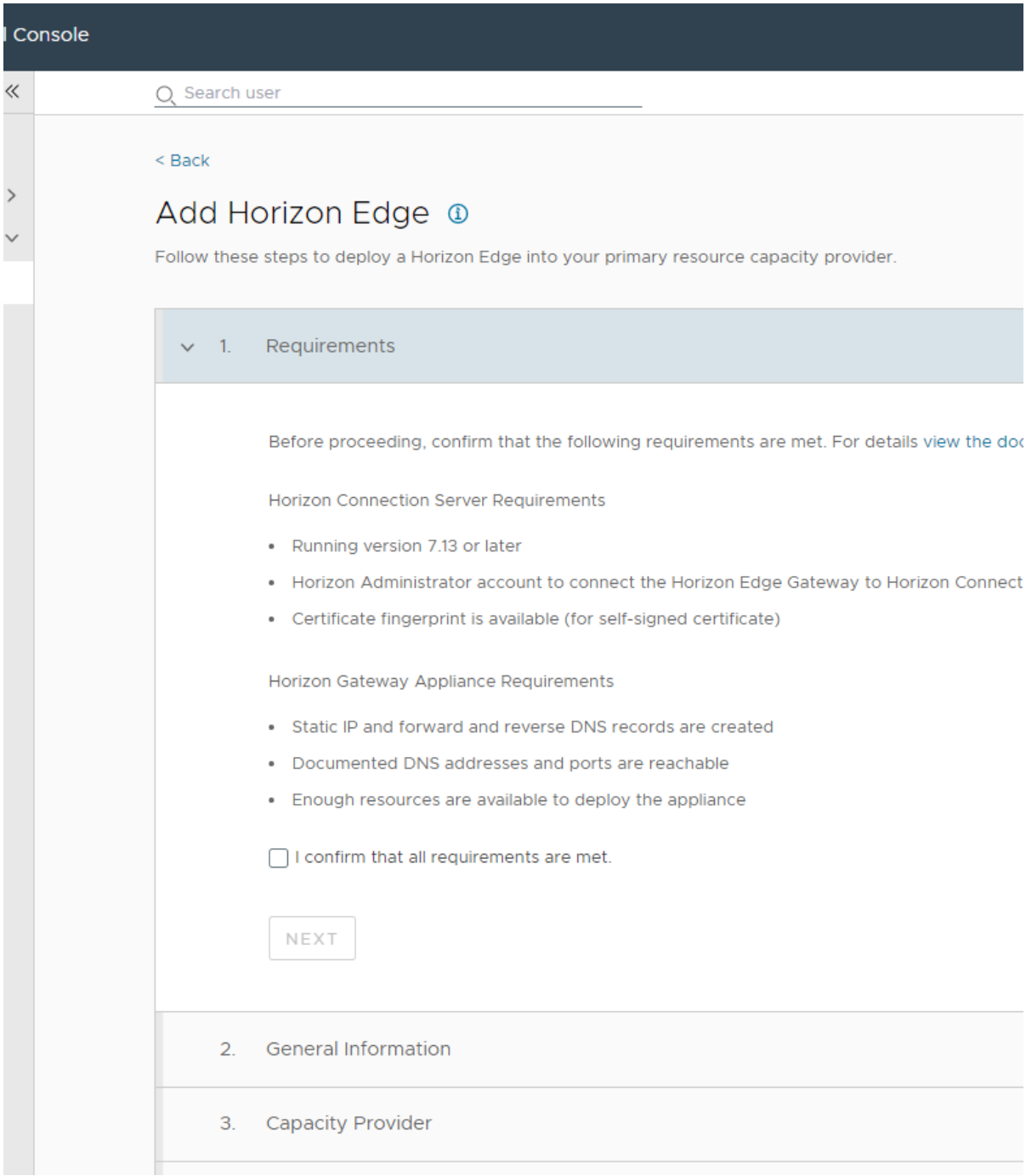
Horizon Edge がありません - 代わりに、コンソールの [キャパシティ] ページから開始します

環境に Horizon Edge がまだデプロイされていない場合、[キャパシティ] ページにはテキストと [開始] メニューが表示されます。このシナリオでは、ウィザードを開始するには、[リソース] - [キャパシティ] の順に移動し、[開始] - [Horizon 8] の順にクリックします。

少なくとも 1 台の Horizon Edge - コンソールの [キャパシティ] ページから開始します

環境に少なくとも 1 台の Horizon Edge がデプロイされている場合、[キャパシティ] ページには既存の Horizon Edge を一覧表示するグリッドが含まれます。このシナリオでは、ウィザードを開始するには、[リソース] - [キャパシティ] の順に移動し、[追加] - [Horizon 8] の順にクリックします。

これらの 3 つの方法のいずれかを使用してウィザードを開始すると、コンソールには [Horizon Edge を追加] ウィザードの手順 1 が表示されます。



画面上のガイダンスに従って、ウィザードの各手順を完了します。

2 一意の [Horizon Edge 名] と必要に応じて説明を追加します。

3 ページの [キャパシティ プロバイダ] セクションで、Horizon Edge Gateway を展開する [キャパシティ タイプ] を選択し、この Horizon Edge の場所を入力します。次のキャパシティ タイプを使用できます。

注 : 参考までに、以下のハイフン (-) 記号の後の値は、Horizon Connection Server で使用される値を反映しています。

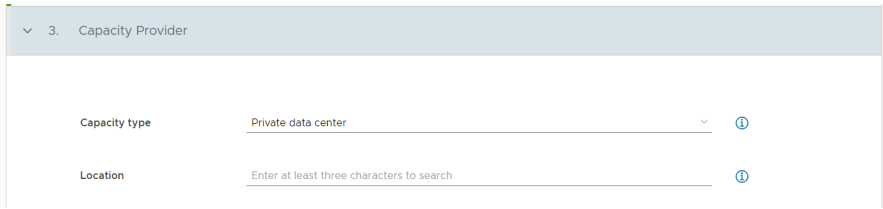
- プライベート データセンター – 全般

- Microsoft Azure – Azure VMware ソリューション (AVS)
- Amazon Web Services – VMware Cloud on AWS (VMC)
- Google Cloud – Google Cloud VMware Engine (GCVE)
- Oracle Cloud – Oracle Cloud VMware ソリューション (OCVS)
- Alibaba Cloud – Alibaba Cloud VMware Solution (ACVS)
- Dell EMC Cloud

選択したキャパシティ タイプがフェデレーションをサポートしている場合は、アーキテクチャ タイプの指定を求めることもできます。選択したキャパシティ タイプに応じて、アーキテクチャ タイプを指定する 3 つのオプションのいずれか 1 つを使用できます。

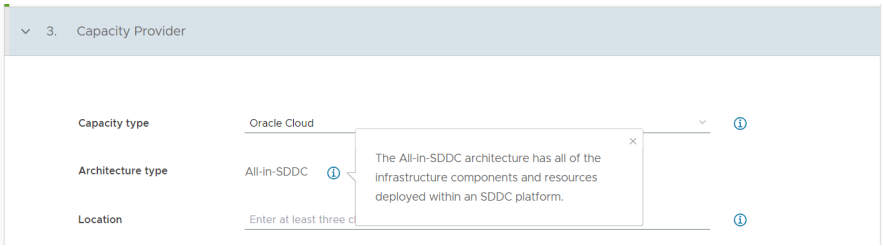
- キャパシティ タイプはプライベート データセンターです。

  キャパシティ タイプがプライベート データセンターの場合、次のスクリーンショットに示すように、アーキテクチャ タイプの設定は表示されません。

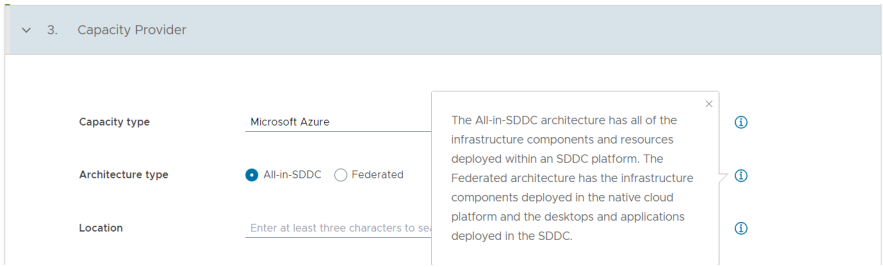
- キャパシティ タイプは、フェデレーション アーキテクチャをサポートしていません。

  キャパシティ タイプがフェデレーション アーキテクチャをサポートしていない場合、アーキテクチャ タイプの設定は、次のスクリーンショットに示すようにデフォルトの選択可能でない [オールイン SDDC] の値で表示されます。

- キャパシティ タイプはフェデレーション アーキテクチャをサポートします。

  キャパシティ タイプがフェデレーション アーキテクチャをサポートしている場合、アーキテクチャ タイプの設定は、次のスクリーンショットに示すように [フェデレーション] または [オールイン SDDC] の選択可能なオプションで表示されます。



次に、適切なアプライアンス タイプを選択します。表示される使用可能なアプライアンス タイプは、[フェデレーション] または [オールイン SDDC] アーキテクチャのどちらのオプションを選択するかによって異なります。

アーキテクチャ タイプとして [フェデレーション] を選択した場合、指定したキャパシティ タイプに応じて、ページの [Horizon Edge Gateway アプライアンスのダウンロード] セクションでは異なる Edge アプライアンス ファイルが使用可能になります。

フェデレーションの Horizon Edge の指定に関する情報については、「Horizon Cloud Service - next-gen を使用した Horizon 8 フェデレーション デプロイの構成」を参照してください。

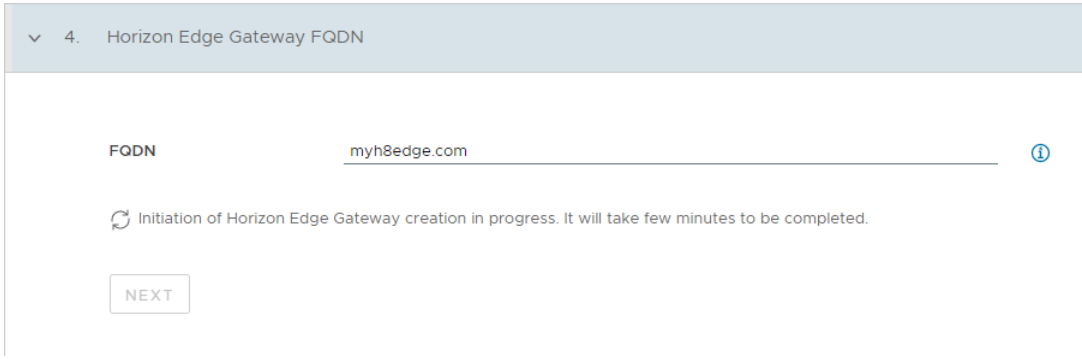
4 [場所] を使用して、このデプロイの場所（通常はキャパシティ プロバイダの場所に最も近い地理的な場所）を指定します。

5 ページの [Horizon Edge Gateway FQDN] セクションで、[Horizon Edge Gateway FQDN] 値に、Horizon Edge Gateway アプライアンスに使用する FQDN を入力します。

重要： アプライアンスが vSphere 環境にデプロイされ、IP アドレスがわかるとすぐに、DNS レコードを DNS サーバに登録して、ここで入力したこの [Horizon Edge Gateway FQDN] に IP アドレスをマッピングする必要があります。実行する操作の図については、Tech Zone のビデオ Edge Gateway のデプロイ - DNS 構成を確認してください。

フェデレーション アーキテクチャで構成された Horizon 8 Edge の場合、デフォルトでは Horizon 8 Edge アプライアンスの Kubernetes クラスタの CIDR 範囲を構成することはできません。目的の CIDR 構成に合わせて k8s クラスタを再構成して再起動するには、カスタマー サポートにお問い合わせください。

FQDN を入力すると、この時点までウィザードに入力した情報の保存が開始されます。システムは、システムのレコードに Horizon Edge レコードを登録します。



重要： Horizon Edge が作成されたことを示すメッセージが画面に表示されますが、そのメッセージは、この Horizon Edge のシステム レコードの作成を示しています。Horizon Edge Gateway アプライアンス バイナリをダウンロードし、そのバイナリを使用して Horizon Edge Gateway アプライアンスを vSphere 環境にデプロイし、そのアプライアンスとクラウド制御プレーンのペアリングを完了し、Horizon Connection Server の詳細を指定するまで、エンドツーエンドのデプロイは不完全です。

6 Horizon ユニバーサル ライセンスを使用している場合は、トグルを使用して [エージェントの監視] を有効または無効にできます。[エージェントの監視] を無効にすることを選択した場合は、チェックボックスをクリックして関連するリスクを確認します。Horizon Plus ライセンスを使用している場合、[エージェントの監視] を無効にすることはできません。[次へ] をクリックします。

注： これは、View Edge タイプにのみ適用され、Azure には適用されません。このアクションにより、エージェントの監視のみが無効になります。CS 監視およびその他すべてのデータは引き続き WS1 に送信されます。

エージェントの監視により、Horizon Agent は仮想マシンの使用率やエラー情報などのデータを Workspace ONE Intelligent Hub に送信できます。Edge でこのオプションを有効にしておくことをお勧めします。

エージェントの監視データを無効にすることは、Horizon Cloud Service - next-gen の機能と保守性に影響するため、推奨されません。

7 [ダウンロード] を使用して、Horizon Edge Gateway アプライアンス バイナリを取得します。

ダウンロードしたバイナリを目的の仮想化プラットフォームにデプロイする場所に保存します。フェデレーション Edge のデプロイの詳細については、「Horizon Cloud Service - next-gen を使用した Horizon 8 フェデレーション デプロイの構成」を参照してください。

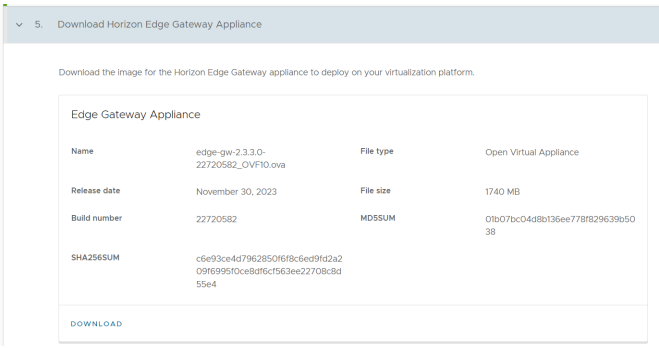
注： バイナリ サイズは約 1.7 GB です。

Tech Zone のビデオに示されているように、vSphere 内で Horizon Edge Gateway をデプロイしている場合は、ボタンを右クリックして URL をコピーし、その URL を vCenter Server の [OVF テンプレートのデプロイ] ユーザー インターフェイスの [URL] フィールドで使用することもできます。この URL メソッドの使用方法の詳細については OVA からの Horizon Edge アプライアンスのデプロイビデオを参照してください。

Horizon Edge Gateway アプライアンスをフェデレーション モードでデプロイする場合は、指定したキャパシティ タイプに対応する「Horizon Cloud Service - next-gen を使用した Horizon 8 フェデレーション デプロイの構成」を参照してください。

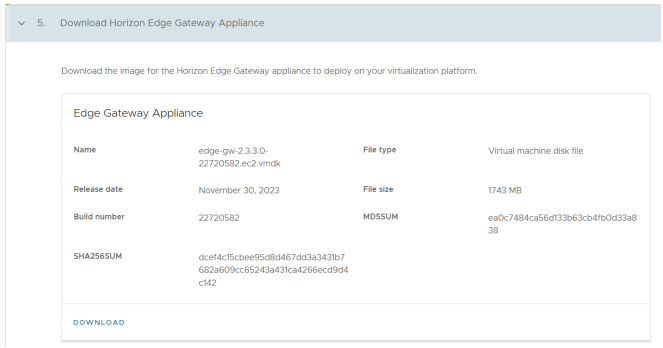
選択したキャパシティ タイプとフェデレーション アーキテクチャに基づいて、ダウンロード手順のサンプル イメージを次に示します。

- キャパシティ タイプを選択したオールイン SDDC アーキテクチャのサンプル イメージを次に示します。

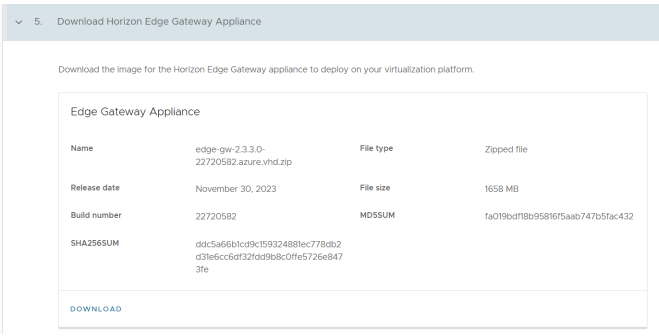


このビルドは、プライベート データセンターでも同じです。

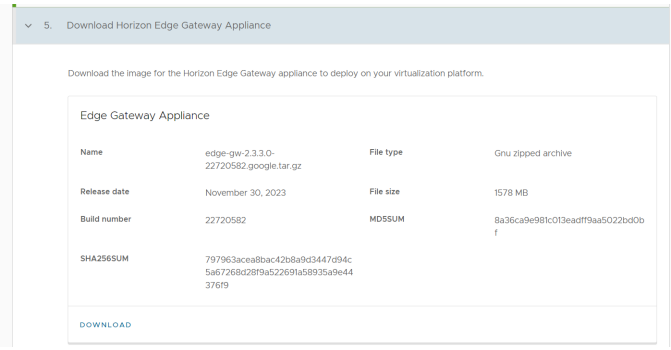
- フェデレーション アーキテクチャを使用する AWS のキャパシティ タイプのサンプル イメージを次に示します。



- フェデレーション アーキテクチャを使用する Microsoft Azure のキャパシティ タイプのサンプル イメージを次に示します。



- フェデレーション アーキテクチャを使用する Google のキャパシティ タイプのサンプル イメージを次に示します。



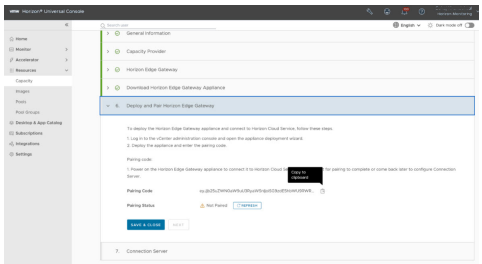
8 [OVF テンプレートのデプロイ] ユーザー インターフェイスで使用するバイナリ ファイルまたは URL を取得したら、[次へ] をクリックします。

9 プロンプトに従って、ユーザー インターフェイスでシステム生成のペアリング コードをコピーし、コピー アンド ペーストできる場所に保存します。これは、[OVF テンプレートのデプロイ] ユーザー インターフェイスを使用してアプライアンスをデプロイするときに必要になります。

注目: ペアリング コードは、エンドツーエンドのプロセスを成功させるために重要です。アプライアンスのデプロイ時に [OVF テンプレートのデプロイ] ユーザー インターフェイス内で、このペアリング コードを使用する必要があります。[OVF テンプレートのデプロイ] ユーザー インターフェイスは、このコードに別のラベル ([OVF テンプレートのデプロイ] ユーザー インターフェイスの [接続文字列]) を使用します。

コンソールに完全なペアリング コード文字列が表示されないため、指定されたコピー アイコンを使用します。コード文字列はコンソールに表示される文字列よりも長いので、表示されているテキストを強調表示してコピーするだけでは、完全なコード文字列を取得できません。

次のイメージは、ユーザー インターフェイスを使用してペアリング コードをコピーする方法を示しています。



10 この手順は、オールイン SDDC アーキテクチャの選択に基づいて vSphere 環境にデプロイする場合にのみ適用されます。代わりに、デプロイにフェデレーション アーキテクチャを使用している場合は、指定したキャパシティ タイプに関連する「Horizon Cloud Service - next-gen を使用した Horizon 8 フェデレーション デプロイの構成」を参照してから、このプロセスの次の手順に戻ります。

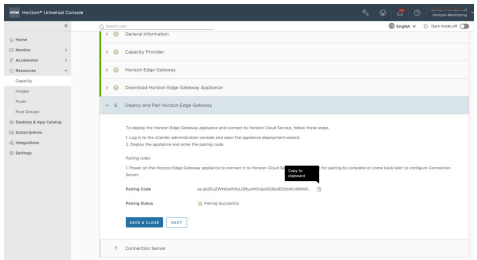
vSphere 環境へのアプライアンスのデプロイに関する画面上のガイダンスを読み、その環境で [OVF テンプレートのデプロイ] ユーザー インターフェイスを使用してアプライアンスをデプロイする手順を実行します。このウィザードに戻ってペアリングが成功したかどうかを確認するため、これらの手順を実行する間、ブラウザでこの [Horizon Edge を追加] ウィザードを開いたままにしておいてください。

[OVF テンプレートのデプロイ] ユーザー インターフェイスを使用して Horizon Edge Gateway アプライアンスをデプロイする手順については、Tech Zone のビデオ「OVA からの Horizon Edge アプライアンスのデプロイ」を参照してください。

注目: [OVF テンプレートのデプロイ] ユーザー インターフェイスの [テンプレートのカスタマイズ] 手順で、[ペアリング コード] フィールドに、前の手順で Horizon Edge を追加 ウィザードからコピーした [ペアリング コード] 文字列を入力する必要があります。

Horizon Edge Gateway アプライアンスを正常にデプロイするには、[ペアリング コード] フィールドに正しいペアリング コードを入力する必要があります。

次のイメージは、Horizon Universal Console の [Horizon Edge を追加] ウィザードからコピーした [ペアリング コード] 文字列を貼り付ける [ペアリング コード] フィールドの場所を示しています。



OVF ツールのユーザー インターフェイスの [設定内容の確認] 手順には、[テンプレートのカスタマイズ] 手順に入力したプロパティが表示されます。

Horizon Universal Console からコピーした完全なペアリング コード文字列がこのプロパティ セットに反映されていることを確認します。

注: [POD ネットワーク] および [サービス ネットワーク] は、アプライアンスの内部 Kubernetes クラスタで使用される内部値です。これらの値はデフォルトのままにします。

11 OVF がデプロイされたら、アプライアンスでパワーオンします。

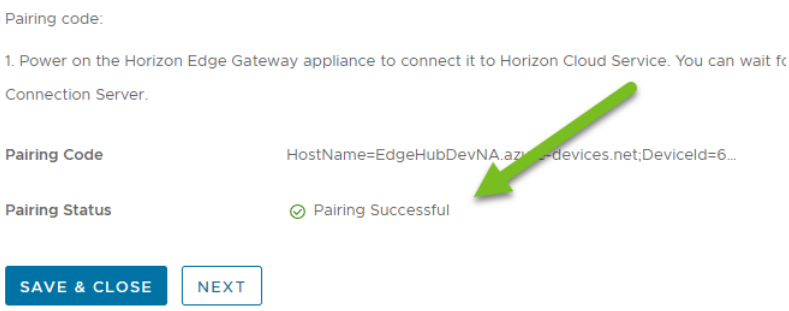
アプライアンスがパワーオン状態で実行されている場合は、Horizon Universal Console の [Horizon Edge を追加] ウィザードに戻り、[ペアリング ステータス] の [更新] をクリックします。

注: デプロイされたアプライアンスからクラウド制御プレーンにシステムがステータスを通知するまでに数分かかる場合があります。

正しくコピーされたペアリング コードを OVA デプロイ ユーザー インターフェイスに入力し、アプライアンスをパワーオンし、DNS レコードの要件を満たし、このドキュメント ページの上部に記載されているすべての前提条件を満たしている場合、システムは成功なペアリングを反映しているはずです。更新時に、表示される [ペアリング ステータス] は [ペアリングに成功しました] に変更されます。

Edge のペアリングが成功しない場合は、診断ツールの実行と、Edge が [ペアリングに成功しました] 状態にならない理由のトラブルシューティングについて、ナレッジベースの記事「Horizon 8 Edge の接続問題のトラブルシューティング」を参照してください。

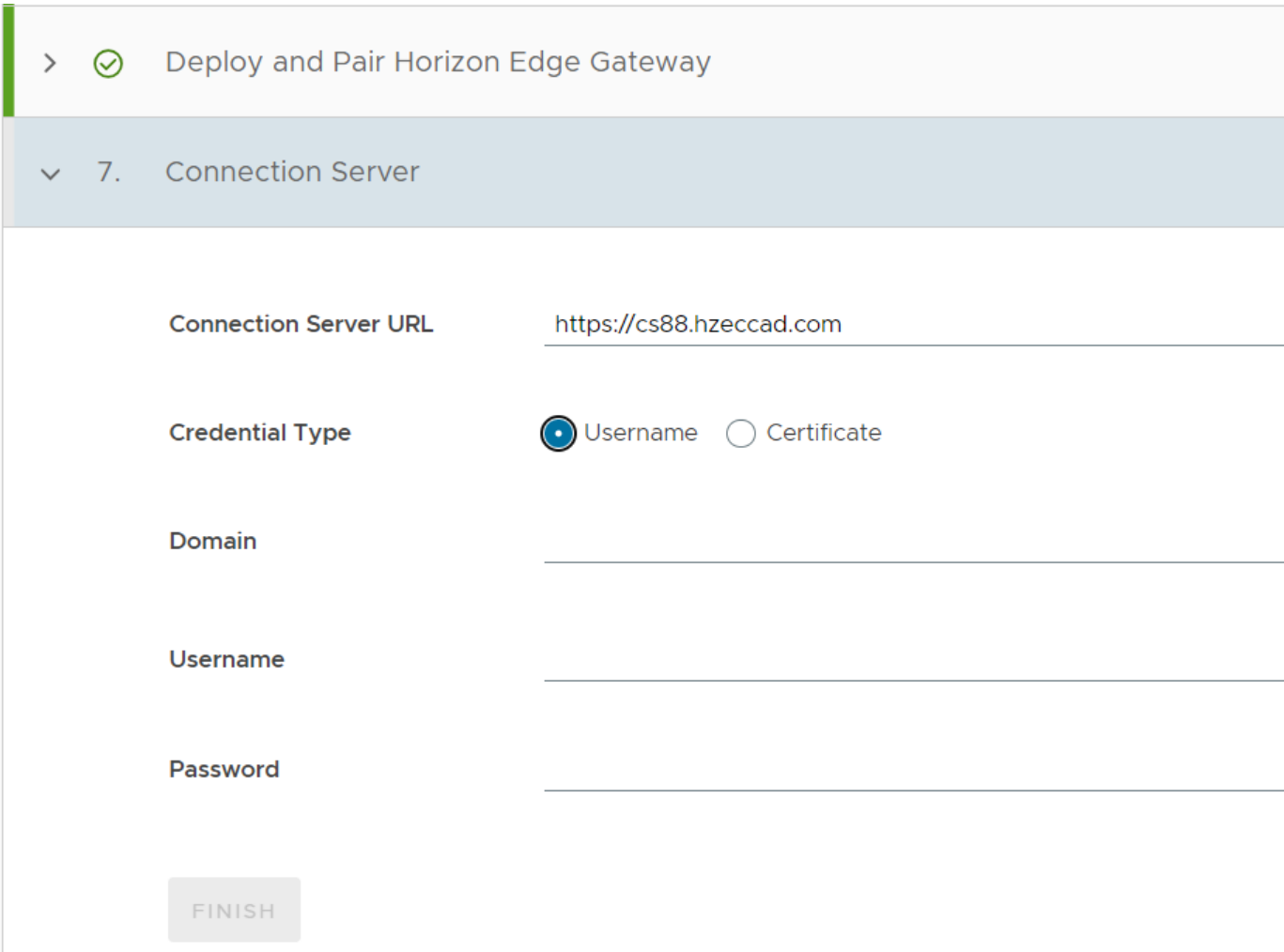
次のスクリーンショットは、成功なペアリングを示しています。



12 [次へ] をクリックして Horizon Connection Server 情報の入力に進みます。

13 Horizon Connection Server 情報のフィールドを入力し、[終了] をクリックします。

このページでは、認証のための [Connection Server URL] と [認証情報タイプ] の入力を求められます。



- Horizon 8 Edge の [ドメイン] 値には、ユーザー アカウントが配置されている場所の DNS [ドメイン] 名を指定します。NetBIOS 名を使用しないでください。

- [ユーザー名] 認証情報タイプを選択した場合は、Horizon Connection Server への接続に使用する Horizon 8 アカウントの [ドメイン]、[ユーザー名]、および [パスワード] を入力します。

  注： Connection Server URL では、ロード バランサの FQDN はサポートされていません。個々の Connection Server の FQDN のみを指定します。Horizon Edge Gateway アプライアンスとロード バランサの FQDN のペアリングはサポートされていません。

  次の表に、このアカウントでサポートされているロールと、アカウントに割り当てられているロールに応じて使用可能なクラウド機能について説明します。これらのロールの詳細については、Horizon ドキュメントにある、該当する製品バージョンの「事前定義された管理者ロール」トピックを参照してください。

ロール	Horizon Cloud の機能
管理者	すべての Horizon Cloud Service の機能を許可します。
Horizon Cloud Service	サブスクリプション ライセンスの適用と管理を許可します。

- [証明書] 認証情報タイプを選択した場合は、PKCS12 または PFX 形式で証明書をアップロードし、証明書がパスワードで保護されている場合はパスワードを入力します。

  注： この認証方法を使用するには、Horizon Connection Server で証明書認証を有効にする必要があります。関連情報については、Horizon 製品ドキュメントの『Horizon セキュリティ』出版物にある「Horizon Console のセキュリティ関連のグローバル設定」を参照してください。

14 [終了] をクリックします。

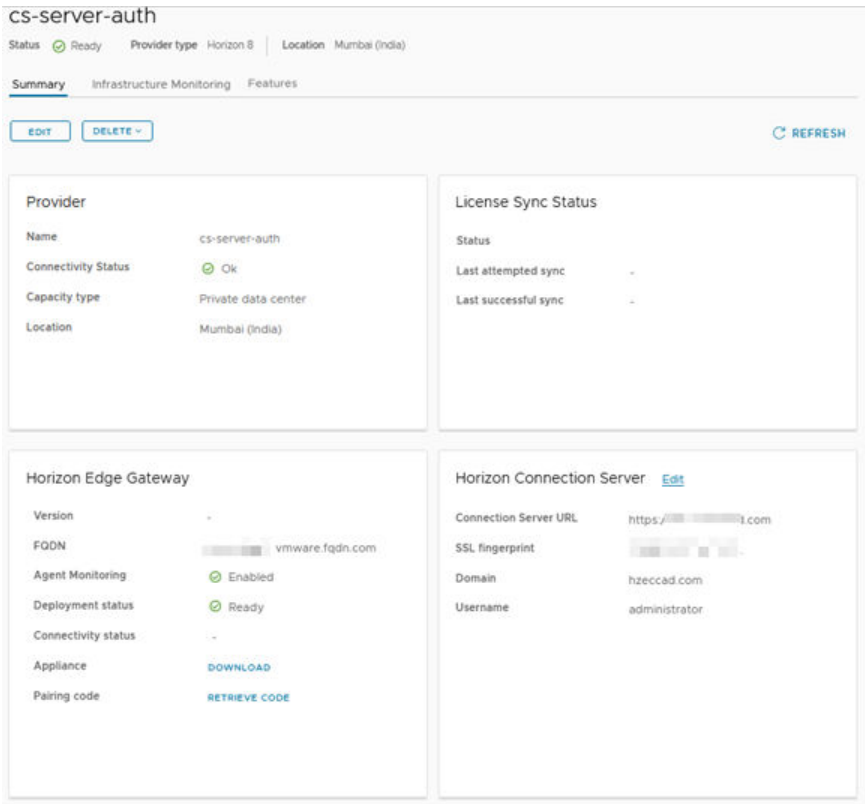
Horizon Connection Server に自己署名証明書があることをシステムが検出すると、証明書の詳細を確認するボックスが表示されます。入力された Horizon Connection Server URL が Connection Server 上の証明書内のどのホスト名とも一致しない場合は、これを確認するメッセージが表示されます。状況に応じて確認します。

結果

すべてが成功すると、コンソールはウィザードのユーザー インターフェイスを閉じ、この新しく追加された Horizon Edge の詳細ページを表示します。

注： ネットワーク トラフィックによっては、詳細ページの接続ステータス インジケータの更新が完了するまでに 1 分かかる場合があります。

次のイメージは、キャパシティ プロバイダとして Horizon 8 ポッドが正常に接続されている詳細ページの例を示しています。



次のステップ

- DNS サーバに DNS レコードを登録し、デプロイされたアプライアンスの IP アドレスをウィザードに入力した [Horizon Edge Gateway FQDN] にマッピングしていることを確認します。何をすべきかについては、Tech Zone のビデオ Edge Gateway のデプロイ - DNS 構成を参照してください。

  注： 2 台以上の Horizon Connection Server インスタンスに DNS エイリアスを使用することはサポートされていません。これにより、Horizon Edge Gateway アプライアンス認証の問題が発生します。

- Horizon 8 Edge の Horizon Connection Server 証明書認証情報の期限切れによるダウンタイムを回避するには、Horizon 8 Edge の Horizon Connection Server 証明書の次回の期限切れに関する通知を探して対応します。Horizon Cloud Service - next-gen は、このタイプの通知を Horizon Universal Console に表示します。また、VMware Cloud Services Platform (CSP) とも呼ばれる VMware Cloud Services に登録されている管理者の場合は、システムによりこの情報が E メールでも送信します。

  これらの通知を受け取ったときに実行するアクションは、有効期限が切れる前に証明書を更新することです。有効期限が切れる前に証明書を更新しないと、エンドユーザーのアクセスと管理操作が中断されます。

Horizon Cloud Service - next-gen 制御プレーンへのアクセス

Horizon Cloud Service - next-gen 制御プレーンは次のデプロイ タイプをサポートしています。

- Microsoft Azure
- ライセンス サービスを使用するためにオールイン SDDC モデルを使用してデプロイされた Horizon 8
- Horizon Plus のデプロイ

Horizon Universal Subscription があり、ユースケースに含まれるのが Horizon 8 ポッドのみで、これらのデプロイで Horizon Image Management Service (IMS)、Universal Broker、マルチクラウド割り当てなどの追加の Horizon SaaS サービスを使用するには、「Horizon Cloud 例外要求」アンケートを記入して、送信してください。

Horizon 8 Edge の Fault Tolerance の構成

次の手順では、Horizon 8 ポッドをリソース プロバイダとして使用する Horizon Edge のフォルト トレランスを構成する方法について説明します。このポッドは、VMware vSphere 環境（オンプレミスまたはオールイン SDDC デプロイ）にあります。

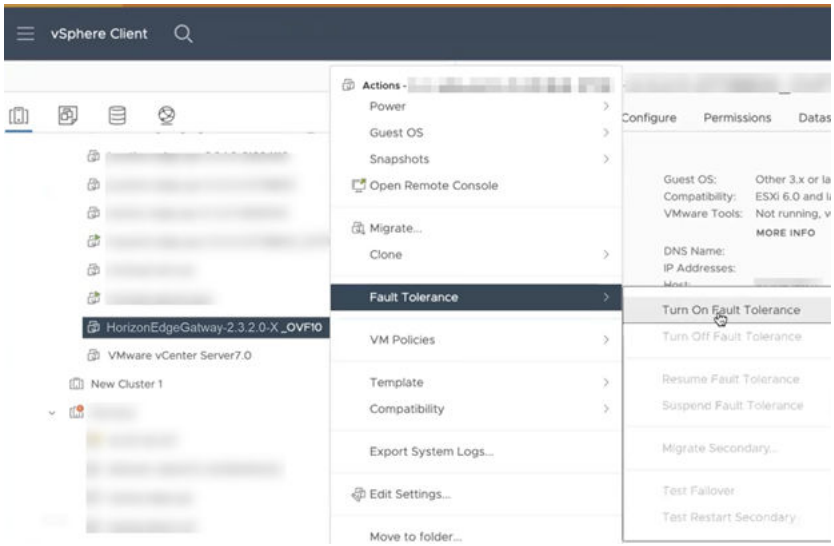
この手順では、vSphere Client を使用して、VMware vSphere インフラストラクチャ内の Horizon Edge Gateway アプライアンスでフォルト トレランスを構成する必要があります。

前提条件

- WAN トランスポートとして 10 ギガビット Etherent (10GbE) を使用します。
- Horizon Edge をデプロイします。Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイを参照してください。

手順

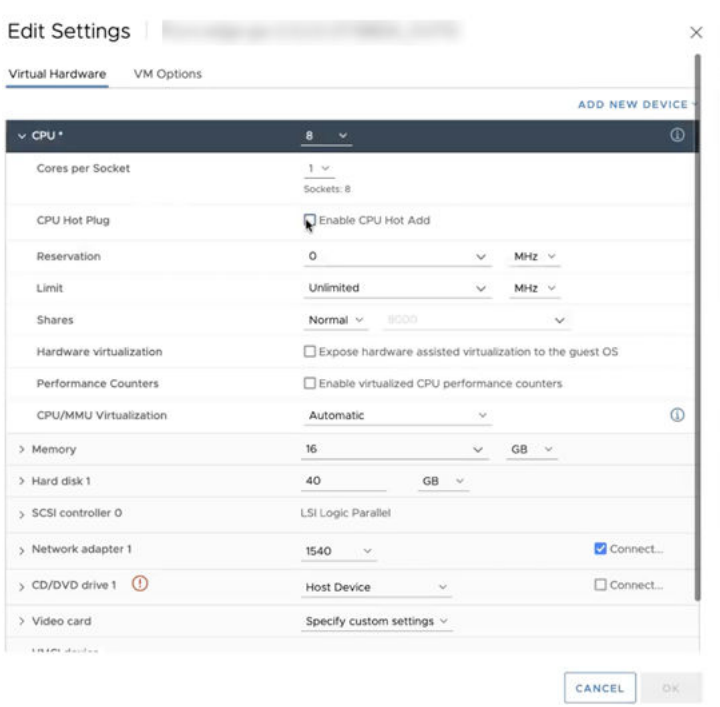
1 vSphere Client を使用して、Horizon Edge Gateway アプライアンス仮想マシンに移動し、[フォルト トレランス] - [フォルト トレランスをオンにする] を選択します。



a 仮想マシンでサポートされていないホット CPU ホット プラグに関するエラーが表示された場合は、仮想マシンをオフにして、[設定の編集] ダイアログ ボックスで [仮想ハードウェア] タブを選択して、仮想マシンの構成を次のように編集します。

1 CPU ホット プラグを無効にします。

CPU ノードを展開し、[CPU ホット プラグ] セクションで [CPU ホット アドを有効にする] チェックボックスを選択解除して無効にします。



2 メモリ ホット プラグを無効にします。

メモリ ノードを展開し、[メモリ ホット プラグ] セクションで [有効] チェック ボックスを選択解除します。

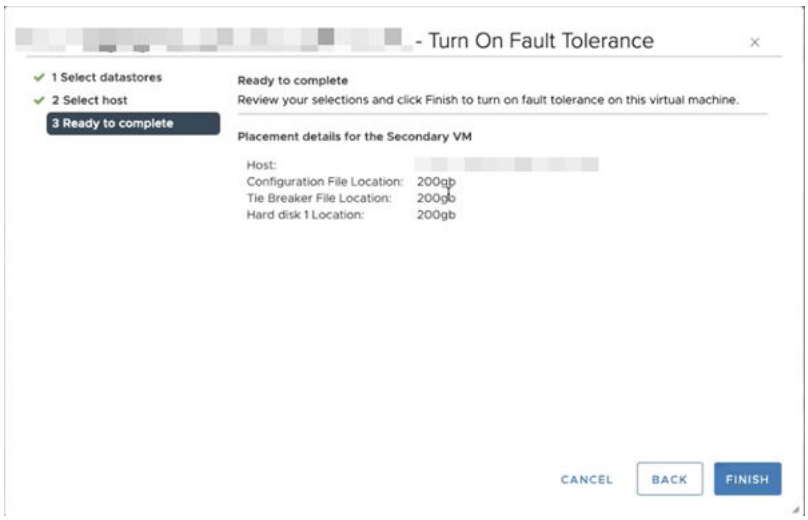
3 CD/DVD ドライブ 1 のホスト デバイスを選択します。

[CD/DVD ドライブ 1] セクションのドロップダウン メニューで、[ホスト デバイス] を選択します。

4 [OK] をクリックします。

2 セカンダリ データストアを選択して [次へ] をクリックし、セカンダリ ホストを選択して [次へ] をクリックし、選択内容を確認してから [終了] をクリックして、仮想マシンのフォルト トレランスを有効にします。

注意： 仮想マシンをデプロイしたときに選択したデータストアとは異なるデータストアを選択します。同じデータストアを選択すると、エラーが発生します。



Horizon Edge 仮想マシンのフォルト トレランスが正常に有効になりました。

3 vSphere Client を使用して、フォルト トレランスがクラスタ内のホスト全体に適用されることを確認します。

a 左側のペインで、プライマリ仮想マシンをデプロイしたホストを選択し、右側のペインで [仮想マシン] を選択して、Horizon 8 Edge 仮想マシンがプライマリ仮想マシンとして表示されていることを確認します。

名前には括弧内に「primary」が含まれます。たとえば、名前は「Example-2.3.2.0-XXX_OVF10（プライマリ）」と表示されることがあります。

b 左側のペインで、セカンダリ仮想マシンをデプロイしたホストを選択し、右側のペインで [仮想マシン] を選択して、Horizon 8 Edge 仮想マシンがセカンダリ仮想マシンとして表示されていることを確認します。

名前は、「secondary」という単語が括弧で表示されていることを除いて、プライマリ仮想マシンの名前と同じです。たとえば、「Example-2.3.2.0-XXX_OVF10（セカンダリ）」と入力します。

4 仮想マシンをパワーオンし、SSH を有効にして、すべてのポッドが起動してすべてのサービスが開始するまで待機します。

SSH を有効にする方法については、「Horizon Edge の SSH アクセスの有効化 」を参照してください

結果

フォルト トレランスが適切に構成されていると、プライマリ ホストが使用できなくなった場合に、セカンダリ仮想マシンが引き継ぎます。したがって、ダウンタイムなしでスイッチが発生し、すべてのサービスが問題なく実行し続けます。

プライマリ仮想マシンを含むホストで障害が自然に発生した場合、またはテスト環境で強制的に障害を発生させた場合は、次の動作が適用されます。

- プライマリ仮想マシンをデプロイしたホストを選択すると、Horizon 8 Edge 仮想マシンがセカンダリ仮想マシンとして表示されるようになりました。名前には、括弧内に「切断」と「セカンダリ」が含まれます。この手順で以前に使用した例に基づいて、名前は「Example-2.3.2.0-XXX_OVF10(切断、セカンダリ)」と表示されます。
- セカンダリ仮想マシンをデプロイしたホストを選択すると、Horizon 8 Edge 仮想マシンがプライマリ仮想マシンとして表示されるようになりました。名前には括弧内に「primary」が含まれます。この手順で以前に使用した例に基づいて、名前は「Example-2.3.2.0-XXX_OVF10(プライマリ)」と表示されます。

Horizon Edge の SSH アクセスの有効化

root ユーザーが Horizon Edge アプライアンスに接続できるように SSH を有効にできます。

手順

1. Horizon Edge アプライアンスが起動して実行されたら、Edge 仮想マシンの vCenter Server Web コンソールを起動します。
2. root ユーザーとしてログインし、パスワードを入力します。
3. コマンド **`/opt/vmware/bin/configure-adapter.py --sshEnable`** を実行し、完了するまで待機します。
4. **`vi /etc/ssh/sshd_config`** と入力します。
5. **`PermitRootLogin <other-value>`** 行を **`PermitRootLogin yes`** に変更します。
6. vim エディタで変更を保存します。
7. コマンド **`systemctl restart sshd`** を実行して、sshd デーモンを再起動します。
8. **`ssh root@<edge-appliance-ip>`** を使用して Edge アプライアンスに SSH 接続できます。

Horizon Cloud Service - next-gen を使用した Horizon 8 フェデレーション デプロイの構成

Horizon Cloud Service - next-gen を使用すると、Horizon Edge Gateway をダウンロードしてデプロイし、Amazon Web Services (AWS)、Microsoft Azure、および Google Cloud Platform (GCP) 環境へのフェデレーション クラウド デプロイ用に Horizon Edge を構成できます。

Horizon 8 フェデレーション デプロイ アーキテクチャは、パブリック クラウド プロバイダ環境で Horizon 8 を使用する場合にスケーラブルなソリューションを提供するように設計されています。これらのサポートされているクラウド環境でフェデレーション デプロイ アーキテクチャを使用するときの Horizon 8 ポッドと Horizon Edge Gateway の構成については、次の 3 つのトピックを参照してください。

Horizon Edge キャパシティ タイプの値を追加または編集する時のフェデレーション アーキテクチャの指定に関する関連情報については、「Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイ」の [キャパシティ プロバイダ] 設定に関する情報を参照してください。

Horizon 8 ポッド - VMware Cloud on AWS を使用したフェデレーション アーキテクチャ：Horizon Cloud Service - next-gen の環境への Horizon Edge Gateway のダウンロードとデプロイ

Horizon Edge Gateway をダウンロードして Amazon Web Services (AWS) の Horizon 8 フェデレーション デプロイにデプロイし、Horizon Cloud Service - next-gen とペアリングできます。

前提条件

次の手順に従って、VMware Cloud on AWS を使用したフェレデーション アーキテクチャを使用するポッド環境の Horizon Edge Gateway アプライアンスをダウンロードしてデプロイします。フェレデーション アーキテクチャでは、Horizon Cloud Service - next-gen のポッドの環境内のネイティブの Amazon Elastic Computer Cloud (EC2) インフラストラクチャに Horizon Edge Gateway をデプロイする必要があります。

- 「Horizon 8 Edge デプロイ」に記載されている Horizon Edge Gateway 関連の前提条件を満たしていることを確認します。
- Horizon Edge Gateway を使用して Horizon 8 ポッドを Horizon Cloud Service とペアリングするための「Horizon 8 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にする」を満たしていることを確認します。
- Horizon Edge Gateway 仮想アプライアンスは、インターネットにアクセスして Horizon Cloud 制御プレーンと通信する必要があります。ご使用の環境で、デプロイされたアプライアンスがインターネットにアクセスするためにプロキシ サーバとプロキシ構成を使用する必要がある場合、プロキシ設定を Horizon Edge Gateway アプライアンスで使用するときのプロキシ関連の情報、既知の制限、既知の問題を認識していることを確認します。
- pair-edge スクリプトの実行時にプロキシを使用する場合、まず次のコマンドを実行し、ProxySSL が有効な場合は *true*、それ以外の場合は *false* として指定する必要があります。

  ```
  /opt/vmware/bin/pair-edge-with-proxy.sh -i 'IP_or FQDN_of Proxy' -o 'Proxy_Port' -u
  'Proxy_User_Name' -p 'Proxy_Password' -s 'true_or_false' -c 'Connection_String'
  ```

  次の「注」でプロキシ関連の情報を確認してください。

  注： [Edge のプロキシ構成の更新]

  ```
  /opt/vmware/bin/configure-edge-webproxy.py --proxyHost 127.0.0.1 --proxyPort 3128 --
  proxyUsername 'exampleUsername' --proxyPassword 'examplePassword'
  ```

  その他のオプションを確認するには、次に示すように `-h` オプションを指定してスクリプトを実行します。

  ```
  /opt/vmware/bin/configure-edge-webproxy.py -h
  ```

- 多くの手順では、コマンドラインを使用する必要があります。ただし、AWS マネジメント コンソールまたは AWS コマンド ライン インターフェイス (CLI) を使用して実行できるデプロイ手順もあります。Amazon EC2 環境の操作の詳細については、https://docs.aws.amazon.com/ec2/index.html にある Amazon Elastic Compute Cloud のドキュメントを参照してください。以下の手順では、特定のタイプの Amazon Elastic Compute Cloud ドキュメントを参照することをお勧めすることがよくあります。

手順

1 Horizon Edge Gateway ディスク イメージをダウンロードします。このためには、*手順 7.[ダウンロード] を使用して、Horizon Edge Gateway アプライアンス バイナリを取得します。* の指示（Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイ ページの手順にある）に従って、画面上のすべてのプロンプトに応答します。

Horizon Edge Gateway ディスク イメージは VMDK ファイルとして使用できます。VMDK ファイルをローカル システムにダウンロードします。

注： `edge-gw-2.3.3.0-22720582.ec2.vmdk` など、バージョン 2.3.3.0 以降の Horizon Edge Gateway ディスク イメージをダウンロードします。

ダウンロードしたバイナリを目的の仮想化プラットフォームにデプロイする場所に保存し、この手順シーケンスに戻って必要なペアリング プロセスを続行します。

ディスク イメージ ファイルを Amazon EC2 環境にアップロードする前に、まず Amazon S3 バケットを作成する必要があります。

2 Amazon EC2 環境で Amazon S3 バケットを作成します。詳細な手順については、Amazon Elastic Compute Cloud のドキュメントを参照してください。

3 ダウンロードした VMDK ファイルを Amazon S3 バケットにアップロードします。この手順は、AWS マネジメント コンソールまたは AWS コマンドライン インターフェイス (CLI) を使用して実行できます。

- （AWS マネジメント コンソール）Amazon EC2 環境の AWS マネジメント コンソールにログインします。S3 サービスに移動し、以前に作成したバケットを選択し、そのバケットに VMDK ファイルをアップロードします。
- (AWS CLI) AWS CLI にアクセスし、次のコマンドを実行します。

```
aws s3 cp <file-path-to-VMDK-file> <S3URI>
```

`cp` コマンドの実行の詳細については、Amazon Elastic Compute Cloud のドキュメントを参照してください。

AWS マネジメント コンソールでは、VMDK ファイルは [オブジェクト] タブに表示されます。

4 サービス ロールとポリシーを作成し、ポリシーをロールに添付します。

a この手順に必要な 3 つの新しい JSON ファイルの最初のファイルを作成します。

この特定の JSON ファイルの目的は、サービスとロールの情報を格納することです。ファイルに任意の名前を付けます。この手順では、このファイルのファイル名の例は `trust-policy.json` です。

次のテキストは、JSON ファイルの内容の例です。

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"",
            "Effect":"Allow",
            "Principal":{
                "Service":"vmie.amazonaws.com"
            },
            "Action":"sts:AssumeRole",
            "Condition":{
                "StringEquals":{
                    "sts:ExternalId":"vmimport"
                }
            }
        }
    ]
}
```

b 任意の名前でサービス ロールを作成し、新しい JSON ファイルにロール情報を保存します。

たとえば、CLI を使用して、次のようなコマンドを実行します。

次のコマンドは一般的な例です。

```
aws iam create-role --role-name <role-name> --assume-role-policy-document <file-path>
```

次のコマンドの例では、プレースホルダ *<role-name>* を特定の例 `vmimport` に置き換え、プレースホルダ *<file-path>* を特定の例 `trust-policy.json` に置き換えています。

```
aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-
policy.json
```

`create-role` コマンドの実行の詳細については、Amazon Elastic Compute Cloud のドキュメントを参照してください。

c この手順に必要な 3 つの新しい JSON ファイルの 2 番目のファイルを作成します。

以下の例で使用する *<bucket-name>* など、VMDK ファイルをアップロードするバケットの名前を指定します。

この特定の JSON ファイルの目的は、新しいポリシーを新しいロールに添付することです。ファイルに任意の名前を付けます。この手順では、このファイルのファイル名の例は `role-policy.json` です。

次のテキストは、サンプルの `role-policy.json` ファイルの内容の例です。

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource":[
                "arn:aws:s3:::<bucket-name>"
            ]
        },
        {
            "Effect":"Allow",
            "Action":[
                "s3:GetObject"
            ],
            "Resource":[
                "arn:aws:s3:::<bucket-name>/*"
            ]
        },
        {
            "Effect":"Allow",
            "Action":[
                "ec2:ModifySnapshotAttribute",
                "ec2:CopySnapshot",
                "ec2:RegisterImage",
                "ec2:Describe*"
            ],
            "Resource":"*"
        }
    ]
}
```

d ポリシーを作成し、新しいロールに添付して、新しく作成した JSON ファイルに保存します。

たとえば、CLI を使用して、次のようなコマンドを実行します。

次のコマンドは一般的な例です。

```
aws iam put-role-policy --role-name <role-name> --policy-name <policy-name> --policy-
document <file-path>
```

次の具体例では、プレースホルダ *<role-name>* を、`vmimport` という名前のポリシーの具体例に置き換え、プレースホルダ *<policy-name>* を以前に名前を付けたロール、つまり `vmimport` という名前のロールの具体例に置き換え、プレースホルダ *<file-path>* を以前に名前を付けた JSON ファイル `role-policy.json` の具体例に置き換えます。

```
aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document
file://role-policy.json
```

`put-role-policy` コマンドの実行の詳細については、Amazon Elastic Compute Cloud のドキュメントを参照してください。

5 インポートされた VMDK ファイルからスナップショットをインポートします。

a この手順に必要な 3 つの新しい JSON ファイルの 3 番目のファイルを作成します。

このファイルに次の情報を含めます。

- バケット名（次の例で使用されている *<bucket-name>* など）。
- Amazon S3 バケットにアップロードした VMDK ファイルのファイル名（次の例で使用されている *<vmdk-file-name-uploaded-to-S3>* など）。

この特定の JSON ファイルの目的は、インポートされた VMDK ファイルのスナップショットを格納することです。ファイルに任意の名前を付けます。この手順では、このファイルのファイル名の例は `container.json` です。

次のテキストは、`container.json` ファイルの内容の例です。

```
{
    "Description": "Adapter-VM",
    "Format": "vmdk",
    "UserBucket": {
        "S3Bucket": "<bucket-name>",
        "S3Key": "<vmdk-file-name-uploaded-to-S3>"
    }
}
```

b コマンドを実行して、インポートした VMDK ファイルから新しく作成した JSON ファイルにスナップショットをインポートします。

CLI を使用して、次のタイプのコマンドを実行します。

```
aws ec2 import-snapshot --role-name <role-name> --description <description> --disk-
container <file-path>
```

`import-snapshot` コマンドの実行の詳細については、Amazon Elastic Compute Cloud のドキュメントを参照してください。

次のコマンドは、`import-snapshot` コマンドの具体例です。ここでは、`role-name` パラメータはオプションで使用されておらず、説明は `"Adapter-VM"` で、コンテナのファイル名は `container.json` です。

```
aws ec2 import-snapshot --description "Adapter-VM" --disk-container file://
container.json
```

`import-snapshot` コマンドは完了まで数分かかることがあります。ただし、コマンドを実行すると、コマンドの出力が作成されます。この出力には、タスクの進行状況の追跡に使用できる `ImportTaskId` 行が含まれています。次の出力に一例を示します。

```
{
    "ImportTaskId": "import-snap-05b4c84af4xxxxxxx",
    "Description": "Adapter-VM",
    "SnapshotTaskDetail": {
        "StatusMessage": "pending",
        "UserBucket": {
```

```
                "S3Bucket": "awsbucket",
               "S3Key": "edge-gw-2.3.3.0-22720582.ec2.vmdk"
           },
         "Progress": "0",
         "Status": "active",
          "Description": "Adapter-VM",
          "DiskImageSize": 0.0
     }

}
```

c import-snapshot コマンド出力の ImportTaskId 値を書き留めます。

6 import-snapshot タスクの進行状況を追跡し、スナップショット ID を取得するには、次のコマンドを実行します。

```
aws ec2 describe-import-snapshot-tasks --import-task-ids <import-task-id>
```

<import-task-id> プレースホルダを import-snapshot コマンド出力にリストされた値に置き換えます。上記の出力例にリストされている値の例は import-snap-05b4c84af4xxxxxxx です。describe-import-snapshot-tasks コマンドの実行の詳細については、Amazon Elastic Compute Cloud のドキュメントを参照してください。

describe-import-snapshot-tasks コマンドは、import-snapshot タスクの進行状況を示す出力を提供し、タスクが完了すると、イメージの登録に必要なスナップショット ID を提供します。次に例を示します。

- "Progress": "43"。この行のような出力の行は、import-snapshot タスクの進行状況の割合を示します。この例では、タスクは 43% 完了しています。
- "Status": "completed"。この行のような出力の行は、import-snapshot タスクが完了したことを示します。
- "SnapshotId": "snap-06d42e043bxxxxxxx"。タスクが完了すると、出力にこのような行が含まれます。この例では、スナップショット ID は snap-06d42e043bxxxxxxx です。

7 describe-import-snapshot-tasks コマンドの出力からスナップショット ID を書き留めます。

8 スナップショット イメージを登録するには、register-image コマンドを実行します。

```
aws ec2 register-image --region us-west-2 --name <image-name> --architecture x86_64 --root-
device-name '/dev/sda1' --virtualization-type hvm --ena-support --block-device-mappings
DeviceName=/dev/sda1,Ebs={SnapshotId=<SnapshotId>}
```

ここでは、--region、--architecture など、各オプションのデプロイに固有の応答を提供する必要があります。register-image コマンドの実行の詳細については、Amazon Elastic Compute Cloud のドキュメントを参照してください。

次の情報は、--name オプションと SnapshotId パラメータに固有です。

- --name - 文字列の制約に従って、イメージの名前を指定します。

- `SnapshotId` - `describe-import-snapshot-tasks` コマンド出力からのスナップショット ID を指定します。

`register-image` コマンドは、Amazon Machine Image (AMI) の ID を含む出力を提供します。次の例は、典型的な `register-image` 出力です。

```
{
        "ImageId": "ami-0721ee000321c4685"
    }
```

`register-image` コマンド出力に示されている AMI は、AWS マネジメント コンソールの AMI のリストの中にも表示されます。

9 Horizon Edge Gateway AMI インスタンスの作成と構成をサポートするには、次の例のような起動スクリプトを準備します。

```
#! /bin/bash
/usr/bin/python3 /opt/vmware/bin/configure-adapter.py --sshEnable
sudo useradd ccadmin
echo -e 'password\npassword' | passwd ccadmin
echo 'cs_ip cs_fqdn' >> /etc/hosts
```

この例では、スクリプトが次の構成をサポートしています。

- Horizon Edge Gateway アプライアンスへの SSH アクセスの有効化。
- 定義されたパスワード (<*Mypassword*>\n<*Mypassword*>) を使用したアプライアンス上での `ccadmin` ユーザー アカウントの作成。強力なパスワードを定義してください。強力なパスワードは 8 文字以上で、1 つ以上の数字、大文字と小文字、特殊文字を含める必要があります。
- Connection Server のホスト名 (*cs_fqdn*) から Connection Server の IP アドレス (*cs_ip*) への解決。

Horizon Edge Gateway AMI インスタンスを起動する次の手順で、このスクリプトをユーザー データに追加する必要があります。

10 Horizon Edge Gateway の AMI インスタンスを起動します。

注： インスタンスで十分な機能が提供されるようにするには、モデル c5.2xlarge 以上を使用します。

インスタンスは、AWS マネジメント コンソールまたは CLI を使用して起動できます。いずれの場合も、`register-image` コマンドの出力で提供される Amazon Machine Image (AMI) の ID を使用し、前の手順で準備した起動スクリプトをユーザー データに追加します。

注： ユーザー データは AMI インスタンスの最初の起動シーケンスでのみ実行されるため、この時点で起動スクリプトを追加する必要があります。

CLI を使用するには、Amazon Elastic Compute Cloud のドキュメントを参照して、`run-instances` コマンドの実行の詳細を確認してください。

AWS マネジメント コンソールを使用するには、Amazon Elastic Compute Cloud のドキュメントで詳細（インスタンスの起動ウィザードを使用したインスタンスの起動など）を参照してください。

AWS マネジメント コンソールを使用してインスタンスを起動する場合、イメージ ID で新しい AMI を探して、AMI を選択し、[起動] をクリックします。その後、デプロイの詳細を指定してウィザードを続行できます。

11 Horizon Edge Gateway AMI が起動したら、AMI インスタンスの構成を編集し、起動スクリプトを削除します。

12 Horizon Edge Gateway 仮想マシン AWS インスタンスに SSH 接続します。

CLI または AWS マネジメント コンソールを使用するには、インスタンスへの接続の詳細について、Amazon Elastic Compute Cloud のドキュメントを参照してください。ペアリング キーのコピー/貼り付けを許可するには、SSH を使用することをお勧めします。

詳細については、「Horizon Edge の SSH アクセスの有効化 」を参照してください。

関連情報については、AWS 製品ドキュメントの「Connect to your Linux instance」および「Connect to your Linux instance with EC2 Instance Connect」も参照してください。

13 次のコマンド形式を使用して pair-edge スクリプトを実行します。ここで、*pairing_code* は、「Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイ」で説明されている手順 9 のスクリーンショットからコピーしたペアリング コードです。

```
sudo /opt/vmware/sbin/pair-edge.sh 'pairing_code'
```

14 セキュリティを強化するには、これらの手順を完了したときに SSH を無効にすることを検討してください。

15 Horizon Universal Console に戻り、Horizon Connection Server の詳細の構成を完了します。Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイを参照してください。

Horizon 8 ポッド - Azure VMware ソリューションを使用したフェデレーション アーキテクチャ: Horizon Cloud Service - next-gen の環境への Horizon Edge Gateway のダウンロードとデプロイ

Horizon Edge Gateway をダウンロードして Azure VMware Solution の Horizon 8 フェデレーション デプロイにデプロイし、Horizon Cloud Service - next-gen とペアリングできます。

VMware Cloud on Microsoft Azure にフェデレーション アーキテクチャを使用するポッド デプロイ用の Horizon Edge Gateway アプライアンスをダウンロードしてデプロイします。フェデレーション アーキテクチャでは、ポッドの環境内のネイティブの Microsoft Azure インフラストラクチャに Horizon Edge Gateway をデプロイする必要があります。

以下は、ポッドの環境内のネイティブの Azure インフラストラクチャに Horizon Edge Gateway をデプロイするために必要な手順の概要です。

- Horizon Edge Gateway VHD ファイルをダウンロードします。
- Azure ストレージ コンテナを作成し、そのストレージ コンテナにアプライアンスの VHD をアップロードします。
- アップロードされた VHD から仮想マシン イメージを作成します。
- 仮想マシン イメージから Horizon Edge Gateway 仮想マシンを作成します。

前提条件

次の手順に従って、Azure VMware Solution (AVS) を使用したフェレデーション アーキテクチャを使用するポッド環境の Horizon Edge Gateway アプライアンスをダウンロードしてデプロイします。フェデレーション アーキテクチャでは、ポッドの環境内のネイティブの Microsoft Azure インフラストラクチャに Horizon Edge Gateway をデプロイする必要があります。

続行する前に、以下の前提条件を満たす必要があります。

- 「Horizon 8 Edge デプロイ」に記載されている Horizon Edge Gateway 関連の前提条件を満たしていることを確認します。
- Horizon Edge Gateway を使用して Horizon 8 ポッドを Horizon Cloud Service とペアリングするための「Horizon 8 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にする」を満たしていることを確認します。
- Horizon Edge Gateway 仮想アプライアンスは、インターネットにアクセスして Horizon Cloud 制御プレーンと通信する必要があります。ご使用の環境で、デプロイされたアプライアンスがインターネットにアクセスするためにプロキシ サーバとプロキシ構成を使用する必要がある場合、プロキシ設定を Horizon Edge Gateway アプライアンスで使用するときのプロキシ関連の情報、既知の制限、既知の問題を認識していることを確認します。

  注： [Edge のプロキシ構成の更新]

  ```
  /opt/vmware/bin/configure-edge-webproxy.py --proxyHost 127.0.0.1 --proxyPort 3128 --
  proxyUsername 'exampleUsername' --proxyPassword 'examplePassword'
  ```

  その他のオプションを確認するには、次に示すように `-h` オプションを指定してスクリプトを実行します。

  ```
  /opt/vmware/bin/configure-edge-webproxy.py -h
  ```

- ペアエッジ スクリプトの実行時にプロキシを使用するには、まず次のコマンドを実行し、ProxySSL が有効な場合は *true*、それ以外の場合は *false* として指定する必要があります。

  ```
  /opt/vmware/bin/pair-edge-with-proxy.sh -i 'IP_or FQDN_of Proxy' -o 'Proxy_Port' -u
  'Proxy_User_Name' -p 'Proxy_Password' -s 'true_or_false' -c 'Connection_String'
  ```

手順

1 Horizon Edge Gateway ディスク イメージをダウンロードします。このためには、*手順 7.[ダウンロード] を使用して、Horizon Edge Gateway アプライアンス バイナリを取得します。* の指示（Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイ ページの手順にある）に従って、画面上のすべてのプロンプトに応答します。

  Horizon Edge Gateway ディスク イメージは VHD ファイルとして使用できます。指定したとおりに VHD ファイルをローカル システムにダウンロードします。

  注： `edge-gw-2.3.3.0-22720582.azure.vhd.zip` など、バージョン 2.3.3.0 以降の Horizon Edge Gateway ディスク イメージをダウンロードします。

ダウンロードしたバイナリを目的の仮想化プラットフォームにデプロイする場所に保存し、この手順シーケンスに戻って必要なペアリング プロセスを続行します。

注： Horizon Edge Gateway とペアリングされた場合、以下の機能とサービスは AVS の Horizon ポッドでサポートされます。

- ライセンス
- 監視

ディスク イメージ ファイルを AVS 環境にアップロードする前に、まず Azure ストレージ コンテナを作成し、共有アクセス署名を使用して共有する必要があります。

2 Azure ポータルで、ストレージ アカウントに移動し、VHD ファイルのストレージ コンテナを作成します。詳細については、https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview を参照してください。

共有アクセス署名の作成時に、SAS トークンが生成されます。SAS トークンをストレージ コンテナの URL に追加して、ディスク イメージ ファイルのストレージ アカウント URL を作成する必要があります。

a [ストレージ アカウント] - [プロパティ] - [URL] の順に移動してストレージ コンテナを開きます。次の手順のために、ストレージ コンテナの URL をメモしておきます。

b 共有アクセス署名を作成します。[ストレージ アカウント] - [共有アクセス署名] - [リソース タイプを選択し、SAS と接続文字列を生成する] に移動します。次の手順のために、生成された SAS トークンをメモしておきます。

c 次の形式を使用して、ストレージ アカウントの URL を作成します。

<*StorageContainerPath*>/EdgeDiskImageName.vhd<*SAS-Token*>

次に、ストレージ アカウントの URL の例を示します。

```
https://azurestorage1.blob.core.windows.net/vmware/edge-
gw-2.3.3.0-22720582.azure.vhd.zip?
sv=2020-01-01&ss=bfqt&srt=sco&sp=rwdlapx&se=2020-01-01T12:00:00Z&st=2020-01-01T06:00:00
Z&spr=https&sig=dUPul74l4K0ah%2FdoCpaTTjY4t2Js8kBY%3D
```

3 作成したストレージ アカウント URL にディスク イメージ ファイルをアップロードします。

a AzCopy ユーティリティをダウンロードして、Horizon Edge Gateway ディスク イメージを含む VHD ファイルを抽出したローカル システムにインストールします。

AzCopy ユーティリティの詳細については、https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10 を参照してください。

b VHD ファイルをアップロードするには、AzCopy ユーティリティで次のコマンドを実行します。

azcopy cp *<Path to extracted VHD file>* "*<StorageAccountURL>*" --blob-type PageBlob

以下に、ローカル Windows コンピュータから発行されたアップロード コマンドの例を示します。

```
azcopy cp c:\edge-gw-2.3.3.0-22720582.azure.vhd.zip "https://
azurestorage1.blob.core.windows.net/vmware/edge-gw-2.3.3.0-22720582.azure.vhd?
sv=2020-01-01&ss=bfqt&srt=sco&sp=rwdlapx&se=2020-01-01T12:00:00Z&st=2020-01-01T06:00:00
Z&spr=https&sig=dUPul74l4K0ah%2FdoCpaTTjY4t2Js8kBY%3D" --blob-type PageBlob
```

4 アップロードされた VHD ファイルから仮想マシン イメージを作成します。

a Azure ポータルで、[イメージ] に移動し、新しい仮想マシン イメージを作成します。イメージの名前を入力し、ターゲットの場所とリソース グループを指定します。

b 以下のオプションを指定します。

- [OS タイプ] オプションを [Linux] に設定します。
- [仮想マシン生成] オプションを [Gen1] に設定します。

c ストレージ BLOB の場合は、作成したストレージ アカウントとコンテナを参照し、アップロードした VHD ファイルを選択します。

d [作成] をクリックして、VHD ファイルから仮想マシン イメージを作成します。

5 仮想マシン イメージからアプライアンス仮想マシンを作成して、Horizon Edge Gateway アプライアンスをデプロイします。

a Azure ポータルで、前の手順で作成した仮想マシン イメージを開きます。[仮想マシンの作成] をクリックします。

b 以下の設定を指定します。

- 新しい仮想マシンの名前を入力します。これは Horizon Edge Gateway アプライアンスのホスト名になります。
- [仮想マシンのサイジング] については、「Horizon 8 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にする」を参照してください。

c 管理者アカウントには、ユーザー名として **ccadmin** を指定します。アプライアンスへの SSH アクセスを許可するには、この **ccadmin** ユーザー アカウントを作成する必要があります。

d SSH アクセスには、[SSH パブリック キー] 認証方法を指定します。

注： SSH パブリック キーとパスワードの両方の認証方法がサポートされています。ただし、より強力なセキュリティを提供する SSH パブリック キーが推奨されます。

e [ファイアウォール] 設定には、次のポートを設定します。

- HTTPS 用のポート 443
- SSH 用のポート 22

アプライアンスのファイアウォールとプロキシ サーバを構成する場合は、特定のパブリック URL を許可するようにアプライアンスを構成する必要もあります。詳細については、「Microsoft Azure 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にする」を参照してください。

f [ネットワーク] 設定には、パブリック ネットワークを介してアプライアンスへのアクセスを許可する必要がある場合は、パブリック IP アドレスの割り当てを指定します。また、HTTPS および SSH のパブリック受信ポートを指定します。

g [仮想マシンのプロパティ] に移動して、アプライアンス仮想マシンの IP アドレスと FQDN をメモします。後でブラウザベースの Horizon Edge Gateway 構成ポータルにアクセスするときに、この情報が必要になります。

6 ご使用の環境で仮想アプライアンスがインターネットにアクセスするために HTTP プロキシ サーバを使用する必要がある場合は、このトピックの「前提条件」セクションの説明に従って、アプライアンスのプロキシ関連の設定を構成します。

7 コマンド ライン インターフェイスを使用して、Horizon Edge Gateway への SSH アクセスを許可します。詳細については、「Horizon Edge の SSH アクセスの有効化 」を参照してください。

8 Horizon Edge Gateway 仮想アプライアンスの完全修飾ドメイン名 (FQDN) でホスト名を解決する場合は、その FQDN を Horizon Edge Gateway アプライアンスの固定 IP アドレスにマッピングする正引き参照と逆引き参照のレコードを DNS サーバに作成します。

9 Horizon Edge Gateway 仮想マシン Microsoft Azure インスタンスに SSH 接続します。

詳細については、「Horizon Edge の SSH アクセスの有効化 」を参照してください。

インスタンスへの接続の詳細については、Microsoft Azure のドキュメントを参照してください。ペアリング キーのコピー/貼り付けを許可するには、SSH を使用することをお勧めします。

10 次のコマンド形式を使用して pair-edge スクリプトを実行します。ここで、*pairing_code* は、[6.Horizon Edge Gateway のデプロイとペアリング] ユーザー インターフェイス ページ（「Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイ」で説明）からコピーしたペアリング コードです。

```
/opt/vmware/sbin/pair-edge.sh 'pairing_code'
```

11 セキュリティを強化するには、これらの手順を完了したときに SSH を無効にすることを検討してください。

12 Horizon Universal Console に戻り、Horizon Connection Server の詳細の構成を完了します。Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイを参照してください。

Horizon 8 ポッド - Google Cloud VMware Engine を使用したフェデレーション アーキテクチャ：Horizon Cloud Service - next-gen の環境への Horizon Edge Gateway のダウンロードとデプロイ

Horizon Edge Gateway をダウンロードして Google Cloud Platform (GCP) の Horizon 8 フェデレーション デプロイにデプロイし、Horizon Cloud Service - next-gen とペアリングできます。

VMware Cloud on Google Cloud Platform にフェデレーション アーキテクチャを使用するポッド デプロイ用の Horizon Edge Gateway アプライアンスをダウンロードしてデプロイします。フェデレーション アーキテクチャでは、ポッドの環境内のネイティブ Google Cloud Platform (GCP) インフラストラクチャに Horizon Edge Gateway をデプロイする必要があります。

以下は、ポッドの環境内のネイティブの GCP インフラストラクチャに Horizon Edge Gateway をデプロイするために必要な手順の概要です。

- Horizon Edge Gateway TAR ファイルをダウンロードします。
- Google Cloud Storage バケットを作成し、アプライアンスの TAR をそのバケットにアップロードします。
- アップロードした TAR ファイルからカスタム イメージを作成します。
- カスタム イメージから Horizon Edge Gateway 仮想マシン (VM) インスタンスを作成します。

前提条件

続行する前に、以下の前提条件を満たす必要があります。

- 「Horizon 8 Edge デプロイ」に記載されている Horizon Edge Gateway 関連の前提条件を満たしていることを確認します。
- Horizon Edge Gateway を使用して Horizon 8 ポッドを Horizon Cloud Service とペアリングするための「Horizon 8 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にする」を満たしていることを確認します。
- Horizon Edge Gateway 仮想アプライアンスは、インターネットにアクセスして Horizon Cloud 制御プレーンと通信する必要があります。ご使用の環境で、デプロイされたアプライアンスがインターネットにアクセスするためにプロキシ サーバとプロキシ構成を使用する必要がある場合、プロキシ設定を Horizon Edge Gateway アプライアンスで使用するときのプロキシ関連の情報、既知の制限、既知の問題を認識していることを確認します。

  注： [Edge のプロキシ構成の更新]

  ```
  /opt/vmware/bin/configure-edge-webproxy.py --proxyHost 127.0.0.1 --proxyPort 3128 --
  proxyUsername 'exampleUsername' --proxyPassword 'examplePassword'
  ```

  その他のオプションを確認するには、次に示すように `-h` オプションを指定してスクリプトを実行します。

  ```
  /opt/vmware/bin/configure-edge-webproxy.py -h
  ```

- ペアエッジ スクリプトの実行時にプロキシを使用するには、まず次のコマンドを実行し、ProxySSL が有効な場合は *true*、それ以外の場合は *false* として指定する必要があります。

  ```
  /opt/vmware/bin/pair-edge-with-proxy.sh -i 'IP_or FQDN_of Proxy' -o 'Proxy_Port' -u
  'Proxy_User_Name' -p 'Proxy_Password' -s 'true_or_false' -c 'Connection_String'
  ```

- Google Cloud のグラフィカル ユーザー インターフェイス (GUI) または Google Cloud のコマンドライン インターフェイス (CLI) のいずれかを使用して、デプロイ手順の一部を実行できます。CLI を使用するには、必要なコンポーネントを最初にローカル システムにインストールする必要があります。
  - `gsutil` ツール。手順については、Google Cloud Storage のドキュメントを参照してください。
  - Google Cloud SDK。手順については、Google Cloud SDK のドキュメントを参照してください。

手順

1 Horizon Edge Gateway ディスク イメージをダウンロードします。このためには、*手順 7.[ダウンロード] を使用して、Horizon Edge Gateway アプライアンス バイナリを取得します。* の指示（Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイ ページの手順にある）に従って、画面上のすべてのプロンプトに応答します。

Horizon Edge Gateway ディスク イメージは TAR ファイルとして使用できます。指定したとおりに TAR ファイルをローカル システムにダウンロードします。

ダウンロードしたバイナリを目的の仮想化プラットフォームにデプロイする場所に保存し、この手順シーケンスに戻って必要なペアリング プロセスを続行します。

注： アプライアンスを GCVE 環境にデプロイするには、バージョン 2.3.3.0 以降の Horizon Edge Gateway ディスク イメージをダウンロードします。たとえば `edge-gw-2.3.3.0-22720582.google.tar.gz` です。

ディスク イメージ ファイルを GCVE 環境にアップロードする前に、まず Google Cloud Storage バケットを作成する必要があります。

2 GCVE 環境に Google Cloud Storage バケットを作成します。詳細な手順については、Google Cloud のドキュメントを参照してください。

3 ダウンロードした TAR ファイルを Google Cloud Storage バケットにアップロードします。Google Cloud のグラフィカル ユーザー インターフェイス (GUI) または Google Cloud のコマンドライン インターフェイス (CLI) のいずれかを使用して、この手順を実行できます。

- (GUI) GCVE 環境の Google Cloud Platform にログインします。[Cloud Storage] ページに移動し、以前に作成したバケットを選択し、そのバケットに TAR ファイルをアップロードします。
- (CLI) `gsutil` コンソールを開き、次のコマンドを実行します。

```
gsutil cp <file-path-to-TAR-file> gs://<bucket-name>
```

4 アップロードした TAR ファイルからカスタム イメージを作成します。

- (GUI) Google Cloud Platform で、[Compute Engine] - [イメージ] ページに移動します。イメージを作成するオプションを選択します。イメージの作成ページで、ソースとして [Cloud Storage] を指定し、バケット内でアップロードされた TAR ファイルを参照します。必要に応じて他のイメージ プロパティを指定し、イメージの作成に進みます。

  新しいイメージが [イメージ] リストに表示されていることを確認します。

- (CLI) `gsutil` コンソールで、次の例に類似したイメージ作成コマンドを実行します。

  ```
  gcloud compute --project <project-name> images create <image-name> --description
  <image-description> --source-uri <TAR-file-uri>
  ```

  注： 必要に応じて、適切なパラメータを使用してコマンドをカスタマイズできます。詳細については、Google Cloud SDK のリファレンス ドキュメントを参照してください。

5 Horizon Edge Gateway 仮想マシン インスタンスの作成と構成をサポートするには、次の例のような起動スクリプトを準備します。

```
#! /bin/bash
/usr/bin/python3 /opt/vmware/bin/configure-adapter.py --sshEnable
sudo useradd ccadmin
echo -e 'password\npassword' | passwd ccadmin
echo 'cs_ip cs_fqdn' >> /etc/hosts
```

この例では、スクリプトが次の構成をサポートしています。

- Horizon Edge Gateway アプライアンスへの SSH アクセスの有効化。
- 定義されたパスワード (*password*) を使用したアプライアンス上での `ccadmin` ユーザー アカウントの作成。
- Connection Server のホスト名 (*cs_fqdn*) から Connection Server の IP アドレス (*cs_ip*) への解決。

6 カスタム イメージから Horizon Edge Gateway 仮想マシン インスタンスを作成します。仮想マシンのサイズ設定またはマシン タイプに対して、最小で [n2-standard-8] を構成していることを確認します。

- (GUI) Google Cloud Platform で、[イメージ] ページに移動し、以前に作成したカスタム イメージを選択し、仮想マシン インスタンスを作成するオプションを選択します。仮想マシンのサイズ設定またはマシン タイプに対して、最小で [n2-standard-8] を指定し、起動ディスクとしてカスタム イメージを指定し、事前に準備した起動スクリプトを追加します。必要に応じて他の仮想マシン プロパティを指定し、仮想マシン インスタンスの作成に進みます。

  Horizon Edge Gateway 仮想マシンが仮想マシン インスタンスのリストに表示されることを確認します。

- (CLI) `gsutil` コンソールで、次の例に類似したインスタンス作成コマンドを実行します。

  ```
  gcloud compute --project <project-name> instances create <instance-name>
  --zone <zone> --machine-type <n2-standard-8-minimum> --network <network>
  --subnet <subnet> --maintenance-policy <maintenance-policy> --scopes <scope>
  --image <custom-TAR-image> --metadata startup-script=<startup-script>
  ```

  注： 必要に応じて、適切なパラメータを使用してコマンドをカスタマイズできます。詳細については、Google Cloud SDK のリファレンス ドキュメントを参照してください。

7 Horizon Edge Gateway 仮想マシンが起動したら、仮想マシン インスタンスの構成を編集し、起動スクリプトを削除します。

重要： 起動スクリプトをインスタンスから削除して、Horizon Edge Gateway が再起動するたびにスクリプトが実行されることがないようにする必要があります。

8 Horizon Edge Gateway 仮想マシン GCP インスタンスに SSH 接続します。

詳細については、「Horizon Edge の SSH アクセスの有効化 」を参照してください。

インスタンスへの接続の詳細については、Google Cloud のドキュメントを参照してください。ペアリング キーのコピー/貼り付けを許可するには、SSH を使用することをお勧めします。

9 次のコマンド形式を使用して pair-edge スクリプトを実行します。ここで、*pairing_code* は、[6.Horizon Edge Gateway のデプロイとペアリング] ユーザー インターフェイス ページ（「Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイ」で説明）からコピーしたペアリング コードです。

```
/opt/vmware/sbin/pair-edge.sh 'pairing_code'
```

10 セキュリティを強化するには、これらの手順を完了したときに SSH を無効にすることを検討してください。

11 Horizon Universal Console に戻り、Horizon Connection Server の詳細の構成を完了します。Horizon 8 のデプロイと Horizon Cloud Service - next-gen 制御プレーンで使用する Horizon Edge のデプロイを参照してください。

Microsoft Azure Edge のデプロイ

Microsoft Azure の Horizon Cloud Service - next-gen から Edge をデプロイするには、次のセクションの説明に従って Horizon Cloud 環境を設定し、管理者アカウントに送信された Horizon Cloud Service - next-gen ウェルカム メールを利用する必要があります。

Horizon Cloud Service - next-gen ウェルカム メールの利用方法については、「4 章 Horizon Cloud Service - next-gen 管理者のオンボーディング」を参照してください。

Active Directory ドメインと ID プロバイダを構成するには、「Edge デプロイの ID およびアクセス プロバイダ情報の設定」を参照してください。

Microsoft Azure Edge デプロイのネットワーク セットアップ

Horizon Cloud Service - next-gen で、DNS サーバ設定やネットワークおよびセキュリティ グループ ルールなどのネットワーク設定を構成します。

Horizon Edge デプロイ用の Microsoft Azure VNet での DNS サーバ設定の構成

Horizon Edge がデプロイされている VNet は、内部マシン名と外部名の両方を解決できる必要があります。内部仮想マシン (VM) 名を解決する機能は、Microsoft Azure 環境にデプロイされる仮想マシンでのサービスの Active Directory ドメイン参加の操作に必要です。

前提条件

- Microsoft Azure リージョンに、Horizon Edge インスタンスをデプロイするときに指定することを計画している VNet トポロジがあることを確認します。
- その VNet トポロジに対してユーザーまたはネットワーク チームが構成する DNS サーバ設定が、Active Directory および Microsoft Azure 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にするに一覧表示されたアドレスに到達して解決できることを確認します。

手順

1 Microsoft Azure ポータルの左側のナビゲーション バーから、仮想ネットワーク ([仮想ネットワーク]) をクリックし、Horizon Edge デプロイに使用する仮想ネットワークをクリックします。

2 [DNS サーバ]をクリックして、仮想ネットワークの DNS サーバ設定を表示します。

3 [カスタム] オプションを使用して、名前解決に使用する DNS サーバのアドレスを追加し、[保存] をクリックします。

Microsoft Azure リージョンのネットワーク設定の構成

Horizon Cloud Service - next-gen の場合、環境には Microsoft Azure リージョンでのサブネット サポートが必要です。これには、そのリージョンに Microsoft Azure 仮想ネットワーク (VNet) が存在する必要があります。

必要なサブネットに適用可能なアドレス空間を持つ VNet を Microsoft Azure リージョンに作成します。

Horizon Cloud Service - next-gen では、事前にサブネットを作成する必要があります。

VNet に、クラスレス インタードメイン ルーティング (CIDR) 形式の重複しないサブネット アドレス範囲を 3 つ作成します。次のサブネット要件が最小です。大規模な環境では、より大きなサブネットが必要になる場合があります。

手順

1 管理サブネット（/26 以上）を作成します。

Edge Gateway (AKS) をデプロイし、送信接続タイプとして NAT ゲートウェイを使用する場合は、NAT ゲートウェイを構成します。また、管理サブネットが次の IP アドレス範囲と競合しないことを確認します。

- 169.254.0.0/16
- 172.30.0.0/16

- 172.31.0.0/16
- 192.0.2.0/24

2 デスクトップ（テナント）サブネットを作成します。

プライマリ デスクトップ（テナント）サブネットの場合は、/27 の最小サブネットを作成しますが、デスクトップと RDS サーバの数に基づいて適切なサイズを設定します。必要に応じてサブネットを追加できます。

注： 内部ロード バランサを使用している場合は、デスクトップ仮想マシンのすべての仮想マシン サブネットが RFC1918 で説明されている IP アドレス範囲に含まれることを確認します。

3 DMZ サブネットを作成します。

Unified Access Gateway のクラスタ用に /27 の最小サブネットを作成します。

注： Unified Access Gateway をデプロイするには、3 つのサブネットが必要です。各 Unified Access Gateway 仮想マシンには、各サブネットから 1 つずつ、合計 3 つの NIC があります。外部ロード バランサ バックエンド プールは DMZ サブネット NIC に接続されます。内部ロード バランサ バックエンド プールは、デスクトップ サブネット NIC に接続されます。インターネットから DMZ ネットワークへの入力方向をブロックするネットワーク セキュリティ グループ (NSG) またはファイアウォール ルールがないことを確認します。VMware がデプロイする NSG は、NIC（サブネットではなく）に接続されている NSG のみであり、デフォルトで入力方向が許可されます。インターネットから DMZ NIC への受信トラフィックをブロックするファイアウォールまたは NSG ルールがあると、外部ロード バランサ経由で Unified Access Gateway に接続しようとしたときに問題が発生します。

NSG の関連情報については、「Microsoft Azure にデプロイされた Horizon Edge と Unified Access Gateway のデフォルトのネットワーク セキュリティ グループ ルールについて」を参照してください。

Microsoft Azure にデプロイされた Horizon Edge と Unified Access Gateway のデフォルトのネットワーク セキュリティ グループ ルールについて

Horizon Cloud Service - next-gen を使用して Microsoft Azure サブスクリプションに Horizon Edge と Unified Access Gateway を作成すると、いくつかのデフォルトのネットワーク セキュリティ グループが作成されます。これらのセキュリティ グループは、Microsoft Azure ポータルにログインしたときに表示され、指定されたとおりに維持する必要があります。

Microsoft Azure への Horizon Edge および Unified Access Gateway のデプロイの一環として、自動デプロイ プロセスは一連のネットワーク セキュリティ グループ (NSG) を作成し、それぞれの NSG を VMware によって制御される Horizon Edge および Unified Access Gateway 仮想マシンにある特定の個別のネットワーク インターフェイス (NIC) に関連付けます。このような Edge および UAG 関連の仮想マシンは、Edge Gateway の仮想マシンと、Edge が Unified Access Gateway で構成されている場合にデプロイされる仮想マシンです。

概要

Horizon Cloud Service - next-gen で、Edge デプロイヤは、Edge の設計とアーキテクチャに従って、適切なデプロイヤによって作成された NSG を適切な NIC に関連付けます。これらの NSG は NIC レベルで使用され、管理される特定のアプライアンス上の各 NIC が、NIC に接続されたサブネット上で標準のサービスおよび Edge 操作に対して管理されるアプライアンスが受信すべきトラフィックを受信し、アプライアンスが受信する必要のないすべてのトラフィックをブロックできるようにします。各 NSG には、各 NIC との間で許可されるトラフィックを定義する一連のセキュリティ ルールが含まれています。

ここで説明するデプロイヤによって作成された NSG は、Horizon Universal Console を使用して作成するときに Edge によってプロビジョニングされるベース仮想マシン、ファーム、および VDI デスクトップに使用される NSG とは異なります。

注： ここに記載されているデプロイヤで作成された NSG ルールは、サービスの構成要件です。自動的に作成され、Edge 仮想マシンの NIC に関連付けられている Horizon Cloud Service - next-gen NSG を削除または編集しないでください。

Horizon Cloud Service - next-gen によって作成された NSG とその内部のルールは、それらが接続されている特定の NIC および仮想マシンに固有であり、それらの NIC および仮想マシンの目的のために明示的に使用されます。これらの NSG またはルールに変更を加えたり、それらを他の目的に使用しようとすると、それらの NIC が接続されている同じサブネット上であっても、接続された NIC との間で必要なネットワーク トラフィックが中断される可能性が高くなります。その中断により、すべての Edge 操作が中断する可能性があります。これらの NSG のライフサイクルは Horizon Cloud Service - next-gen によって管理されており、それぞれに特定の理由があります。

これらのデプロイヤで作成された NSG はサービスの構成要件であるため、それらを変更または移動しようとすると Horizon Cloud Service - next-gen のサポートされていない使用および提供サービスの誤用と見なされます。

ただし、Edge の仮想マシン用に Horizon Cloud Service - next-gen によって自動作成および管理される Edge のリソース グループ外のリソース グループには、組織の独自のルールを含む独自の NSG を作成することができます。独自の NSG のルールは、Edge の仮想マシンの管理と操作に関する Horizon Cloud Service - next-gen の要件と競合しないようにする必要があります。このような NSG は、Edge で使用される管理サブネット、テナント サブネット、および DMZ サブネットに接続する必要があります。Horizon Cloud Service - next-gen によって管理されるリソース グループ内に独自の NSG を作成すると、それらのリソース グループの NSG が別のリソース グループにあるリソースに関連付けられている場合、Horizon Cloud Service - next-gen 管理対象リソース グループでの削除アクション中にエラーが発生します。

Microsoft Azure ドキュメントで説明するように、ネットワーク セキュリティ グループ (NSG) の目的は、セキュリティ ルールを使用して Microsoft Azure 環境のリソースとの間のネットワーク トラフィックをフィルタリングすることです。各ルールには、NSG が関連付けられているリソースに許可されるトラフィックを決定する、送信元、宛先、ポート、プロトコルなどの一連のプロパティがあります。Horizon Cloud Service - next-gen が自動的に作成し、制御される Edge 仮想マシンの NIC と関連付ける NSG には、Horizon Cloud Service - next-gen が、サービスの Edge の管理、進行中の Edge 操作の正しい実行、および Edge のライフサイクルの管理に必要と判断した特定のルールが含まれています。一般的に、これらの NSG で定義されている各ルールは、エンド ユーザーに仮想デスクトップを提供する VDI のユースケースなど、Horizon Cloud Service - next-gen サブスクリプションの標準的なビジネス目的を実現するサービス フルフィルメントの一部である Edge 操作のポート トラフィックを提供することを目的としています。詳細については、「Horizon 8 Edge をデプロイするためのポートとプロトコルの要件」を参照してください。

以下のセクションでは、これらのデプロイヤで作成された NSG で Horizon Cloud Service - next-gen が定義する NSG ルールが一覧表示されています。

デプロイヤが作成した NSG に関する一般的な事実

このリストは、デプロイヤが Edge 関連仮想マシン上の特定の NIC に関連付ける、デプロイヤによって作成されたすべての NSG に適用されます。

- これらの自動的に作成された NSG は、制御されたソフトウェア アプライアンスのセキュリティを確保するための NSG です。新しいソフトウェアがサブスクリプションに追加され、追加のルールが必要になると、これらの新しいルールがこれらの NSG に追加されます。
- Microsoft Azure ポータルの Unified Access Gateway では、NSG の名前にパターン `vmw-hcs-UUID` が含まれています。ここで *UUID* は Edge の識別子です。ただし、専用の VNet にデプロイされる外部ゲートウェイ構成用の NSG は除きます。その場合、ゲートウェイに関連する NSG の名前にはパターン `vmw-hcs-ID` が含まれています。ここで *ID* はその外部ゲートウェイのデプロイ ID です。

  注： 外部ゲートウェイ構成が別のサブスクリプションにデプロイされるシナリオで、そのサブスクリプションで事前に作成した既存のリソース グループにデプロイするオプションが使用される場合、ゲートウェイ コネクタの仮想マシンの管理 NIC の NSG には、`vmw-hcs-UUID` パターンの代わりにリソース グループの名前に基づいたパターンで名前が付けられます。たとえば、そのリソース グループに `hcsgateways` という名前を付けた場合、そのリソース グループで Horizon Cloud Service - next-gen は `hcsgateways-mgmt-nsg` という名前の NSG を作成し、その NSG をゲートウェイ コネクタ仮想マシンの管理 NIC に関連付けます。

  Horizon Edge Gateway の場合、NSG には名前付けパターン `aks-agentpool-ID-nsg` があります。`ID` は Microsoft Azure によって追加されたランダムな数字で、NSG は名前付けパターン `vmw-hcs-UUID-edge-aks-node` を持つリソース グループの一部です。ここで、`UUID` は Edge 識別子です。

  これらの識別子を見つけるには、管理コンソールの [キャパシティ] ページから Edge の詳細に移動します。

  注： Edge の外部 Unified Access Gateway でカスタム リソース グループを使用することを選択した場合、ゲートウェイ コネクタ仮想マシンのデプロイヤによって作成された NSG の名前には、パターン `vmw-hcs-ID` の代わりにそのカスタム リソース グループの名前が含まれます。たとえば、Edge の外部ゲートウェイに `ourhcspodgateway` という名前のカスタム リソース グループを使用することを指定した場合、デプロイヤが作成してゲートウェイ仮想マシンの NIC に関連付ける NSG の名前は `ourhcspodgateway-mgmt-nsg` になります。

- NSG は、関連付けられている仮想マシンおよび NIC と同じリソース グループにあります。たとえば、外部ゲートウェイが Edge の VNet にデプロイされ、デプロイヤによって作成されたリソース グループを使用している場合、外部 Unified Access Gateway 仮想マシンの NIC に関連付けられている NSG は、`vmw-hcs-UUID-uag` というリソース グループにあります。
- Horizon Cloud では、サービスの保守性を維持するために、必要に応じて新しいルールが追加されたり、既存のルールが変更されたりすることがあります。
- Edge の更新中、NSG とルールは保持されます。それらは削除されません。
- Horizon Cloud Service - next-gen ルールは優先度 1000 から始まり、優先度は通常 100 単位で増えます。Horizon Cloud Service - next-gen ルールは、優先度 3000 のルールで終了します。
- Microsoft Azure ドキュメントのトピック「IP アドレス 168.63.129.16 について」で説明するとおり、送信元 IP アドレス 168.63.129.16 に対する `AllowAzureInBound` ルールによって、NSG は Microsoft Azure プラットフォームからの受信通信を受け付けます。Edge に関連するすべての仮想マシンは、Microsoft Azure の

仮想マシンです。その Microsoft Azure ドキュメントのトピックで説明されているように、IP アドレス 168.63.129.16 は、Microsoft Azure クラウド プラットフォームがクラウド内のすべての仮想マシンに対して実行するさまざまな仮想マシン管理タスクを容易にします。例として、この IP アドレスを使用すると、仮想マシン内にある仮想マシン エージェントが Microsoft Azure プラットフォームと通信して、仮想マシンが準備完了状態にあることを簡単に通知できます。

- Microsoft Azure は、各 NSG が作成されると自動的にいくつかのデフォルトのルールを作成します。作成されるすべての NSG で、Microsoft Azure はいくつかのインバウンド ルールとアウトバウンド ルールを 65000 以上の優先度で作成します。このような Microsoft Azure のデフォルトのルールは、Microsoft Azure によって自動的に作成されるため、このドキュメント トピックでは説明しません。これらのデフォルトのルールの詳細については、Microsoft Azure ドキュメントのデフォルトのセキュリティ ルールトピックを参照してください。
- これらの NSG で定義されている各ルールは、エンド ユーザーに仮想デスクトップを提供する VDI のユースケースなど、Horizon Cloud Service - next-gen サブスクリプションの標準的なビジネス目的を実現するサービス フルフィルメントの一部である Edge 操作のポート トラフィックを提供することを目的としています。詳細については、「Horizon 8 Edge をデプロイするためのポートとプロトコルの要件」を参照してください。
- Edge を編集してファームおよび VDI デスクトップ割り当てで使用するための追加のテナント サブネットを指定する場合、Edge Gateway 仮想マシンのテナント サブネットに関連する NSG と Unified Access Gateway 仮想マシンの NIC のルールが更新され、追加のテナント サブネットが含まれるようになります。

Edge Gateway AKS デプロイヤによって作成された NSG

Edge Gateway AKS には、各仮想マシン インスタンスが管理サブネットに 1 つの NIC を接続する仮想マシン (VM) スケール セットがあります。Microsoft Azure は、特定の NSG を自動的に作成し、仮想マシン スケール セット インスタンスに関連付けられているすべての NIC に関連付けます。

Edge Gateway 仮想マシン タイプの場合、現在 NSG は作成されていません。

Microsoft Azure 環境では、Edge AKS NSG は Edge の aks ノード リソース グループに配置されます。このリソース グループは、`vmw-hcs-UUID-edge-aks-node` パターンで名前が付けられます。

NSG には `aks-agentpool-ID-nsg` というパターンで名前が付けられます。ここで、`ID` は Microsoft Azure によって割り当てられたランダムな数字です。

前述したように、Microsoft Azure は Microsoft Azure ドキュメントのトピック「デフォルトのセキュリティ ルール」で説明されているように、デフォルトで次の表に示すルールを作成します。

表 5-1. Edge Gateway AKS 仮想マシン スケール セット インスタンスの管理 NIC でデプロイヤによって作成された NSG ルール - 受信セキュリティ ルール

優先順位	名前	ポート	プロトコル	ソース	送信先	アクション
65000	AllowVnetInBound	任意	任意	VirtualNetwork	VirtualNetwork	許可
65001	AllowAzureLoadBalancerInBound	任意	任意	AzureLoadBalancer	任意	許可
65500	DenyAllInbound	任意	任意	任意	任意	拒否

表 5-2. Edge Gateway AKS 仮想マシン スケール セット インスタンスの管理 NIC でデプロイヤによって作成された NSG ルール - 送信セキュリティ ルール

優先順位	名前	ポート	プロトコル	ソース	送信先	アクション
65000	AllowVnetOutBound	任意	任意	VirtualNetwork	VirtualNetwork	許可
65001	AllowInternetOutBound	任意	任意	任意	インターネット	許可
65500	DenyAllOutbound	任意	任意	任意	任意	拒否

外部 Unified Access Gateway 仮想マシンのデプロイヤによって作成された NSG

外部 Unified Access Gateway 構成用の各仮想マシンには 3 つの NIC があり、それぞれ、管理サブネット、テナント サブネット、および DMZ サブネットに接続されています。デプロイヤは、これら 3 つの NIC にそれぞれ特定の NSG を作成し、各 NSG を適切な NIC に関連付けます。

- 管理 NIC には、名前が `vmw-hcs-`*`ID`*`-uag-management-nsg` というパターンの NSG があります。
- テナント NIC には、名前が `vmw-hcs-`*`ID`*`-uag-tenant-nsg` というパターンの NSG があります。
- DMZ NIC には、名前が `vmw-hcs-`*`ID`*`-uag-dmz-nsg` というパターンの NSG があります。

Microsoft Azure 環境では、これらの NSG には、パターン `vmw-hcs-`*`ID`*`-uag` の名前が付けられます。ここで、*ID* は、コンソールの Edge の詳細ページに表示される Edge の ID です。ただし、外部ゲートウェイが Edge の VNet とは別の専用の VNet にデプロイされている場合を除きます。外部ゲートウェイが専用の VNet にデプロイされている場合、*ID* は、Edge の詳細ページに表示される [デプロイ ID] 値になります。

表 5-3. 外部 Unified Access Gateway 仮想マシンの管理 NIC でデプロイヤによって作成された NSG ルール

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1000	AllowHttpsInBound	9443	TCP	管理サブネット	任意	許可	サービスが管理インターフェイスを使用してゲートウェイの管理設定を構成するため。Unified Access Gateway の製品ドキュメントで説明されているように、その管理インターフェイスはポート 9443/TCP にあります。
受信	1100	AllowAzureInBound	任意	任意	168.63.129.16	任意	許可	前の「一般的な事実」セクションおよび Microsoft Azure ドキュメントのトピック IP アドレス 168.63.129.16 について」で説明するように、仮想マシンが Microsoft Azure プラットフォームからの受信通信を受け付けるようにするため。

表 5-3. 外部 Unified Access Gateway 仮想マシンの管理 NIC でデプロイヤによって作成された NSG ルール（続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1200	AllowSshInBound	22	任意	管理サブネット	任意	許可	トラブルシューティングに必要な場合、VMware が仮想マシンへの緊急アクセスを実行するため。緊急アクセスには、事前にお客様の許可を得る必要があります。
受信	3000	DenyAllInBound	任意	任意	任意	任意	拒否	この NIC の受信トラフィックを前の行のアイテムに制限するためにデプロイヤによって追加されました。
送信	3000	DenyAllOutBound	任意	任意	任意	任意	拒否	この NIC からの送信トラフィックを拒否するためにデプロイヤによって追加されました。

表 5-4. 外部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1000	AllowAzureInBound	任意	任意	168.63.129.16	任意	許可	前の「一般的な事実」セクションおよび Microsoft Azure ドキュメントのトピック IP アドレス 168.63.129.16 について」で説明するように、仮想マシンが Microsoft Azure プラットフォームからの受信通信を受け付けるようにするため。
受信	1400	AllowPcoipUdpInBound	任意	UDP	テナント サブネット	任意	許可	このルールは、Horizon Agent を操作する Unified Access Gateway の標準構成をサポートします。デスクトップ仮想マシンとファーム仮想マシンの Horizon Agent は、UDP を使用して PCoIP データを Unified Access Gateway インスタンスに送信します。

表 5-4. 外部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	3000	DenyAllInBound	任意	任意	任意	任意	拒否	この NIC の受信トラフィックを前の行のアイテムに制限するためにデプロイヤによって追加されました。
送信	1000	AllowHttpsOutBound	443 8443	TCP	任意	テナント サブネット	許可	このルールは、Edge Gateway への新しいクライアント接続要求の目的で Edge Gateway 仮想マシンと通信する Unified Access Gateway インスタンスをサポートします。
送信	1100	AllowBlastOutBound	22443	任意	任意	テナント サブネット	許可	このルールは、デスクトップ仮想マシンまたはファーム仮想マシンの Horizon Agent への Horizon Client Blast Extreme セッションのユースケースをサポートします。

表 5-4. 外部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
送信	1200	AllowPcoipOutBound	4172	任意	任意	テナント サブネット	許可	このルールは、デスクトップ仮想マシンの Horizon Agent への Horizon Client PCoIP セッションのユースケースをサポートします。
送信	1300	AllowUsbOutBound	32111	TCP	任意	テナント サブネット	許可	このルールは、USB リダイレクト トラフィックのユースケースをサポートします。USB リダイレクトは、デスクトップ仮想マシンまたはファーム仮想マシンのエージェント オプションです。そのトラフィックは、デスクトップ仮想マシンまたはファーム仮想マシンの Horizon Agent へのエンドユーザー クライアント セッションにポート 32111 を使用します。

表 5-4. 外部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
送信	1400	AllowMmrOutBound	9427	TCP	任意	テナント サブネット	許可	このルールは、マルチメディア リダイレクション (MMR) およびクライアント ドライバ リダイレクション (CDR) トラフィックのユースケースをサポートします。これらのリダイレクションは、デスクトップ仮想マシンまたはファーム仮想マシンのエージェント オプションです。そのトラフィックは、デスクトップ仮想マシンまたはファーム仮想マシンの Horizon Agent へのエンドユーザー クライアント セッションにポート 9427 を使用します。

表 5-4. 外部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
送信	1500	AllowAllOutBound	任意	任意	任意	テナント サブネット	許可	複数のユーザー セッションをサポートする仮想マシンで実行している場合、Horizon Agent はセッションの PCoIP トラフィックに使用するさまざまなポートを選択します。これらのポートは事前に決定できないため、特定のポートに名前を付けてそのトラフィックを許可する NSG ルールを事前に定義することはできません。したがって、優先度 1200 のルールと同様に、このルールは、そのような仮想マシンとの複数の Horizon Client PCoIP セッションのユースケースをサポートします。
送信	3000	DenyAllOutBound	任意	任意	任意	任意	拒否	この NIC の送信トラフィックを前の行のアイテムに制限

表 5-4. 外部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
								するためにデプロイヤによって追加されました。

表 5-5. 外部 Unified Access Gateway 仮想マシンの DMZ NIC でデプロイヤによって作成された NSG ルール

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1000	AllowHttpsInBound	80 443	TCP	インターネット	任意	許可	このルールは、Horizon Client および Horizon Web Client からの外部エンド ユーザーの受信トラフィックが Edge Gateway へのログイン認証要求を要求することを提供します。デフォルトでは、Horizon Client および Horizon Web クライアントはこの要求にポート 443 を使用します。HTTPS ではなく HTTP をクライアントに入力するユーザーのための簡単なリダイレクト方法として、そのトラフィックはポート 80 に送信され、自動的にポート 443 にリダイレクトされます。
受信	1100	AllowBlastInBound	443 8443	任意	インターネット	任意	許可	このルールは、外部エンド ユーザーの Horizon Client から Blast トラフィックを受信する

表 5-5. 外部 Unified Access Gateway 仮想マシンの DMZ NIC でデプロイヤによって作成された NSG ルール（続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
								Unified Access Gateway インスタンスをサポートします。
受信	1200	AllowPcoipInBound	4172	任意	インターネット	任意	許可	このルールは、外部エンド ユーザーの Horizon Client から PCoIP トラフィックを受信する Unified Access Gateway インスタンスをサポートします。

表 5-5. 外部 Unified Access Gateway 仮想マシンの DMZ NIC でデプロイヤによって作成された NSG ルール（続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1300	AllowAzureInBound	任意	任意	168.63.129.16	任意	許可	前の「一般的な事実」セクションおよび Microsoft Azure ドキュメントのトピック IP アドレス 168.63.129.16 について」で説明するように、仮想マシンが Microsoft Azure プラットフォームからの受信通信を受け付けるようにするため。
受信	3000	DenyAllInBound	任意	任意	任意	任意	拒否	この NIC の受信トラフィックを前の行のアイテムに制限するためにデプロイヤによって追加されました。

内部 Unified Access Gateway 仮想マシンのデプロイヤによって作成された NSG

内部 Unified Access Gateway 構成用の各仮想マシンには 2 つの NIC があり、それぞれ、管理サブネットおよびテナント サブネットに接続されています。デプロイヤは、これら 2 つの NIC にそれぞれ特定の NSG を作成し、各 NSG を適切な NIC に関連付けます。

- 管理 NIC には、名前が `vmw-hcs-podUUID-uag-management-nsg` というパターンの NSG があります。
- テナント NIC には、名前が `vmw-hcs-podUUID-uag-tenant-nsg` というパターンの NSG があります。

Microsoft Azure 環境では、これらの NSG は名前が `vmw-hcs-podUUID-uag-internal` というパターンの Edge のリソース グループにあります。

表 5-6. 内部 Unified Access Gateway 仮想マシンの管理 NIC でデプロイヤによって作成された NSG ルール

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1000	AllowHttpsInBound	9443	TCP	管理サブネット	任意	許可	サービスが管理インターフェイスを使用してゲートウェイの管理設定を構成するため。Unified Access Gateway の製品ドキュメントで説明されているように、その管理インターフェイスはポート 9443/TCP にあります。
受信	1100	AllowAzureInBound	任意	任意	168.63.129.16	任意	許可	前の「一般的な事実」セクションおよび Microsoft Azure ドキュメントのトピック IP アドレス 168.63.129.16 について」で説明するように、仮想マシンが Microsoft Azure プラットフォームからの受信通信を受け付けるようにするため。

表 5-6. 内部 Unified Access Gateway 仮想マシンの管理 NIC でデプロイヤによって作成された NSG ルール（続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1200	AllowSshInBound	22	任意	管理サブネット	任意	任意	トラブルシューティングに必要な場合、VMware が仮想マシンへの緊急アクセスを実行するため。緊急アクセスには、事前にお客様の許可を得る必要があります。
受信	3000	DenyAllInBound	任意	任意	任意	任意	拒否	この NIC の受信トラフィックを前の行のアイテムに制限するためにデプロイヤによって追加されました。
送信	3000	DenyAllOutBound	任意	任意	任意	任意	拒否	この NIC からの送信トラフィックを拒否するためにデプロイヤによって追加されました。

表 5-7. 内部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1000	AllowAzureInBound	任意	任意	168.63.129.16	任意	許可	前の「一般的な事実」セクションおよび Microsoft Azure ドキュメントのトピック IP アドレス 168.63.129.16 について」で説明するように、仮想マシンが Microsoft Azure プラットフォームからの受信通信を受け付けるようにするため。
受信	1100	AllowHttpsInBound	80 443	TCP	VirtualNetwork	任意	許可	このルールは、Horizon Client および Horizon Web Client からの内部エンド ユーザーの受信トラフィックが Edge Gateway へのログイン認証要求を要求するために提供されます。デフォルトでは、Horizon Client および Horizon Web クライアントはこの要求にポート 443 を使用します。HTTPS

表 5-7. 内部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
								ではなく HTTP をクライアントに入力するユーザーのための簡単なリダイレクト方法として、そのトラフィックはポート 80 に送信され、自動的にポート 443 にリダイレクトされます。
受信	1200	AllowBlastInBound	443 8443	任意	VirtualNetwork	任意	許可	このルールは、内部エンド ユーザーの Horizon Client から Blast トラフィックを受信する Unified Access Gateway インスタンスをサポートします。
受信	1300	AllowPcoipInBound	4172	任意	VirtualNetwork	任意	許可	このルールは、内部エンド ユーザーの Horizon Client から PCoIP トラフィックを受信する Unified Access Gateway インスタンスをサポートします。

表 5-7. 内部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1400	AllowPcoipUdpInBound	任意	UDP	テナント サブネット	任意	許可	このルールは、Horizon Agent を操作する Unified Access Gateway の標準構成をサポートします。デスクトップ仮想マシンとファーム仮想マシンの Horizon Agent は、UDP を使用して PCoIP データを Unified Access Gateway インスタンスに送信します。
受信	3000	DenyAllInBound	任意	任意	任意	任意	拒否	この NIC の受信トラフィックを前の行のアイテムに制限するためにデプロイヤによって追加されました。

表 5-7. 内部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
送信	1000	AllowHttpsOutBound	443 8443	TCP	任意	テナント サブネット	許可	このルールは、Edge への新しいクライアント接続要求の目的で Edge Gateway 仮想マシンと通信する Unified Access Gateway インスタンスをサポートします。
送信	1100	AllowBlastOutBound	22443	任意	任意	テナント サブネット	許可	このルールは、デスクトップ仮想マシンまたはファーム仮想マシンの Horizon Agent への Horizon Client Blast Extreme セッションのユースケースをサポートします。
送信	1200	AllowPcoipOutBound	4172	任意	任意	テナント サブネット	許可	このルールは、デスクトップ仮想マシンの Horizon Agent への Horizon Client PCoIP セッションのユースケースをサポートします。

表 5-7. 内部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
送信	1300	AllowUsb OutBound	32111	TCP	任意	テナント サブネット	許可	このルールは、USB リダイレクト トラフィックのユース ケースをサポートします。USB リダイレクトは、デスクトップ仮想マシンまたはファーム仮想マシンのエージェント オプションです。そのトラフィックは、デスクトップ仮想マシンまたはファーム仮想マシンの Horizon Agent へのエンドユーザー クライアント セッションにポート 32111 を使用します。

表 5-7. 内部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
送信	1400	AllowMmrOutBound	9427	TCP	任意	テナント サブネット	許可	このルールは、マルチメディア リダイレクション (MMR) およびクライアント ドライバ リダイレクション (CDR) トラフィックのユースケースをサポートします。これらのリダイレクションは、デスクトップ仮想マシンまたはファーム仮想マシンのエージェント オプションです。そのトラフィックは、デスクトップ仮想マシンまたはファーム仮想マシンの Horizon Agent へのエンドユーザー クライアント セッションにポート 9427 を使用します。

表 5-7. 内部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
送信	1500	AllowAllOutBound	任意	任意	任意	テナント サブネット	許可	複数のユーザー セッションをサポートする仮想マシンで実行している場合、Horizon Agent はセッションの PCoIP トラフィックに使用するさまざまなポートを選択します。これらのポートは事前に決定できないため、特定のポートに名前を付けてそのトラフィックを許可する NSG ルールを事前に定義することはできません。したがって、優先度 1200 のルールと同様に、このルールは、そのような仮想マシンとの複数の Horizon Client PCoIP セッションのユースケースをサポートします。
送信	3000	DenyAllOutBound	任意	任意	任意	任意	拒否	この NIC の送信トラフィックを前の行のアイテムに制限

表 5-7. 内部 Unified Access Gateway 仮想マシンのテナント NIC でデプロイヤによって作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
								するためにデプロイヤによって追加されました。

Microsoft Azure Edge のデプロイ

このドキュメント ページでは、Horizon Edge を Microsoft Azure サブスクリプションにデプロイするために使用する Horizon Universal Console の Horizon Edge の追加 UI フローの手順について説明します。

概要

Horizon Edge は、シン Edge クラウド インフラストラクチャです。Microsoft Azure デプロイの場合、Azure サブスクリプションはプロバイダです。

環境が少なくとも 1 つの Active Directory ドメインと ID プロバイダで構成されると、コンソールによってこの [Horizon Edge を追加] UI フローが使用可能になります。

デプロイ タイプ

Microsoft Azure にデプロイされた Horizon Edge は、Edge Gateway (VM) 形式または Edge Gateway (AKS) 形式のいずれかを使用します。

必要な資質に基づいて、使用するタイプを決定します。

デプロイ タイプ	主な品質	詳細
AKS	■ 5,000 を超えるセッションをサポート ■ Azure Kubernetes サービスには、満たす必要がある Microsoft 関連の要件があります ■ SSO ログイン エクスペリエンスと監視データ収集は、障害が発生した場合に完全なフェイルオーバー機能を備えたこれらの機能の提供をサポートする複製されたサービスを介して処理されます。	AKS は、Microsoft Azure データセンターのエンタープライズ クラウド ネイティブ アプリケーションの Microsoft Azure 標準です。 AKS タイプは、クラスタ化されたアーキテクチャの Edge Gateway を提供し、SSO ログイン エクスペリエンスと監視データ収集をサポートする複製されたサービスを提供します。
仮想マシン	■ 最大 5,000 セッションをサポート ■ AKS タイプよりも Microsoft Azure サブスクリプションに関連する前提条件が少ない ■ デプロイされた仮想マシンが将来使用できない場合、結果の動作は次のようになります。 ■ エンド ユーザーはシングル サインオン (SSO) なしでログインする必要があります。 ■ 仮想マシンが使用できない間、デスクトップの監視データは記録されません。	AKS タイプよりも前提条件が少ないため、仮想マシン タイプのデプロイがより簡単ですが、デプロイされた仮想マシンが使用できなくなった場合は、次のようになります。 ■ エンド ユーザーには、SSO ログイン エクスペリエンスなしでログイン フローが表示されます。たとえば、Active Directory 資格情報を使用してログインする必要があります。 ■ Edge Gateway 仮想マシンに送信されるデスクトップの監視データは、仮想マシンが使用できない間は記録されません。

前提条件

コンソールでこれらの手順を実行する前に、ユーザーまたは IT チームが次の項目を完了していることを確認する必要があります。

重要： コンソール ユーザー インターフェイスで項目を選択すると、システムはその特定の項目が設定されていることを確認します。それらの要件が満たされていない場合、ユーザー インターフェイスの手順を完了できなくなります。

たとえば、AKS タイプをデプロイする場合、[クラスタ送信タイプ] で選択した NAT ゲートウェイが選択した [管理サブネット] に接続されていない場合、[デプロイ] をクリックすると、ユーザー インターフェイスにメッセージが表示され、それ以上の手順に進むことはできません。その時点で、ウィザードを終了し、NAT ゲートウェイを管理サブネットに接続する要件を満たしてから、ウィザードを最初からやり直す必要があります。

- Microsoft Edge をデプロイするための要件チェックリストを確認し、それらの要件が満たされていることを確認します。
- Microsoft Azure のデプロイ、Horizon Edge - デプロイの準備ページ内のハイパーリンクされたページで説明されている準備項目を確認し、それらの項目が完了していることを確認します。
- Azure サブスクリプション情報、ネットワーク情報、FQDN、および関連する項目を確認し、ウィザードのフィールドとリストで指定できるようにします。
- 必要な送信ポートが許可されていることを確認します。Microsoft Azure 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にするを参照してください。

- トラフィックのルーティングにプロキシ サーバを使用する場合は、Edge 管理サブネットを介してアクセスできる必要があります。
- この Horizon Edge のプライマリ プロバイダを Horizon Edge Gateway および Unified Access Gateway インスタンス専用にするか、プライマリ プロバイダがエンドユーザーのデスクトップとアプリケーションも提供するようにするかを決定します。

  注： プライマリ プロバイダをこの Horizon Edge のゲートウェイ アプライアンス専用にする場合は、デスクトップとアプリケーションのセカンダリ プロバイダを指定するウィザードの手順で Azure サブスクリプション情報が必要になります。

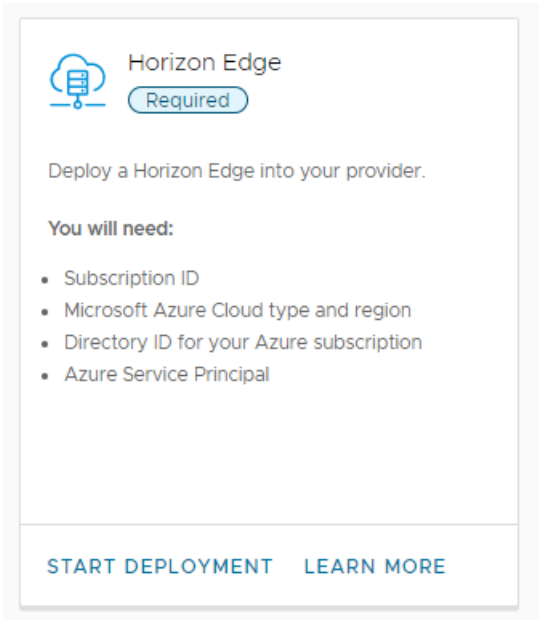
デプロイ ウィザードの開始

コンソールでは、[Horizon Edge を追加] ウィザードをさまざまなエントリ ポイントから使用できます。コンソールでのこの手順の開始点は通常、環境が新規であるか、Horizon 8 または Microsoft Azure 向けの Horizon Edge の既存のデプロイがあるかによって異なります。

Horizon Edge はまだありません - コンソールの Horizon Edge カードから開始します

環境に Horizon Edge がない場合、通常は [デプロイの開始] をクリックしてウィザードを開始します。

次のスクリーンショットは、この [Horizon Edge] カードを示しています。



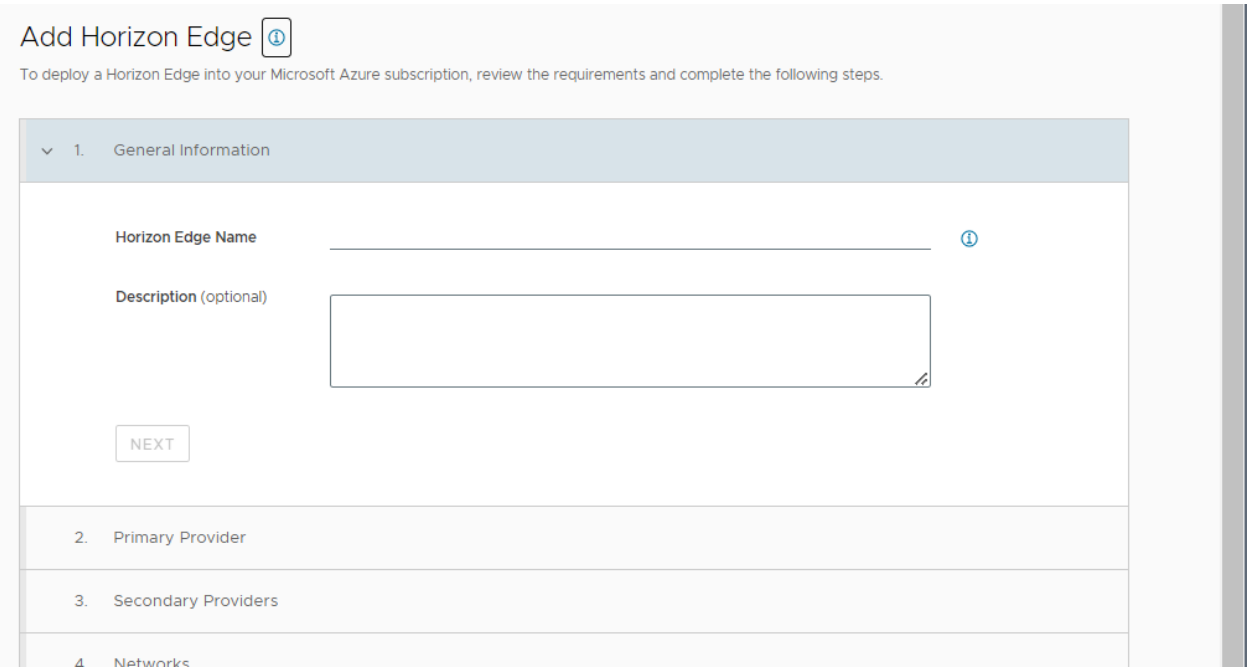
Horizon Edge がありません - 代わりに、コンソールの [キャパシティ] ページから開始します

環境に Horizon Edge がまだデプロイされていない場合、[キャパシティ] ページにはテキストと [開始] メニューが表示されます。このシナリオでは、ウィザードを開始するには、[リソース] - [キャパシティ] の順に移動し、[開始] - [Microsoft Azure] の順にクリックします。

少なくとも 1 台の Horizon Edge - コンソールの [キャパシティ] ページから開始します

環境に少なくとも 1 台の Horizon Edge がデプロイされている場合、[キャパシティ] ページには既存の Horizon Edge を一覧表示するグリッドが含まれます。このシナリオでは、ウィザードを開始するには、[リソース] - [キャパシティ] の順に移動し、[追加] - [Microsoft Azure] の順にクリックします。

これらの 3 つの方法のいずれかを使用してウィザードを開始すると、コンソールには [Horizon Edge を追加] ウィザードの手順 1 が表示されます。



全般情報

この Horizon Edge をコンソールに表示される他の Edge と区別する一意の [Horizon Edge 名] を追加します。オプションで説明を追加できます。

プライマリ プロバイダ

このセクションに入力します。この手順が完了したら、次の手順に進みます。

1 [Azure サブスクリプション] の場合、環境の既存のプロバイダの 1 つを選択するか、[新規追加] を使用して新しいプロバイダ サブスクリプション情報を提供します。

新しいプロバイダ サブスクリプション情報を追加する場合は、次の情報を指定します。

- コンソールに表示される他のプロバイダと区別する、このプロバイダの一意の名前。
- Microsoft Azure ポータルからの Microsoft Azure サブスクリプション ID。
- その Microsoft Azure サブスクリプション ID に適用可能な Azure クラウド タイプ、Azure リージョン、ディレクトリ ID を選択します。
- この目的のために Microsoft Azure ポータルで作成したサービス プリンシパルの情報（[アプリケーション ID] および [アプリケーション キー]）を指定します。

2 このプロバイダを Horizon Edge Gateway および Unified Access Gateway インスタンス専用にし、エンド ユーザーに使用資格が付与されたリソースを提供するために別のプロバイダを使用する場合は、表示されたチェックボックスをオンにします。

選択しない場合、このプロバイダはエンドユーザーに資格が付与されたリソースも提供します。

3 必要に応じて、ユーザー インターフェイスを展開してこのセクションを表示することで、この Horizon Edge のデプロイに使用する Azure リソース タグを指定できます。

4 必要に応じて、このユーザー インターフェイスの手順では、最大 4 つのサービス プリンシパル（[アプリケーション ID] と [アプリケーション キー] のペア）を追加できます。

セカンダリ プロバイダ

Horizon Edge へのセカンダリ プロバイダの追加はオプションです。

セカンダリ プロバイダは、プライマリ プロバイダと同じ Azure リージョンにある必要があります。

セカンダリ プロバイダごとに、最大 20,000 台の Horizon Edge の仮想マシンの合計キャパシティに対して、最大 5 つの一意のサービス プリンシパルを追加できます。

ネットワーク

[ネットワーク] セクションで、プライマリ プロバイダとセカンダリ プロバイダに使用するテナント（デスクトップ）サブネットを選択します。

後の段階でサブネットを選択できます。ただし、Horizon Edge に少なくとも 1 つのテナント サブネットが関連付けられるまで、システムはリソースをプロバイダにデプロイしないようにします。

サイト

[サイト] セクションで、環境内の既存のサイトから選択するか、[新規追加] を選択して新しいサイト情報を追加します。新しいサイトの場合は、一意の名前と、必要に応じて説明を入力します。

接続

[接続] セクションに必要な情報を入力します。この手順が完了したら、次の手順に進みます。

1 この Horizon Edge に使用するネットワーク接続のタイプ ([Azure Private Link] または [インターネット]) を選択します。

この要件の詳細については、「Microsoft Azure サブスクリプションの要件」を参照してください。

2 [App Volumes アプリケーション ストレージ] セクションで、Azure プライベート エンドポイントのサブネットを選択します。

注： プライベート エンドポイントを構成した後、エンド ユーザーは仮想マシンからログアウトし、再度ログインすることをお勧めします。

オプション	説明
[Edge Gateway 管理サブネットの使用]	プライベート エンドポイント リソースが作成される Edge Gateway 管理サブネット。 このデフォルト オプションを使用することをお勧めします。
[カスタム サブネットの構成]	前提条件が設定されていることを確認します。これらの前提条件の詳細については、「App Volumes アプリケーション ストレージ アカウントの Azure プライベート エンドポイント」を参照してください。 1 確認チェック ボックスを選択します。 2 [プライベート エンドポイントの vNet] ドロップダウンから仮想ネットワークを選択します。 3 [サブネット] ドロップダウンから対応するサブネットを選択します。

Horizon Edge がデプロイされ、プライベート エンドポイントが正常に作成されると、プライベート エンドポイントのステータスが `Configured` になります。ステータスが `Not Configured` の場合は、Horizon Edge の [App Volumes アプリケーション ストレージ] セクションの [プライベート エンドポイントの構成] オプションを使用して、プライベート エンドポイントを再度構成できます。このオプションの使用方法の詳細については、「Horizon Edge の詳細」の「App Volumes アプリケーション ストレージ アカウントのプライベート エンドポイントの構成」セクションを参照してください。

既存のデスクトップ プールとファイル共有の間にアプリケーションの提供に影響を与える接続の問題があり、これらの問題をトラブルシューティングするまでストレージ アカウントのパブリック ネットワーク アクセスに戻す場合は、[プライベート エンドポイントの削除] オプションを使用できます。このオプションは、構成済みのプライベート エンドポイントを削除し、Azure ポータルのストレージ アカウントのパブリック ネットワーク アクセスを自動的に有効にします。問題を修正したら、[プライベート エンドポイントの構成] オプションを使用してプライベート エンドポイントを構成できます。

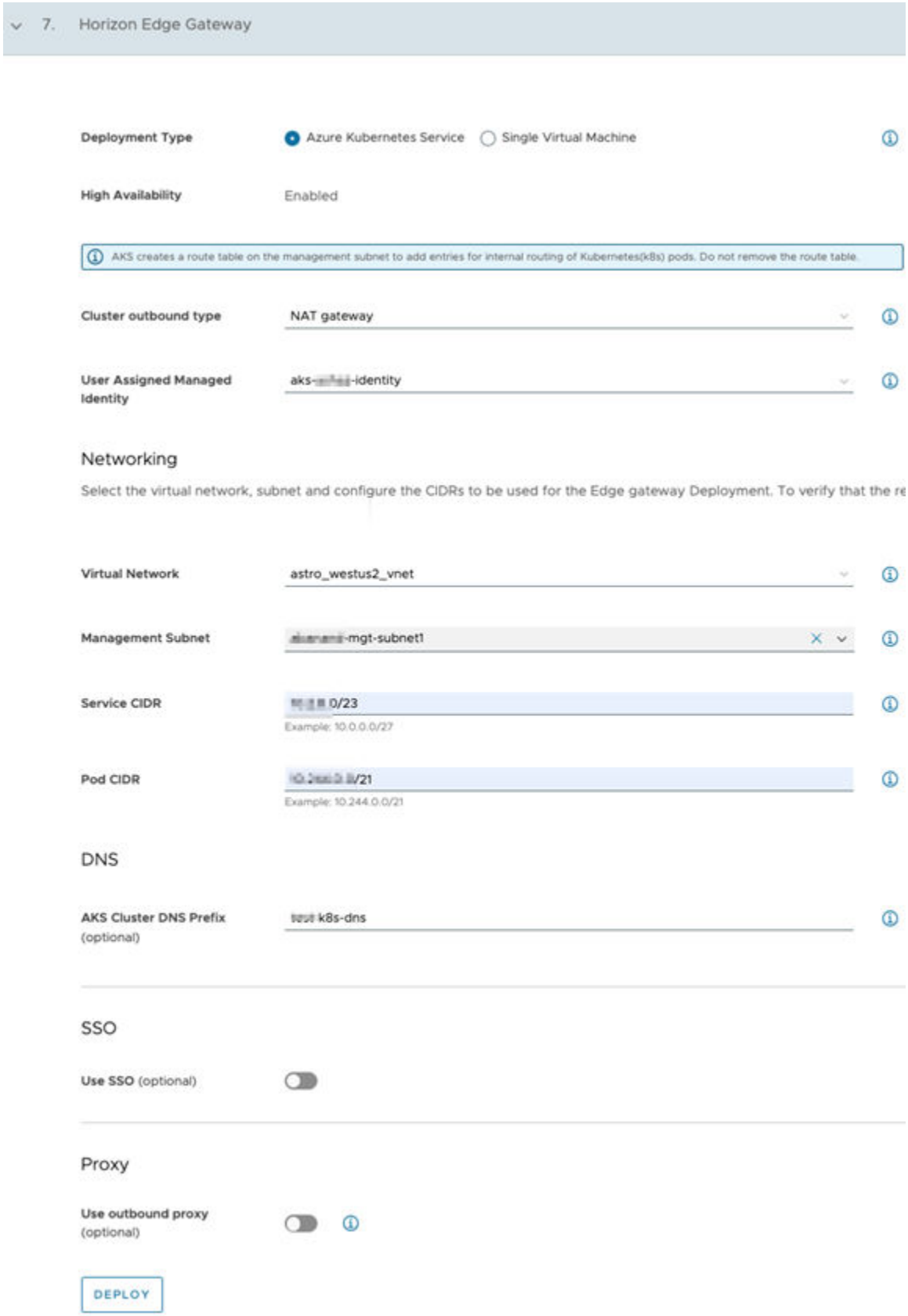
Horizon Edge Gateway

[Horizon Edge Gateway] セクションで、デプロイ タイプ（[Azure Kubernetes サービス] または [単一の仮想マシン]）を選択します。

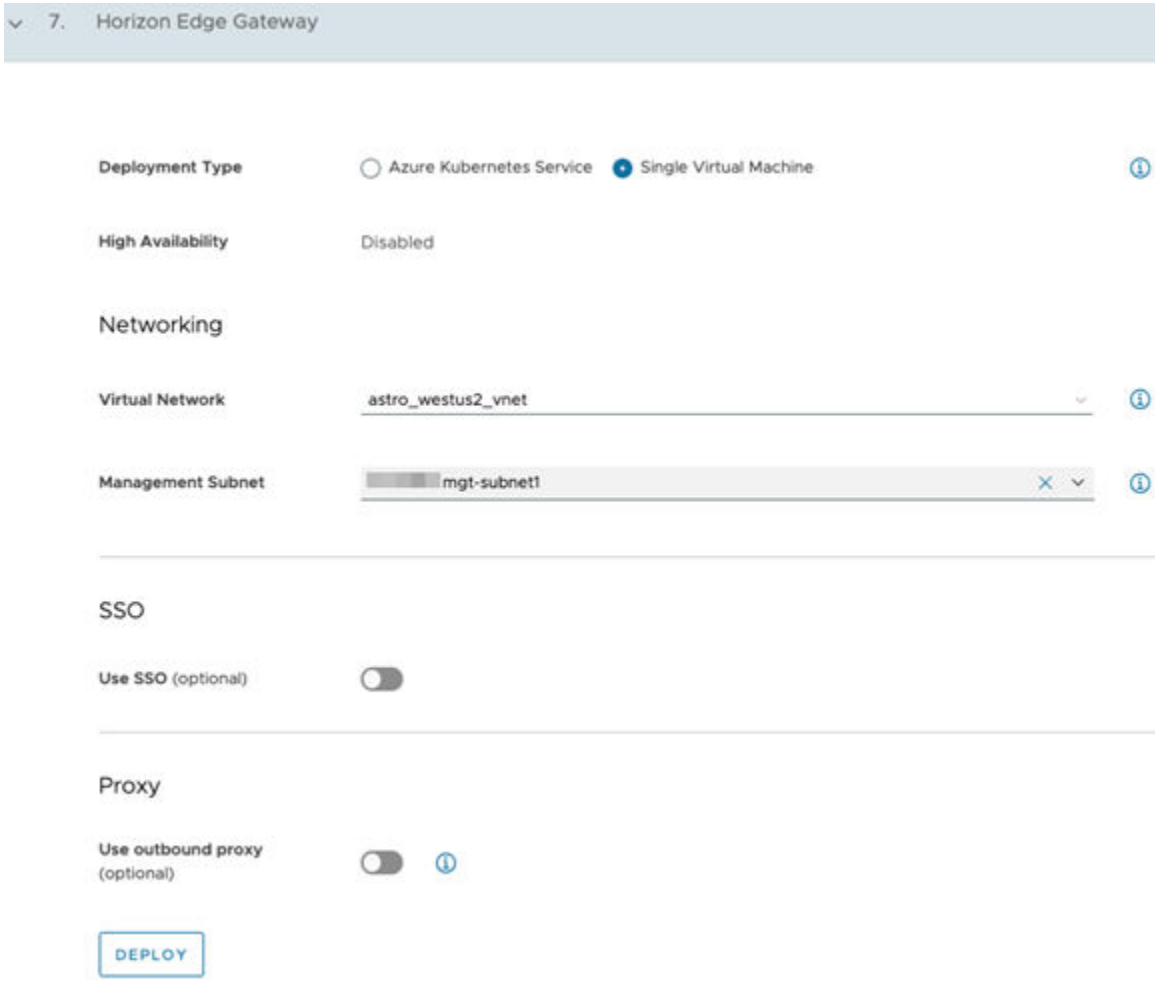
デプロイ タイプを選択したら、次のように、その特定のデプロイ タイプの手順を使用して Horizon Edge Gateway 設定を構成します。

選択した展開タイプに表示される UI フィールドを完了したら、画面のプロンプトに従います。

- [Azure Kubernetes サービス] - このオプションは Edge Gateway (AKS) 用です。次のスクリーンショットは、[Azure Kubernetes サービス] デプロイ タイプを選択したときに表示される情報および要求される情報のタイプを示しています。



- [単一の仮想マシン] - このオプションは Edge Gateway (VM) 用です。次のスクリーンショットは、[単一の仮想マシン] デプロイ タイプを選択したときに表示される情報および要求される情報のタイプを示しています。



注： ユーザー インターフェイスには、選択したデプロイ タイプに基づいて **高可用性** に関するラベルが表示されます。後で編集することはできません。単一仮想マシンのデプロイ タイプの場合、表示される文字列は、仮想マシンが使用できない場合、エンド ユーザーに SSO ログイン エクスペリエンスなしでログイン フローが表示され、仮想マシンが使用できない間はデスクトップの監視データが記録されないことを意味します。Azure Kubernetes サービスの展開タイプの場合、表示される文字列は、SSO ログイン エクスペリエンスと監視データ収集が、これらの機能の完全なフェイルオーバーを可能にする複製されたサービスを介して処理されることを意味します。

デプロイ タイプ	手順
Azure Kubernetes サービス (AKS)	[Azure Kubernetes サービス] オプションの場合 1 [NAT ゲートウェイ] と [ユーザー定義ルート] から [クラスタ送信タイプ] を選択します。 デフォルトの選択は、[NAT ゲートウェイ] です。[NAT ゲートウェイ] を選択すると、[NAT ゲートウェイ] を管理サブネットに関連付ける必要があります。[ユーザー定義ルート] を選択すると、ルート テーブルを管理サブネットに接続し、仮想アプライアンスのネクスト ホップ タイプを使用してデフォルト ルートを構成する必要があります。詳細については、ネットワーク要件を参照してください。また、必要なポートと URL がアクセス可能である必要があります。アクセスできない場合、AKS Edge のデプロイが失敗することがあります。詳細については、Microsoft Azure 環境に Horizon Edge Gateway をデプロイするために適切なターゲット URL をアクセス可能にするを参照してください。 AKS は、Kubernetes ポッドの内部ルーティングのために、管理サブネットのルート テーブルにエントリを追加します。エントリは削除しないでください。 [クラスタ送信タイプ] は、Horizon Edge の作成後に編集できません。 2 必要なロールを持つ [ユーザーが割り当てた管理対象 ID] を選択します。 [ユーザーが割り当てた管理対象 ID] の詳細については、Microsoft Azure Edge をデプロイするための要件チェックリストを参照してください。 3 [仮想ネットワーク] サブセクションで、サイトの仮想ネットワークを選択します。 利用可能な仮想ネットワークは、以前に選択した Microsoft Azure リージョンによって決まります。新しい仮想ネットワークを作成するには、Microsoft Azure ポータルに移動します。 4 Horizon Edge Gateway および Unified Access Gateway インスタンスに使用する [管理サブネット] を選択します。 AKS クラスタを使用する Horizon Edge は送信接続用に NAT ゲートウェイを必要とするため、選択した管理サブネットが NAT ゲートウェイで構成されていることを確認します。 **注意：** 選択した管理サブネットが別の AKS クラスタで使用されていないことを確認します。ネットワーク要件を参照してください。 5 [サービス CIDR] テキスト ボックスに、この CIDR の IP アドレス範囲を入力します。 少なくとも /27 の範囲を指定してください。この CIDR 範囲が、管理サブネットの仮想ネットワーク上にある、または接続されているネットワーク要素によって使用されていないことを確認します。この CIDR 範囲が、DNS サーバの IP アドレス、Active Directory サーバの IP アドレス、Unified Access Gateway の IP アドレスなどの他の重要な IP アドレスと競合しないことを確認します。 6 [ポッド CIDR] テキスト ボックスに、この CIDR の IP アドレス範囲を入力します。 少なくとも /21 の範囲を指定してください。この CIDR 範囲が、管理サブネットの仮想ネットワーク上にある、または接続されているネットワーク要素によって使用されていないことを確認します。この CIDR 範囲が、DNS サーバの IP アドレス、Active Directory サーバの IP アドレス、Unified Access Gateway の IP アドレスなどの他の重要な IP アドレスと競合しないことを確認します。 7 必要に応じて、デフォルトの [AKS クラスタ DNS プリフィックス] を調整します。 8 この Horizon Edge の一部であるリソースに対してシングル サインオンを有効にするには、[SSO を使用] を切り替えて、[SSO 構成] ドロップダウン メニューから適切な構成を選択します。 9 プロキシ サーバ経由で送信要求をルーティングするには、[送信プロキシを使用] を有効にします。 a プロキシ サーバの名前と IP アドレスを入力します。 b HTTP/TCP プロキシが HTTP/HTTPS トラフィックをリッスンするポート番号を入力します。 c SSL/TLS の安全な通信の証明書を追加するには、[SSL を有効にする] を選択します。 Horizon Cloud Service は SSL 認証のみをサポートします。ユーザー名とパスワードの認証はサポートされていません。 d プロキシ証明書をアップロードします。

デプロイ タイプ	手順
	Horizon Cloud Service は PEM 形式の証明書のみをサポートします。証明書は、廃止された共通名の代わりにサブジェクトの別名 (SAN) をサポートする必要があります。 10 [デプロイ] をクリックして、Horizon Edge 作成プロセスを有効にします。
単一の仮想マシン	[単一の仮想マシン] オプションの場合 1 [仮想ネットワーク] サブセクションで、サイトの仮想ネットワークを選択します。 利用可能な仮想ネットワークは、以前に選択した Microsoft Azure リージョンによって決まります。新しい仮想ネットワークを作成するには、Microsoft Azure ポータルに移動します。 2 Horizon Edge Gateway および Unified Access Gateway インスタンスに使用する [管理サブネット] を選択します。 3 この Horizon Edge の一部であるリソースに対してシングル サインオンを有効にするには、[SSO を使用] を切り替えて、[SSO 構成] ドロップダウン メニューから適切な構成を選択します。 4 プロキシ サーバ経由で送信要求をルーティングするには、[送信プロキシを使用] を有効にします。 a オプションで、別の Horizon Edge から [プロキシ設定] を選択します。 b プロキシ サーバの名前と IP アドレスを入力します。 c HTTP/TCP プロキシが HTTP/HTTPS トラフィックをリッスンするポート番号を入力します。 d オプションで、プロキシ サーバで認証情報が必要な場合は、[ユーザー名] および [パスワード] を入力します。 e SSL/TLS の安全な通信の証明書を追加するには、[SSL を有効にする] を選択します。 5 [デプロイ] をクリックして、Horizon Edge 作成プロセスを有効にします。

Unified Access Gateway

[Unified Access Gateway] セクションで、デプロイに必要なフィールドに入力します。

ユーザー インターフェイスのフィールドが完了したら、次の手順に進みます。

1 [アクセス タイプ] を選択します。

次の 3 つのオプションがあります。

- [企業のネットワーク経由の内部アクセス] - イントラネット（社内ネットワーク）経由でのみ仮想マシンにアクセスする場合。レイヤー 4 ロード バランサは、デスクトップ ネットワークにフロントエンドを使用してデプロイされます。
- [インターネット経由の外部アクセス] - インターネット経由で仮想マシンにアクセスする場合。レイヤー 4 ロード バランサは、パブリック IP アドレスを使用してデプロイされます。
- [内部および外部アクセス] - 内部および外部の両方のアクセスを許可します。

注： 3 つのすべてのオプションで、`*.horizon.vmware.com` への送信インターネット アクセスが引き続き必要です。Unified Access Gateway の要件を参照してください。[企業のネットワーク経由の内部アクセス] を使用する場合、ユーザー定義のルーティングまたは NAT ゲートウェイのいずれかを [管理サブネット] に適用して送信トラフィックを許可できます。外部アクセスが DMZ ネットワークを使用して外部に構成されている場合は、DMZ ネットワーク上で `*.horizon.vmware.com` への外部アクセスを構成する必要があります。

2 UAG の [自動パブリック IP アドレス] を有効にするにはトグルをオンに切り替え、手動パブリック IP アドレスを使用する場合はオフに切り替えます。

トグルはデフォルトでオンになっています。手動のカスタム IP アドレスが選択されている場合、外部 UAG は DMZ ネットワーク上にプライベート フロントエンド IP アドレスを使用してデプロイされます。次に、このプライベート IP アドレスからユーザーが提供したパブリック IP アドレスへのルーティングを行う必要があります。

Unified Access Gateway デプロイの FQDN を指定します。

3 [証明書タイプ] フィールドで、ドロップダウン メニューから [PEM] と [PFX] のいずれかを選択します。

4 [証明書] フィールドで、クライアントが Microsoft Azure の Unified Access Gateway との接続を信頼できる証明書をアップロードします。

5 メニューの使用可能な仮想マシン モデルから [仮想マシン モデル] を選択します。

6 [UAG 仮想マシン] フィールドに値を追加します。

7 [保存] をクリックします。

次の手順

この手順を完了したら、Unified Access Gateway インスタンスに対して入力した FQDN に一致する DNS レコードを作成する必要があります。Horizon Edge Gateway および Unified Access Gateway のデプロイ後に必要な DNS レコードを構成するを参照してください。

注： Horizon Cloud デプロイを完了し、デスクトップまたはアプリケーションの使用資格をエンド ユーザーに付与したら、次の Unified Access Gateway の動作が Horizon HTML Access（Web クライアント）を使用するエンド ユーザーに与える影響とメリットについて理解しておく必要があります。

Unified Access Gateway 2203.1 以降では、Unified Access Gateway インスタンスがメンテナンス モードになるか、または健全でない状態になり、アクセスできなくなった場合、Horizon HTML Access を使用するエンド ユーザーの進行中のセッションは健全な Unified Access Gateway インスタンスに再接続します。再接続には数分かかることがあります。

Unified Access Gateway の SSL 証明書を更新すると、エンド ユーザー セッションが終了します。

Horizon Edge および Unified Access Gateway の編集

Horizon Cloud Service - next-gen を使用して Horizon Edge および Unified Access Gateway をデプロイした後、一部のフィールドを編集できます。

Edge の編集中に、プロキシ サーバを介してインターネットへの送信要求をルーティングするように選択できます。プロキシの詳細を編集すると、Edge が再デプロイされる場合があります。これは、再デプロイが完了するまで、次のサービスの 1 つ以上に影響する可能性があります。

- デスクトップ接続用のシングル サインオン。

  ユーザー名とパスワードを使用してデスクトップに接続することは可能です。

- Unified Access Gateway の証明書の更新。
- Workspace ONE Intelligence のデータ損失の監視。
- エージェント DCT（データ収集ツール）のログ収集。
- ファイル共有間での App Volumes アプリケーションの追加とレプリケーション。

- 可用性監視でのシミュレートされたリソース起動タイプの構成済みのテストは、再デプロイ プロセスで失敗します。

手順

1 Horizon Universal Console にログインします。

2 [Horizon Edge] タイルで [Horizon Edge] をクリックします。

3 [キャパシティ] ページで、編集する [Horizon Edge] を選択し、[編集] をクリックします。

4 [全般情報] セクションで Horizon Edge の [名前] および [説明] を [編集] できます。[次へ] をクリックします。

5 プライマリ プロバイダを Horizon Gateway アプライアンス（Horizon Edge Gateway と Unified Access Gateway）のデプロイ専用にするには、[チェックボックス]を選択します。

チェックボックスが選択されていない場合、プロバイダはデスクトップとアプリケーションも提供します。

6 オプションで、最大 10 個の [Azure リソース タグ] の名前と値のペアを追加できます。

7 最大 4 つの [追加のサービス プリンシパル] を追加することもできます。

8 また、[セカンダリ プロバイダ] をこの Horizon Edge に追加し（プロバイダごとに最大 5 つの一意のサービス プリンシパル）、Horizon Edge の最大合計キャパシティ（20,000 台の仮想マシン）を実現することもできます。[次へ] をクリックします。

9 [ネットワーク] セクションで、[プライマリ プロバイダ] および [セカンダリ プロバイダ] のテナント（デスクトップ）サブネットを [選択] または [編集] します。[次へ] をクリックします。

後の段階でサブネットを選択できます。ただし、少なくとも 1 つのサブネットを選択するまで、プロバイダにリソースをデプロイすることはできません。

10 [サイト] を選択するか、サイトの [新規追加] を選択します。

11 新しいサイトを追加する場合は、[サイト名] を入力します。必要に応じて、[説明] を追加します。[次へ] をクリックします。

12 [接続] セクションで [次へ] をクリックします。

13 [Horizon Edge Gateway] セクションで、次の手順に従って、目的と選択したデプロイのタイプ（[Azure Kubernetes サービス] または [単一の仮想マシン]）に応じて Horizon Edge Gateway 設定を適切に編集します。

注： Edge Gateway (AKS) をデプロイし、高可用性を有効にしなかった場合は、[高可用性を有効にする] トグルを今すぐ有効にします。

a この Horizon Edge の一部であるリソースに対してシングル サインオンを有効にするには、[SSO を使用] を切り替えて、[SSO 構成] ドロップダウン メニューから適切な構成を選択します。

b 必要に応じて、プロキシ設定を再構成します。

重要： [送信プロキシを使用] トグルを有効にすると、再デプロイが完了するまで、次の 1 つ以上のサービスに影響する可能性があります。

- デスクトップ接続用のシングル サインオン。

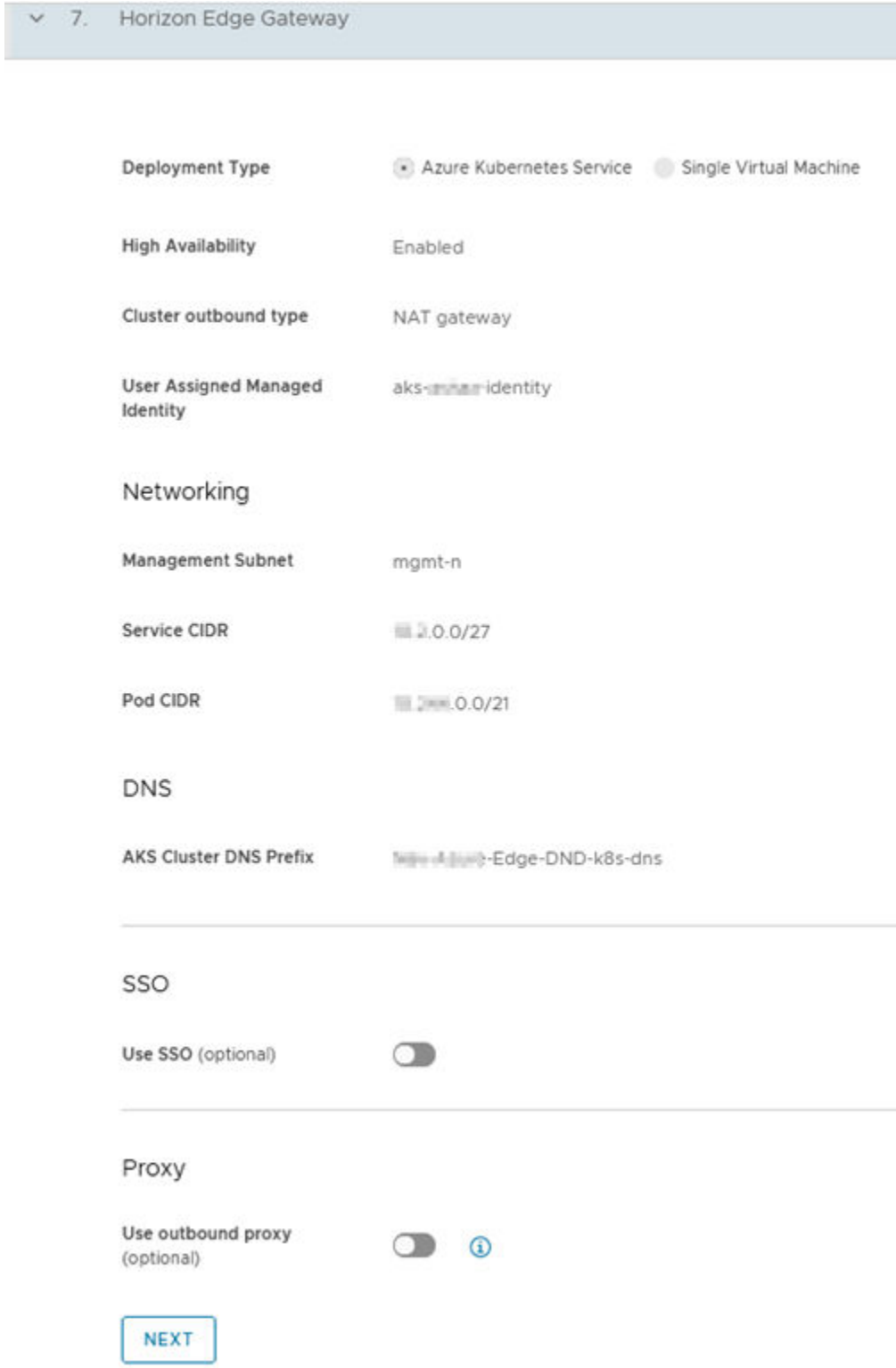
  ユーザー名とパスワードを使用してデスクトップに接続することは可能です。
- Universal Access Gateway の証明書の更新。
- Workspace ONE Intelligence のデータ損失の監視。
- エージェント DCT（データ収集ツール）のログ収集。
- ファイル共有間での App Volumes アプリケーションの追加とレプリケーション。
- 可用性監視でのシミュレートされたリソース起動タイプの構成済みのテストは、再デプロイ プロセスで失敗する場合があります。

c [次へ] をクリックします。

[デプロイ タイプ] および [高可用性] オプションなど、ほとんどのオプションは編集できません。

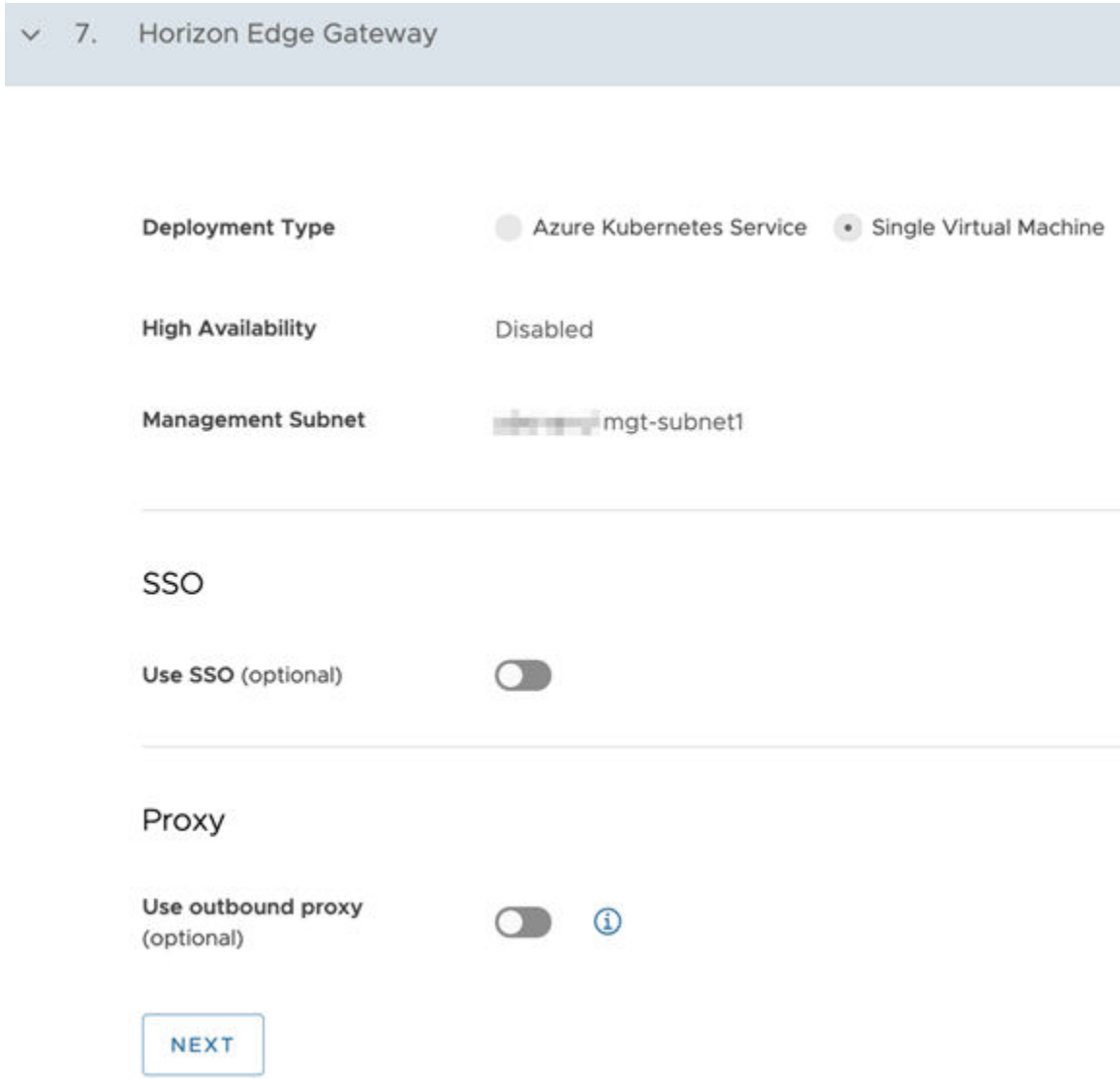
- [Azure Kubernetes サービス]

  このオプションは、Edge Gateway (AKS) 用です。次のスクリーンショットは、[Azure Kubernetes サービス] デプロイ タイプを選択したときに表示される情報のタイプを示しています。



- [単一の仮想マシン]

  このオプションは、Edge Gateway (VM) 用です。次のスクリーンショットは、[単一の仮想マシン] デプロイ タイプを選択したときに表示される情報のタイプを示しています。



14 [Unified Access Gateway] セクションで、UAG の [自動パブリック IP アドレス] を有効にするにはトグルをオンに切り替え、手動パブリック IP アドレスを使用する場合はオフに切り替えます。

トグルはデフォルトでオンになっています。手動のカスタム IP アドレスが選択されている場合、外部 UAG は DMZ ネットワーク上にプライベート フロントエンド IP アドレスを使用してデプロイされます。次に、このプライベート IP アドレスからユーザーが提供したパブリック IP アドレスへのルーティングを行う必要があります。

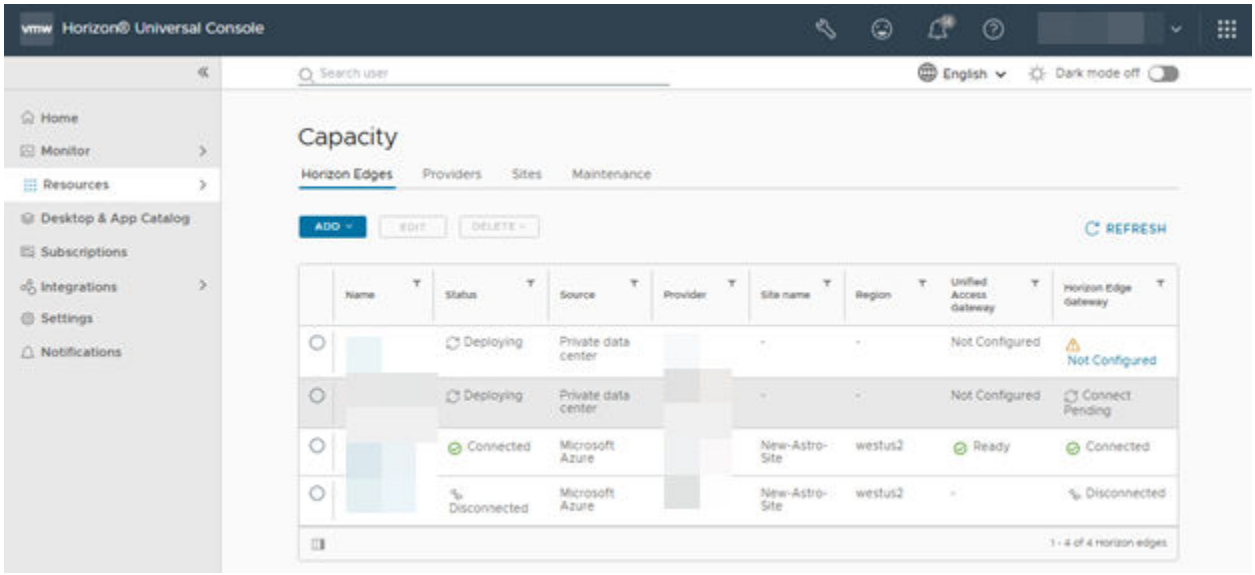
15 [保存] をクリックします。

Horizon Edge の詳細

1 つ以上の Horizon Edge を追加したら、Horizon Universal Console を使用して Horizon Edge ページに移動し、Horizon Edge のリストに関する一般的なデータを表示できます。特定の Horizon Edge の名前をクリックして、その特定の Horizon Edge に関する詳細情報を表示することもできます。

デプロイされた Horizon Edge の表示と特定の Horizon Edge に対するアクションの実行

Horizon Edge ページには、環境内の各 Horizon Edge に関する基本情報が表示されます。このページでは、Horizon Edge を追加、編集、および削除することもできます。



Horizon Edge ページを表示するには、[リソース] - [キャパシティ] を選択します。

Horizon Edge ページには、Horizon Edge のテーブルが表示されます。

ヒント:

- [名前]、[ステータス]、[Horizon Edge Gateway] など、テーブルの列見出しにある多くのフィルタのいずれかを使用して、ページに Horizon Edge が表示される方法を変更できます。
- [ステータス] 列には、各 Horizon Edge のデプロイのステータスが表示されます。
- [Horizon Edge Gateway] 列には、各 [Horizon Edge Gateway] のステータスが表示されます。
- [Unified Access Gateway] 列には、各 [Horizon Edge Gateway] に関連付けられている Unified Access Gateway のステータスが表示されます。
- [ソース] 列には、Horizon Edge ごとのプロバイダ タイプが一覧表示されます。たとえば、「Microsoft Azure」は Microsoft Azure Edge に対して、「プライベート データセンター」は Horizon 8 Edge に対してそれぞれ表示されます。[ソース] 列に表示されるプロバイダ タイプは、持っているライセンスのタイプと、以前にデプロイした Horizon Edge のタイプによって異なります。

プロバイダ

Horizon Edge、イメージ、またはプールに関連付けられているプロバイダ タイプを追加または編集できます。

1 Horizon Universal Console にログインします。

   - Horizon Edge：[リソース] - [キャパシティ] - [プロバイダ] - [追加] の順に移動し、ドロップダウン リストからプロバイダ タイプを選択します。
   - イメージ：[イメージ] をクリックし、次に [開始] をクリックして、ドロップダウン リストからプロバイダを選択します。

- プール：[プール] をクリックし、次に [開始] をクリックして、ドロップダウン リストからプロバイダを選択します。

機能	プロバイダ タイプ
Horizon Edge	Microsoft Azure および Windows 365
イメージ	Microsoft Azure および Horizon 8
プール	Microsoft Azure

2 選択したプロバイダ タイプの詳細を入力して保存します。

3 プロバイダを編集するには、リストからプロバイダを選択し、[編集] をクリックします。

すべての値が編集可能であるわけではありません。編集できない値は、プロバイダ タイプによって異なります。

4 プロバイダの詳細を表示するには、プロバイダの横にある二重矢印をクリックします。

右側のペインにプロバイダの詳細が表示されます。一覧表示される情報のタイプは、プロバイダ タイプによって異なります。

5 プロバイダを削除するには、リストからプロバイダを選択し、[削除] をクリックします。

特定の Horizon Edge の詳細を表示し、アクションを実行する

特定の Horizon Edge に関するデータを表示したり、アクション（編集や削除など）を実行したりするには、Horizon Edge ページで Horizon Edge の名前をクリックします。

特定の Horizon Edge の詳細ページには、プロバイダ、Unified Access Gateway、Horizon Edge Gateway などを含む、Horizon Edge に関連するさまざまな情報が表示されます。ただし、詳細ページで使用可能な情報は、Horizon Edge が Microsoft Azure 環境にデプロイされているか、Horizon 8 環境にデプロイされているかによって大きく異なります。

Microsoft Azure Edge と Horizon 8 Edge の詳細ページの大きな違いは、Horizon 8 Edge には [サマリ] タブ、[インフラストラクチャの監視] タブ、[機能] タブが含まれていることです。Microsoft Azure Edge の場合、詳細ページ上で直接サマリ情報を表示していますが、インフラストラクチャの監視情報は現時点で含まれません。

次のスクリーンショットは、さまざまな Horizon Edge のタイプの Horizon Edge 詳細ページを部分的に示しています。

図 5-1. Microsoft Azure Edge

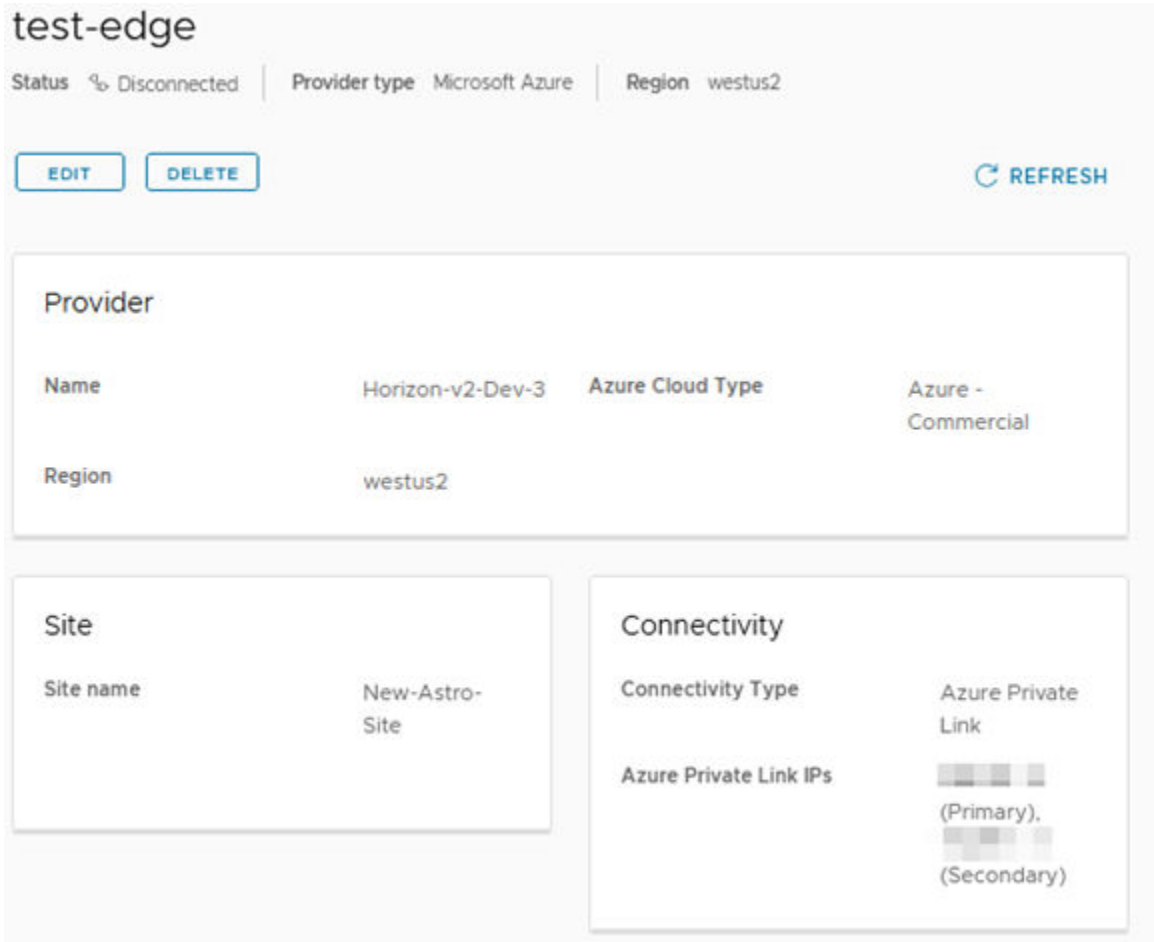
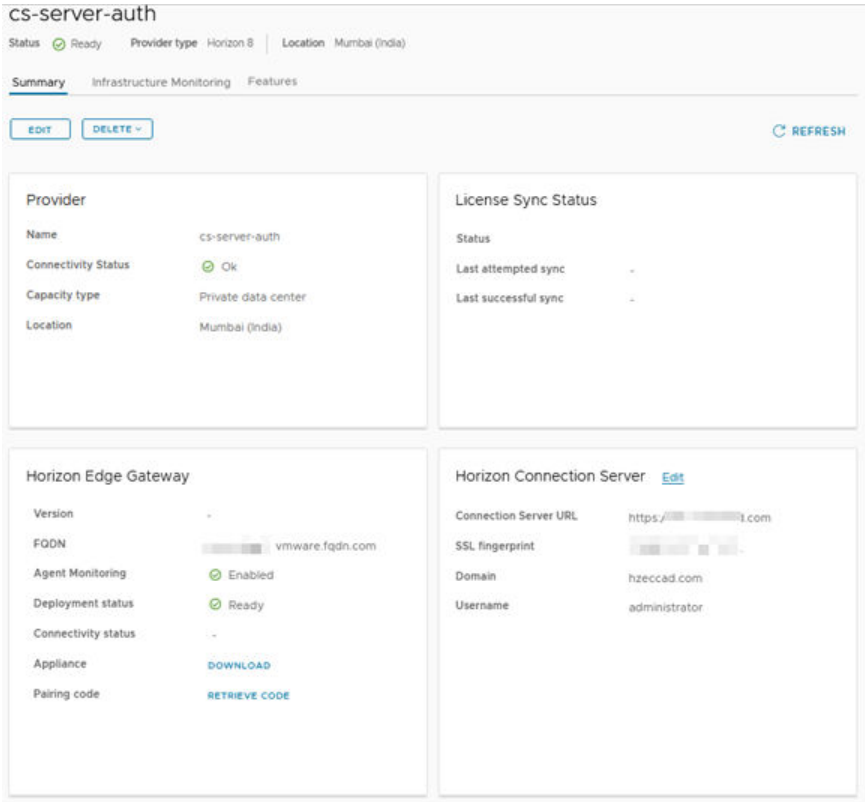


図 5-2. Horizon 8 Edge



Horizon 8 Edge の場合は、[サマリ] ページで、次の手順を実行して監視用の UAG を追加できます。

1 [Unified Access Gateway] セクションで、[監視用の Unified Access Gateway の追加] をクリックします。

2 [Unified Access Gateway] ページの [ロード バランサ] セクションで、[名前] と [FQDN または IP アドレス] を追加し、[保存] をクリックします。

3 [ゲートウェイ] セクションで、ロード バランサ情報を追加および保存してゲートウェイを追加できます。[追加] をクリックして [Unified Access Gateway を追加] します。

4 [名前]、ゲートウェイ管理エンドポイントの完全修飾ドメイン名、IP アドレスまたはホスト名である [管理エンドポイント]、United Access Gateway の [ユーザー名] および [パスワード] を追加します。

   CA 署名付き証明書または自己署名証明書を追加し、この UAG にアップロードすることができます。自己署名証明書の場合、ユーザーは証明書の詳細を確認するための通知を受け取ります。ユーザーは、この証明書を信頼する場合は [確認] をクリックする必要があります。クリックしないと、監視エラーが発生します。ユーザーが [確認] をクリックした場合、次回の確認の通知は受信されません。

   注： CA 署名付き証明書はすべての本番環境で推奨され、自己署名証明書は POC/テストにのみ推奨されます。

5 [保存] をクリックします。

上記のタスクを完了したら、[インフラストラクチャの監視] タブから追加した UAG を監視できます。Horizon 8 Edge で使用可能な [インフラストラクチャの監視] タブに表示されるデータの詳細については、Horizon 8 環境での Horizon Edge Gateway および Unified Access Gateway のインフラストラクチャ データの監視を参照してください。

App Volumes アプリケーション ストレージ アカウントのプライベート エンドポイントの構成

ストレージ アカウントのプライベート エンドポイントのステータスが `Not Configured` の場合は、[プライベート エンドポイントの構成] オプションを使用して、ストレージ アカウントのプライベート エンドポイントを構成します。

注： プライベート エンドポイントを構成した後、エンド ユーザーは仮想マシンからログアウトし、再度ログインすることをお勧めします。

1 Horizon Universal Console で、[リソース] - [キャパシティ] に移動します。

2 プライベート エンドポイントを構成する必要がある Horizon Edge をクリックします。

3 [App Volumes アプリケーション ストレージ] セクションに移動します。

4 [Azure ストレージ アカウント] テーブルで、プライベート エンドポイントのステータスが `Not Configured` または `Disconnected` のストレージ アカウントのオーバーフロー アイコン（縦に並んだ 3 つのドット）をクリックします。

5 [プライベート エンドポイントの構成] をクリックします。

6 [ストレージ アカウントのプライベート エンドポイントの構成] ウィンドウで、すべての要件が満たされていることを確認し、[権限] チェック ボックスを選択します。

これらの要件の詳細については、「App Volumes アプリケーション ストレージ アカウントの Azure プライベート エンドポイント」を参照してください。

7 [プライベート エンドポイントの vNet] ドロップダウン ボックスから仮想ネットワークを選択します。

8 [サブネット] ドロップダウン ボックスからサブネットを選択します。

9 [保存] をクリックします。

プライベート エンドポイントのステータスは `Connected` です。

既存の Horizon Edge デプロイでストレージ アカウントのプライベート エンドポイントを構成した後、ストレージ アカウントのパブリック ネットワーク アクセスを無効にする前に、次の手順を実行します。

- ストレージ アカウントと Horizon Edge およびストレージ アカウント、および各デスクトップ プール間の接続が正常であることを確認します。
- プライベート エンドポイントが構成される前に割り当てられた既存のアプリケーション添付ファイルを持つエンド ユーザーは、仮想マシンからログアウトする必要があります。

Azure ポータルで、[ストレージ アカウント] - [セキュリティ + ネットワーク] - [ファイアウォールと仮想ネットワーク] セクションに移動し、特定のストレージ アカウントの [パブリック ネットワーク アクセス] オプションを `Disabled` に設定します。詳細については、対応する Microsoft ドキュメントを参照してください。

既存のデスクトップ プールとファイル共有の間にアプリケーションの提供に影響を与える接続の問題があり、これらの問題をトラブルシューティングするまでストレージ アカウントのパブリック ネットワーク アクセスに戻す場合は、[プライベート エンドポイントの削除] オプションを使用できます。このオプションは、構成済みのプライベート エンドポイントを削除し、Azure ポータルのストレージ アカウントのパブリック ネットワーク アクセスを自動的に有効にします。問題を修正したら、[プライベート エンドポイントの構成] オプションを使用してプライベート エンドポイントを構成できます。

Horizon Cloud Service - next-gen での Unified Access Gateway または Horizon Connection Server 設定の更新

Horizon Universal Console から、既存の Unified Access Gateway または Horizon Edge Gateway 構成の指定された Horizon Cloud Service - next-gen 設定を直接変更できます。

Horizon Universal Console の [リソース] - [キャパシティ] ページを使用して、ステッパー メニュー シーケンス内で指定した Unified Access Gateway または Horizon Edge Gateway 構成を変更できます。

詳細については、「Horizon Edge のデプロイの再試行」および「Horizon Cloud Service - next-gen での Unified Access Gateway デプロイの再試行」を参照してください。

次のシナリオに示すように、Microsoft Azure Edge の Unified Access Gateway 設定または Horizon Edge の Horizon Connection Server を開いて編集できます。

ステータスが「失敗」の場合、Edge のリスト ページから Unified Access Gateway を再試行します。

[リソース] - [キャパシティ] - [Edge] リスト ページから、Microsoft Azure Edge のステッパー メニュー シーケンスで Unified Access Gateway 構成手順を開いて編集できます。

1 Horizon Cloud Service - next-gen にログインし、Horizon Universal Console を表示します。

2 [リソース] - [キャパシティ] - [Edge] リスト ページに移動します。

3 失敗した Unified Access Gateway デプロイの [失敗] アイコンをクリックしてサインポスト ヘルプを表示し、[再試行] をクリックします。

Microsoft Azure Edge の編集ページが開き、Unified Access Gateway の手順が表示され、Edge 設定を編集してデプロイを再試行できます。

ステータスが「失敗」の場合、Edge の詳細ページから Unified Access Gateway を再試行します。

[リソース] - [キャパシティ] - [Edge] 詳細ページから、Microsoft Azure Edge のステッパー メニュー シーケンスで Unified Access Gateway 構成手順を開いて編集できます。

1 Horizon Cloud Service - next-gen にログインし、Horizon Universal Console を表示します。

2 失敗したデプロイの [リソース] - [キャパシティ] - [Edge] 詳細ページに移動します。

3 Unified Access Gateway カードのエラー アラートから [再試行] をクリックします。

Microsoft Azure Edge の編集ページが開き、Unified Access Gateway の手順が表示され、Edge 設定を編集してデプロイを再試行できます。

Edge リスト ページから Unified Access Gateway を構成する

Edge リスト ページから、Microsoft Azure Edge のステッパー メニュー シーケンスで Unified Access Gateway 構成手順を開いて編集できます。

1 Horizon Cloud Service - next-gen にログインし、Horizon Universal Console を表示します。

2 [リソース] - [キャパシティ] - [Edge] リスト ページに移動します。

3 Unified Access Gateway 列の [構成] リンクをクリックします。

Microsoft Azure Edge の編集ページが開き、Unified Access Gateway の手順が表示され、Edge 設定を編集できます。

Edge 詳細ページから Unified Access Gateway を構成する

[キャパシティ] - [Edge] 詳細ページから、Microsoft Azure Edge のステッパー メニュー シーケンスで Unified Access Gateway 構成手順を開いて編集できます。

1 Horizon Cloud Service - next-gen にログインし、Horizon Universal Console を表示します。

2 Unified Access Gateway デプロイを含まない [リソース] - [キャパシティ] - [Edge] 詳細ページに移動します。

3 Unified Access Gateway カードの [追加] をクリックします。

Microsoft Azure Edge のページが開き、Unified Access Gateway の手順が表示され、Edge 設定を構成できます。

Edge 詳細ページから Unified Access Gateway を編集する

準備完了状態にあるデプロイの [リソース] - [キャパシティ] - [Edge] 詳細ページから、Microsoft Azure Edge のステッパー メニュー シーケンスで Unified Access Gateway 構成手順を開いて編集できます。

1 Horizon Cloud Service - next-gen にログインし、Horizon Universal Console を表示します。

2 準備完了状態にある Unified Access Gateway デプロイの [リソース] - [キャパシティ] - [Edge] 詳細ページに移動します。

3 Unified Access Gateway カードの [編集] をクリックします。

Microsoft Azure Edge のページが開き、Unified Access Gateway の手順が表示され、Edge 設定を編集できます。

Edge リスト ページから Horizon Connection Server を構成する

[リソース] - [キャパシティ] - [Edge] 詳細ページから、Horizon 8 Edge のステッパー メニュー シーケンスで Horizon Connection Server 構成手順を開いて編集できます。

1 Horizon Cloud Service - next-gen にログインし、Horizon Universal Console を表示します。

2 [リソース] - [キャパシティ] - [Edge] リスト ページに移動します。

3 Horizon Connection Server カードの Horizon Edge Gateway 列で [未構成] をクリックしてサインポスト ヘルプを表示し、[構成] をクリックします。

[ビューの編集] ページが開き、Connection Server の手順が表示され、Edge 設定を編集できます。

概要ページから Horizon Connection Server を構成する

[リソース] - [キャパシティ] - [Edge] 概要ページから、Horizon 8 Edge のステッパー メニュー シーケンスで Horizon Connection Server 構成手順を開いて編集できます。

1 Horizon Cloud Service - next-gen にログインし、Horizon Universal Console を表示します。

2 [リソース] - [キャパシティ] - [Edge] 概要ページに移動します。

3 Horizon Connection Server カードの [構成] をクリックします。

[ビューの編集] ページが開き、Connection Server の手順が表示され、Edge 設定を編集できます。

サマリ ページから Horizon Connection Server を編集する

[リソース] - [キャパシティ] - [Edge] サマリ ページから、Horizon 8 Edge のステッパー メニュー シーケンスで Horizon Connection Server 構成手順を開いて編集できます。

1 Horizon Cloud Service - next-gen にログインし、Horizon Universal Console を表示します。

2 [リソース] - [キャパシティ] - [Edge] サマリ ページに移動します。

3 Horizon Connection Server カードの [編集] をクリックします。

[ビューの編集] ページが開き、Connection Server の手順が表示され、Edge 設定を編集できます。

Horizon Edge のデプロイの再試行

Horizon Edge のデプロイは、失敗した場合でも、Horizon Edge を削除して新たに作成することなく再試行できます。

手順

1. [ホーム] ページで、[Horizon Edge] タイルの [Horizon Edge] をクリックします。
2. [キャパシティ] ページで、[Horizon Edge Gateway] の [作成が失敗しました] のサインポストをクリックしてエラーを表示します。
3. エラーを解決し、[再試行] をクリックして Edge のデプロイを再試行します。
4. [ログの表示] をクリックして、[アクティビティ ログ] を表示します。
5. [すべてを表示] をクリックして、エラーのリストを表示します。

   [再試行] が失敗すると、[キャパシティ] ページに通知が表示され、失敗の理由が示されます。

Horizon Cloud Service - next-gen での Unified Access Gateway デプロイの再試行

Unified Access Gateway のデプロイが失敗した場合は、Horizon Cloud Service - next-gen で Unified Access Gateway を削除して新たに作成することなく再試行できます。

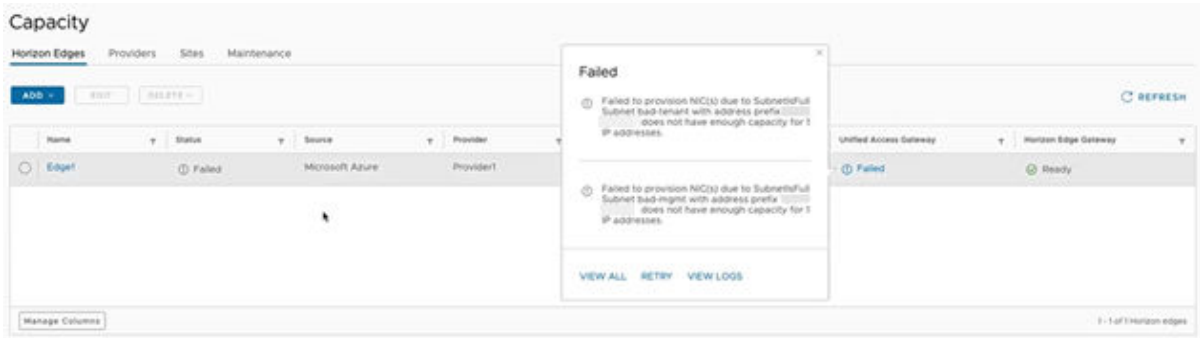
ネットワーク情報が不正確な場合、Unified Access Gateway のデプロイが失敗することがあります。仮想ネットワーク、仮想マシン サブネット、管理サブネット、DMZ サブネット情報などのネットワーク情報を再入力して、Unified Access Gateway を再試行できます。

Horizon Universal Console では、次の手順で説明する方法に加えて、Unified Access Gateway を再試行する方法がいくつかあります。たとえば、 ホーム ページで [Horizon Edge] を選択し、[Unified Access Gateway] 列にステータスとして「[失敗]」と表示される Horizon Edge の名前をクリックすると、その Horizon Edge の詳細ページを下にスクロールして Unified Access Gateway セクションに移動できます。Unified Access Gateway セクションでは、[再試行] をクリックして Unified Access Gateway のデプロイを再試行することもできます。

手順

1 Horizon Cloud Service - next-gen にログインし、Horizon Edge をクリックします。

2 Unified Access Gateway の [失敗] のサインポストをクリックします。



3 [すべてを表示] をクリックして、エラーの完全なリストを表示します。

3 つ以上のエラーがある場合は、[すべてを表示] ボタンが表示されます。

4 [再試行] をクリックします。

Microsoft Azure Edge の編集ページが開き、Unified Access Gateway の手順が表示されます。

5 適切な値を編集して、[保存] をクリックします。

6 [アクティビティ ログ] ページに移動する場合は、[ログの表示] をクリックできます。

Edge の削除

Edge を削除でき、削除すると Edge 内のすべてのリソースが削除されます。

前提条件

- Edge 内のプール グループが削除されます。
- Edge 内のプールが削除されます。
- Edge 内のイメージが削除されます。
- UAG が削除されます。

手順

1 [キャパシティ] ページで、削除する Edge を選択します。

2 [削除] をクリックし、ドロップダウン メニューから [Horizon Edge Gateway] を選択します。

3 [削除の確認] ダイアログ ボックスで [削除] をクリックし、すべてのアプリケーション ボリューム ファイル共有を削除します。

Edge を削除すると、アプリケーション ストレージ（ファイル共有）、App Volumes のアプリケーションとパッケージなど、Edge に関連するすべてのリソースがバックグラウンドで削除されます。

Horizon Edge Gateway および Unified Access Gateway のデプロイ後に必要な DNS レコードを構成する

Horizon Edge Gateway および Unified Access Gateway インスタンスをデプロイしたら、Unified Access Gateway インスタンスの FQDN に一致する DNS レコードを作成します。

このタスクは、Horizon Edge Gateway および Unified Access Gateway インスタンスをデプロイした後に実行します。Microsoft Azure Edge のデプロイを参照してください。

注： 複数の Unified Access Gateway クラスタがある場合は、ピアリングされていないすべての VNet に DNS サーバを構成します。

今後、サブネットを指定する必要グループがあるプール グループをさらに作成する場合は、ピアリングされていないすべての VNet の DNS サーバの構成も適用されます。

前提条件

Horizon Universal Console を使用して、次の IP アドレスと FQDN を取得します。たとえば、[リソース] - [キャパシティ] を選択し、構成する Horizon Edge Gateway インスタンスの名前をクリックして、対応する IP アドレスと FQDN を次のように書き留めます。

Unified Access Gateway セクションで、Unified Access Gateway インスタンスに関連付けられているロード バランサの IP アドレスと FQDN を取得します。リストには、Horizon Edge Gateway インスタンスをデプロイしたときに構成したロード バランサのタイプのラベルが含まれています。内部ロード バランサと外部ロード バランサの両方を構成した場合は、対応するロード バランサ関連のラベルが Unified Access Gateway セクションに表示されます。

ラベル	説明
ロード バランサの IP アドレス	パブリック（外部）ロード バランサの IP アドレス
ロード バランサのプライベート IP アドレス	内部ロード バランサの IP アドレス
FQDN	Unified Access Gateway インスタンスの FQDN。 この FQDN は、内部と外部の両方のロード バランサの IP アドレスに使用できます。

手順

1 Unified Access Gateway の場合は、ロード バランサの構成に応じて、次の適切な手順を実行します。

- [インターネット経由の外部アクセス] を選択した場合

  DNS レコードを作成し、FQDN を使用して、Unified Access Gateway 構成内の外部ロード バランサのパブリック IP アドレスを参照します。

- [企業のネットワーク経由の内部アクセス] を選択した場合

DNS レコードを作成し、FQDN を使用して、Unified Access Gateway 構成内の内部ロード バランサのプライベート IP アドレスを参照します。

このプライベート ロード バランサの IP アドレスは、Unified Access Gateway クラスタのデプロイ時に選択したデスクトップ（テナント）サブネットにあります。

- [内部および外部アクセス] を選択した場合

  内部 DNS で、Unified Access Gateway FQDN を内部ロード バランサのプライベート IP アドレスにマッピングします。

  また、外部 DNS で、Unified Access Gateway FQDN を外部ロード バランサのパブリック IP アドレスにマッピングします。

2 行った更新を確認します。

統合の構成

Horizon Cloud Service - next-gen で、デプロイ構成とセットアップの一環として、Identity Manager やアプリケーション ボリュームなどのさまざまな統合を構成します。

Horizon Cloud Service - next-gen 環境での ID とアクセス管理

このドキュメント ページでは、Horizon Cloud Service - next-gen 環境での ID とアクセス管理の使用方法について簡単に紹介し、詳細な情報を含むページへのリンクを一覧表示します。

ユーザー ID とマシン ID について

Horizon Cloud Service - next-gen は、ID の処理方法が他の環境とは異なります。Horizon Cloud Service - next-gen では、サービスはユーザー ID とマシン ID を区別し、クライアントとリモート デスクトップまたはアプリケーション間の安全な接続を確立するときに両方のタイプの ID に依存します。

注： 第 1 世代の Horizon Cloud 環境や Horizon 8 オンプレミス環境など、単一の ID プロバイダを使用してユーザーとマシンの両方の ID を認証する環境に慣れている場合は、ユーザー ID とマシン ID の区別を行うのは初めてかもしれません。

Horizon Cloud Service - next-gen では、ユーザー ID を認証するための ID プロバイダとマシン ID を認証するための ID プロバイダで構成される ID 構成を設定する必要があります。

ユーザー ID

Horizon Cloud Service - next-gen では、ユーザー ID プロバイダを登録する必要があります。サービスは、この ID プロバイダを使用して、リモート デスクトップおよびアプリケーションにアクセスしようとするクライアント ユーザーを認証します。

マシン ID

Horizon Cloud Service - next-gen では、マシン ID プロバイダも登録する必要があります。サービスは、この ID プロバイダを使用して、リモート デスクトップとアプリケーションを提供する仮想マシンのマシン ID を確立します。

マシン ID プロバイダを介して、サービスはリモート デスクトップとリモート アプリケーションの仮想マシン ソースを、クライアント ユーザーがアクセスする資格が付与されている信頼できるネットワーク ドメインに参加させます。

ユーザー ID とマシン ID の要件

Horizon Cloud Service - next-gen でサポートされる ID 構成の詳細、およびユーザー ID とマシン ID の詳細な要件については、「Microsoft Azure Edge をデプロイするための要件チェックリスト」を参照してください。

管理者およびロール ベースのアクセス制御 (RBAC)

環境への管理者アクセスのために、サービスは、VMware Cloud services の機能を使用してロール ベースのアクセス制御を提供します。これらの制御により、権限のある担当者のみが適切なレベルのアクセス権を持つようになります。コントロールは、最小権限の原則に基づいています。詳細については、オンボーディング ページにあるユーザーの追加とロールの割り当ての概要セクションを参照してください。

詳しい情報

次のリンクを使用して、環境の ID およびアクセス管理構成に関する詳細情報にアクセスします。

Active Directory ドメインの設定

Horizon Cloud Service - next-gen で、Horizon Universal Console の次の手順を実行して、最初の Active Directory ドメインをサービスに登録するか、追加の Active Directory ドメインを登録します。

注： このドキュメント ページは、環境で Microsoft Azure に Horizon Edge を展開する場合に適用されます。これは、Horizon 8 のデプロイにも Horizon Plus サブスクリプションにも適用されません。

Horizon Cloud Service - next-gen 環境での ID とアクセス管理 で説明されているように、サービスは仮想デスクトップおよびリモート アプリケーションのマシン ID に登録された Active Directory を使用します。

前提条件

Active Directory の要件

コンソールの [ドメイン登録] ウィザードでは、特定の情報を入力する必要があります。コンソールでこれらの手順を実行する前に、ユーザーまたは IT チームが Microsoft Azure Edge をデプロイするための要件チェックリストの Active Directory の要件セクションで説明されている Active Directory に関連する要件を満たしていることを確認します。

LDAPS 固有の重要なポイントと要件

デプロイで LDAPS を使用する場合は、次の重要なポイントと要件に注意してください。

- PEM でエンコードされたルート CA 証明書と中間 CA 証明書のアップロードの準備ができている必要があります。
- 自己署名証明書はサポートされていません。
- このサービスでは、LDAPS を使用するように構成されたドメインの SRV レコードが DNS に含まれている必要があります。ドメインに LDAPS を使用することを選択すると、SRV レコードの使用が暗黙的に指定されます。

- チャネルのバインドを強制するように Active Directory 環境を構成することが強く推奨されます。チャネル バインドの強制は、LDAPS を正しく保護するために（特に中間者攻撃 (MITM) を回避するために）不可欠です。
- 「Microsoft Azure での Horizon Cloud 環境のポートとプロトコルの要件」で説明するように、ファイアウォール構成では、次のポートとプロトコルを使用して、Horizon Edge Gateway からドメイン コントローラへの送信接続を許可する必要があります。
  - ポート 88/TCP：Kerberos 認証
  - ポート 636/TCP、3269/TCP：LDAPS 通信
- ルート証明書を除く、信頼チェーン内のすべての証明書に対して HTTP の失効エンドポイントが定義されている必要があり、そのエンドポイントは `HTTP` を介してアクセスできる必要があります。この要件には次のポイントが含まれています。
  - 失効エンドポイントには LDAP を使用できません。
  - サービスは、証明書に定義されている OCSP または CRL `HTTP` URL を使用して失効チェックを実行します。
  - 証明書で HTTP プロトコルの OCSP または CRL エンドポイントが定義されていない場合、サービスは失効チェックを実行できません。その場合、LDAPS 接続が失敗します。
  - エンドポイントには可視化の失効を利用できる必要があります。ファイアウォールは、`HTTP` を介して失効エンドポイントに向かう送信トラフィックをブロックすることはできません。

手順

1 左側のペインで [統合] をクリックし、[ID とアクセス] タイルで [管理] をクリックします。

2 [ドメイン] タブで、[追加] をクリックして、コンソールの [ドメイン登録] ウィザードを起動します。

3 ウィザードの最初の手順で、指示された情報を入力します。

フィールド	説明
[名前]	Active Directory ドメインの名前。
[説明]	（オプション）説明。
[DNS ドメイン名]	この Active Directory ドメイン（`our-ad.example.com` など）の完全修飾名。
[デフォルト OU]	適切なデフォルト OU を入力します。 この OU は、仮想デスクトップおよびリモート アプリケーション用に作成されたマシン ID を追加するときに、サービスでデフォルトとして使用する Active Directory 組織単位 (OU) です。 `OU=MyOrg,DC=our-ad,DC=example,DC=com` などの OU の完全な識別名 (DN) を入力します。 **注：** デフォルトの `CN=Computers` を使用する場合は、フィールドに入力する必要があります。ユーザー インターフェイスのフィールドにこのデフォルト値が表示される場合でも、このフィールドに直接入力しない限り、ウィザードで [次へ] ボタンを使用できるようにはなりません。

フィールド	説明
[ドメイン バインド アカウント]	Microsoft Azure Edge をデプロイするためのチェックリスト要件の Active Directory の要件セクションの説明に従って、ユーザーまたはユーザーの IT チームがこの目的のために構成した 2 つのサービス アカウントのユーザー名とパスワードを入力します。 これらのサービス アカウントは、Active Directory ドメインでルックアップを実行するために使用されます。最初に入力したアカウントは、サービスがこの目的で使用するプライマリ アカウントです。補助アカウントは、プライマリ アカウントのバックアップです。 ここに入力したアカウントが、要件チェックリストに記載されている要件を満たしていることを確認します。
[ドメイン参加アカウント]	Microsoft Azure Edge をデプロイするためのチェックリスト要件の Active Directory の要件セクションの説明に従って、ユーザーまたはユーザーの IT チームがこの目的のために構成した 2 つのサービス アカウントのユーザー名とパスワードを入力します。 これらのサービス アカウントは、マシン ID を Active Directory ドメインに参加させ、Sysprep 操作を実行するために使用されます。最初に入力したアカウントは、サービスがこの目的で使用するプライマリ アカウントです。補助アカウントは、プライマリ アカウントのバックアップです。 ここに入力したアカウントが、要件チェックリストに記載されている要件を満たしていることを確認します。
[プロトコル]	Active Directory を Horizon Edge Gateway に接続するために使用するプロトコル ([LDAP] または [LDAPS]) を選択します。 [LDAPS] を選択した場合は、[参照] 機能を使用して PEM でエンコードされたルート CA 証明書と中間 CA 証明書をアップロードします。これらの証明書は、このタスクの前提条件で参照されます。

必要なすべての情報を入力すると、[次へ] ボタンが使用可能になります。

4 [次へ] をクリックして、次のウィザード手順に進みます。

この時点で、ドメイン情報のシステムへの保存を完了するための [保存] アクションが、ウィザードで使用できるようになります。

- SSO を使用する予定がない場合は、[保存] をクリックして、この時点で UI ウィザードを完了できます。
- True SSO 機能を使用する予定がある場合は、このページの次の手順に進みます。True SSO 機能を使用するには、Microsoft Azure で Horizon Edge により SSO を使用するためにサポートされる認証局タイプに説明されているように、Microsoft Enterprise Certificate Authority が必要です。
- VMware CA または Microsoft Enterprise Certificate Authority 以外の認証局に依存する SSO を使用する場合は、[保存] をクリックして、この時点で UI ウィザードを完了できます。後で、Horizon Cloud Service - next-gen への VMware CA 向けの SSO 構成の追加 の手順を使用して SSO 構成を完了できます。

5 (オプション) エンド ユーザーの仮想デスクトップとリモート アプリケーションで True SSO を使用する場合は、ウィザードの [ドメイン登録サービス アカウント] セクションで、[登録サービス アカウントを使用] トグルをオンにします。

このトグルをオンにすると、True SSO 機能で必要なドメイン登録アカウントのアカウント認証情報を入力するためのフィールドがユーザー インターフェイスに表示されます。情報を入力します。

注目: 代わりに、VMware CA に依存する SSO を使用する場合は、ドメイン登録アカウント情報を入力するこの手順をスキップできます。

ドメイン登録アカウントは、True SSO 機能が Microsoft AD CS（Active Directory 証明書サービス）から短期証明書を取得するために使用する登録サービス アカウントです。True SSO は認証に証明書を使用し、ユーザーに Active Directory 認証情報の入力を求めるプロンプトを表示しないようにします。Horizon Universal Console では、ドメイン登録アカウント、登録サービス アカウント、およびドメイン登録サービス アカウントという用語が同じ意味で使用されている場合があります。

フィールドの入力が完了すると、ウィザードでドメイン情報のシステムへの保存を完了するための [保存] アクションが使用できるようになります。

[保存] をクリックして、ウィザードで入力したすべての情報の保存を完了します。

結果

Horizon Edge を使用した Active Directory の構成が完了しました。ただし、デプロイの構成を続行するときに、Active Directory 接続の問題を検出した場合は、Horizon Edge の診断 - Microsoft Azure デプロイの Active Directory 接続を参照してください。

次のステップ

前述の手順が完了すると、サービスには、Horizon Cloud on Microsoft Azure 環境に必要な Active Directory ドメイン情報が含まれます。

エンド ユーザーがデスクトップおよびアプリケーションにアクセスするときにシングル サインオン (SSO) 機能を追加する方法については、Microsoft Azure で Horizon Edge により SSO を使用するためにサポートされる認証局タイプ を参照してください。

Active Directory ドメインの編集 - Horizon Cloud Service - next-gen

Active Directory ドメインを追加したら、Horizon Universal Console を使用してそのドメインを編集できます。

Active Directory ドメインの編集に関する前提条件と手順は、Active Directory ドメインを構成する最初の手順とよく似ています。詳細については、Active Directory ドメインの設定を参照してください。このタスクで実行する必要がある前提条件は、更新する予定のドメイン情報によって異なります。たとえば、プロトコルを LDAP から LDAPS に変更する場合は、PEM エンコードされたルート CA 証明書と中間 CA 証明書を準備し、適切な LDAPS ポートを使用可能にするなど、LDAPS 関連の前提条件を実行する必要があります。

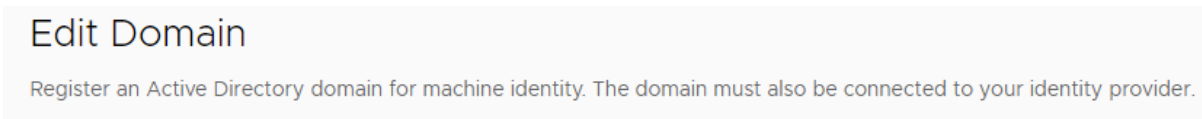
手順

1 コンソールの [ドメイン] タブに移動します。

左側のペインで [統合] をクリックし、[ID とアクセス] タイルで [管理] をクリックします。

2 編集するドメインを選択し、[編集] をクリックします。

3 更新する情報を編集します。



フィールド	説明
[全般情報]	必要に応じて、[名前] や [デフォルト OU] などの全般情報を編集します。
[ドメイン バインド アカウント]	該当する場合は、Microsoft Azure Edge をデプロイするためのチェックリスト要件の Active Directory の要件セクションの説明に従って、ユーザーまたはユーザーの IT チームがこの目的のために構成した 2 つのサービス アカウントのユーザー名とパスワードを更新します。
[ドメイン参加アカウント]	該当する場合は、Microsoft Azure Edge をデプロイするためのチェックリスト要件の Active Directory の要件セクションの説明に従って、ユーザーまたはユーザーの IT チームがこの目的のために構成した 2 つのサービス アカウントのユーザー名とパスワードを入力します。
[プロトコル]	必要に応じて、プロトコルを [LDAP] から [LDAPS] に変更するか [LDAPS] から [LDAP] に変更します。 [LDAP] から [LDAPS] に変更する場合は、[参照] 機能を使用して PEM でエンコードされたルート CA 証明書と中間 CA 証明書をアップロードします。これらの証明書は、このタスクの前提条件で参照されます。

4 [保存] をクリックします。

5 （オプション） エンド ユーザーの仮想デスクトップとリモート アプリケーションで True SSO を使用する場合は、ウィザードの [ドメイン登録サービス アカウント] セクションで、[登録サービス アカウントを使用] トグルをオンにします。

このトグルをオンにすると、True SSO 機能で必要なドメイン登録アカウントのアカウント認証情報を入力するためのフィールドがユーザー インターフェイスに表示されます。情報を入力します。

注目: 代わりに、VMware CA に依存する SSO を使用する場合は、ドメイン登録アカウント情報を入力するこの手順をスキップできます。

ドメイン登録アカウントは、True SSO 機能が Microsoft AD CS（Active Directory 証明書サービス）から短期証明書を取得するために使用する登録サービス アカウントです。True SSO は認証に証明書を使用し、ユーザーに Active Directory 認証情報の入力を求めるプロンプトを表示しないようにします。Horizon Universal Console では、ドメイン登録アカウント、登録サービス アカウント、およびドメイン登録サービス アカウントという用語が同じ意味で使用されている場合があります。

フィールドの入力が完了すると、ウィザードでドメイン情報のシステムへの保存を完了するための [保存] アクションが使用できるようになります。

[保存] をクリックして、ウィザードで入力したすべての情報の保存を完了します。

結果

Horizon Edge を使用した Active Directory の更新が完了しました。ただし、Active Directory の接続で問題を検出した場合は、Horizon Edge の診断 - Microsoft Azure デプロイの Active Directory 接続を参照してください。

ドメインの削除

ドメインを削除する場合は、関連付けられているすべてのリソースを削除する必要があります。関連付けられたリソースがなくなると、ドメインを削除できます。

手順

1 Horizon Universal Console にログインします。

2 ナビゲーション バーの [統合] をクリックします。

3 [ID とアクセス] タイルで [管理] をクリックします。

4 [ID とアクセス] ページで削除するドメインを選択し、[削除] をクリックします。

5 ドメインに関連付けられている [SSO] および [プール グループ] を削除します。

リソースがドメインに関連付けられている場合、ドメインを削除することはできません。ドメインに関連付けられているリソースがない場合は、追加の手順を実行せずに永久に削除できます。

Microsoft Azure で Horizon Edge により SSO を使用するためにサポートされる認証局タイプ

このドキュメント ページには、Horizon Cloud Service - next-gen がエンド ユーザーの仮想デスクトップおよびリモート アプリケーションにシングル サインオン機能を提供する際の使用をサポートする認証局タイプのカテゴリが一覧表示されています。

概要

エンド ユーザーが Microsoft Azure の Horizon Edge によって提供される仮想デスクトップおよびアプリケーションにシングル サインオン (SSO) できるようにしたい場合は、Horizon Cloud でその SSO 機能を提供するために必要な項目を構成する必要があります。

重要な項目は、Active Directory 認証情報の入力を求めるプロンプトを表示しないようにするために、認証に使用するサービスの SSO 機能の短期的な証明書を提供する認証局です。

サポートされるタイプ

SSO 機能については、Horizon Cloud Service - next-gen が現在、次の認証局タイプの使用をサポートしています。

Microsoft Enterprise Certificate Authority (Active Directory Certificate Services)

Microsoft Enterprise Certificate Authority というフレーズは、エンタープライズ モードで実行されている Microsoft Certificate Authority (Microsoft CA) を指します。Microsoft の Microsoft Enterprise Certificate Authority を構成する 手順では、Active Directory Certificate Services (AD CS) ロールがインストールされ、エンタープライズ CA として動作するように構成されます。

このタイプの Microsoft Enterprise Certificate Authority を使用する場合は、Horizon Universal Console で [Microsoft CA] という名前のオプションを選択します。この選択により、Horizon Edge は、True SSO 機能を使用して、エンド ユーザーのシングル オン機能を提供するように構成されます。

その他の認証局

このカテゴリには、Microsoft スタンドアローン認証局とサードパーティの認証局が含まれます。Microsoft Standalone Certificate Authority という語句は、スタンドアローン モードで実行されている Microsoft CA（AD CS ロールのセットアップ プロセスにおけるスタンドアローン CA タイプ）を指します。

証明書にこのタイプの CA を使用する場合は、Horizon Universal Console で [VMware CA] という名前のオプションを選択します。この選択により、Horizon Edge は、エンド ユーザーのシングル サインオン機能を提供するために VMware CA 機能を使用するように構成されます。

その他の資料

現在サポートされている認証局タイプの使用方法の詳細については、以下を参照してください。

各タイプの使用方法とその前提条件へのリンクについては、以下を参照してください。

- Horizon Cloud - True SSO 要件 - Microsoft Enterprise Certificate Authority、必要な証明書テンプレート
- Horizon Edge で True SSO を使用するための Horizon Cloud Service - next-gen への SSO 構成の追加
- Horizon Cloud Service - next-gen への VMware CA 向けの SSO 構成の追加

Horizon Cloud - True SSO 要件 - Microsoft Enterprise Certificate Authority、必要な証明書テンプレート

Horizon Cloud Service - next-gen の場合、このページでは、Microsoft Azure の Horizon Edge で True SSO 機能を使用するために必要な要素について説明します。

Horizon 8 オンプレミス環境や第 1 世代の Horizon Cloud on Microsoft Azure 展開などの以前の Horizon 環境で、すでに True SSO の使用に慣れているかもしれません。

Horizon Cloud Service - next-gen 環境の場合、True SSO 機能を使用してエンド ユーザーにデスクトップおよびアプリケーションへのシングル サインオン (SSO) アクセスを提供するために必要な要素は、Microsoft Enterprise Certificate Authority と、その Microsoft Enterprise Certificate Authority で特別に構成されている証明書テンプレートです。

Microsoft Enterprise Certificate Authority

True SSO を使用するには、Microsoft Enterprise 認証局が必要です。

Microsoft Enterprise Certificate Authority という用語は、エンタープライズ モードで実行されている Microsoft 認証局 (Microsoft CA) を指します。True SSO にはエンタープライズ構成が必要であるため、True SSO のドキュメントでは Microsoft Enterprise Certificate Authority という語句を使用します。

ヒント: 本番環境では、冗長性とロード バランシングを提供するために、このような認証局を少なくとも 2 つ使用することがベスト プラクティスです。

認証局をまだ設定していない場合、Active Directory Certificate Services (AD CS) ロールを Microsoft Windows Server に追加し、Windows Server がエンタープライズ CA になるように構成する必要があります。

Microsoft Enterprise Certificate Authority を構成するための Microsoft の手順では、Active Directory Certificate Services (AD CS) ロールをインストールします。AD CS のセットアップ プロセスでは、CA をエンタープライズ CA として実行するか、スタンドアローン CA として実行するかを選択できます。

Horizon Cloud を使用した True SSO に必要な証明書テンプレートの設定

True SSO テンプレートの Windows Server 署名証明書の最小キー サイズを含む、次の設定を指定します。Windows Server 署名証明書の場合、必要な最小キー サイズは 2048 です。2048 未満の最小キー サイズを指定すると、認証に失敗します。

True SSO テンプレートの場合は、[暗号化] タブで次の設定を指定します。

1 [プロバイダのカテゴリ] には、[キー格納プロバイダ] を選択します。

2 [アルゴリズム名] には、[RSA] を選択します。

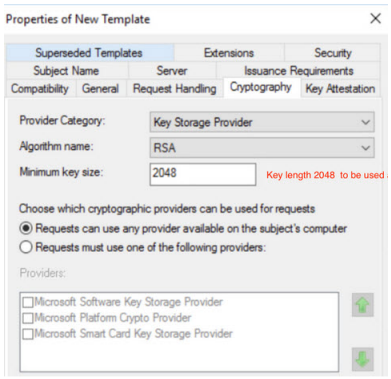
3 [最小キー サイズ] には、[2048] を指定します。

4 [要求に使用できる暗号化プロバイダを選択] には、[要求にはサブジェクトのコンピュータで利用可能な任意のプロバイダを使用できる] を使用します。

5 [要求ハッシュ] には、[SHA384] を指定します。

6 [保存] をクリックします。

2048 の最小キー サイズの値を示す部分的なスクリーン ショットを以下に示します。



非永続的な証明書処理を有効にする

True SSO で使用される Microsoft Enterprise 認証局ごとに、ベスト プラクティスは、非パーシステント証明書の処理を有効にすることです。

Microsoft Enterprise Certificate Authority で非永続的な証明書処理が有効になっていない場合、True SSO 証明書はエンタープライズ CA のデータベースに保存されたままになり、次のことが発生します。

- エンタープライズ CA のデータベースが必要を超えて急速に増大します。True SSO が、新しい接続ごとに新しい証明書を要求します。
- データベースの増大に伴い、エンタープライズ CA のディスク容量が不足するため、パフォーマンスに影響します。

VMware KB 2149312 で説明されているように、上記の問題を回避するために、`DBFLAGS_ENABLEVOLATILEREQUESTS` 設定を有効にすることをお勧めします。手順については、ナレッジベースの記事を参照してください。

注： `DBFLAGS_ENABLEVOLATILEREQUESTS` を有効にするための推奨事項の説明に加えて、このナレッジベースの記事では、別の設定、`CRLF_REVCHECK_IGNORE_OFFLINE` の使用についても説明しています。`CRLF_REVCHECK_IGNORE_OFFLINE` 設定を有効にする方法は、公開鍵基盤 (PKI) アーキテクチャによって異なります。`CRLF_REVCHECK_IGNORE_OFFLINE` 設定を有効にすることは、True SSO と Horizon Cloud の厳格な要件ではありません。

Horizon Cloud を使用した True SSO に必要な証明書テンプレートの設定

True SSO 機能を使用するには、True SSO および Horizon Edge で使用するために提供する Microsoft Enterprise Certificate Authority で証明書テンプレートを構成する必要があります。

証明書テンプレートは、Microsoft Enterprise Certificate Authority が True SSO で使用するために生成する証明書の基盤となります。

登録サービス アカウントには、`TrueSsoEnrollmentAgent` テンプレートと `TrueSso` テンプレートの両方のテンプレートで **読み取り** および **登録** 権限が必要です。

前提条件

- Microsoft Azure で Horizon Edge により SSO を使用するためにサポートされる認証局タイプの説明に従って、True SSO 機能で必要な Microsoft Enterprise Certificate Authority (AD CS) インスタンスがあることを確認します。
- Microsoft Azure での Horizon Cloud 環境のポートとプロトコルの要件の説明に従って、デプロイされた Horizon Edge が、必要なプロトコルとポートの組み合わせを使用して認証局インスタンスと通信できるように、ファイアウォールを構成します。

  通信では、インスタンスの Active Directory Certificate Services (AD CS) が使用されます。必要なプロトコルは RPC/TCP (RPC over TPC) です。最初のポートはポート 135 で、2 番目のポートは 49152 ～ 65535 の範囲内です。
- よりファイアウォールに適した構成を実現するために、静的 DCOM ポートを使用するように Microsoft Enterprise Certificate Authority (AD CS) インスタンスを構成し、ポート 135 と選択した静的 DCOM ポートを許可するようにファイアウォールを構成し、その静的ポートがすべてのインスタンスで同じになるように構成します。この構成については、Microsoft TechNet の「AD CS の静的 DCOM ポートを構成する方法」を参照してください。

注： 次の手順は、Microsoft Windows Server 2016 Standard オペレーティング システムを実行している Microsoft Enterprise Certificate Authority を使用して実行されました。手順のスクリーンショットは、そのシステムから取得したものです。このため、手順に記載されているラベルとスクリーンショットは、そのオペレーティング システムを反映しています。Microsoft Enterprise Certificate Authority が異なるオペレーティング システム バージョンの Windows Server を実行している場合は、以下のラベルおよびスクリーンショットと比較すると、システムに若干の違いがある可能性があります。

手順

1 Active Directory で新しいユニバーサル セキュリティ グループを作成します。

このグループを作成すると、ユーザーに代わって証明書を発行するために必要な権限を単一のセキュリティ グループに割り当てることができるようになります。すべての登録サービス アカウントが、このグループのメンバーになることによってそれらの必要な権限を継承できます。

a サーバ マネージャの [ツール] メニューから、または **dsa.msc** コマンドを実行して、Active Directory ユーザーおよびコンピュータ ツールを開きます。

b Active Directory ユーザーおよびコンピュータ ツールで、True SSO が必要とするドメイン登録アカウントの新しいグループを作成します。

グループに **True SSO 登録アカウント** など、任意の名前を付けます。また、次の設定も行います。

設定	値
[グループのスコープ]	ユニバーサル
[グループ タイプ]	セキュリティ

c [OK] をクリックして、新しいグループを保存します。

d 次に、ドメイン登録アカウントをこの新しいグループのメンバーとして追加します。

True SSO を使用する目的で使われる、すべてのドメイン登録サービス アカウントを追加します。

これらのアカウントは、Active Directory ドメインの設定 の説明に従って、Horizon Universal Console を使用して、ドメイン登録 UI フローで追加したものと同じアカウントです。

2 認証局ツールとその証明書テンプレート コンソールを使用して、True SSO 登録エージェントの証明書テンプレートを構成します。

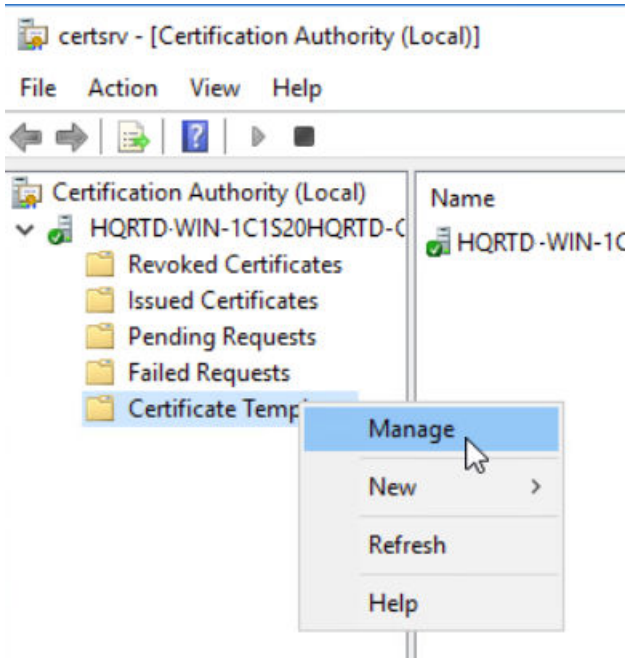
a 認証局ツールを開きます。

このツールを開くには、サーバ マネージャの [ツール] メニューや、[開始] メニューの Windows 管理ツールを使用したり、`certsrv.msc` を実行したりするなどいくつかの方法があります。

b 認証局ツールの左側のツリーで、証明書テンプレート フォルダが表示されるまでローカル CA 名を展開します。

c 証明書テンプレート フォルダを右クリックし、[管理] を選択して、証明書テンプレート コンソールを開きます。

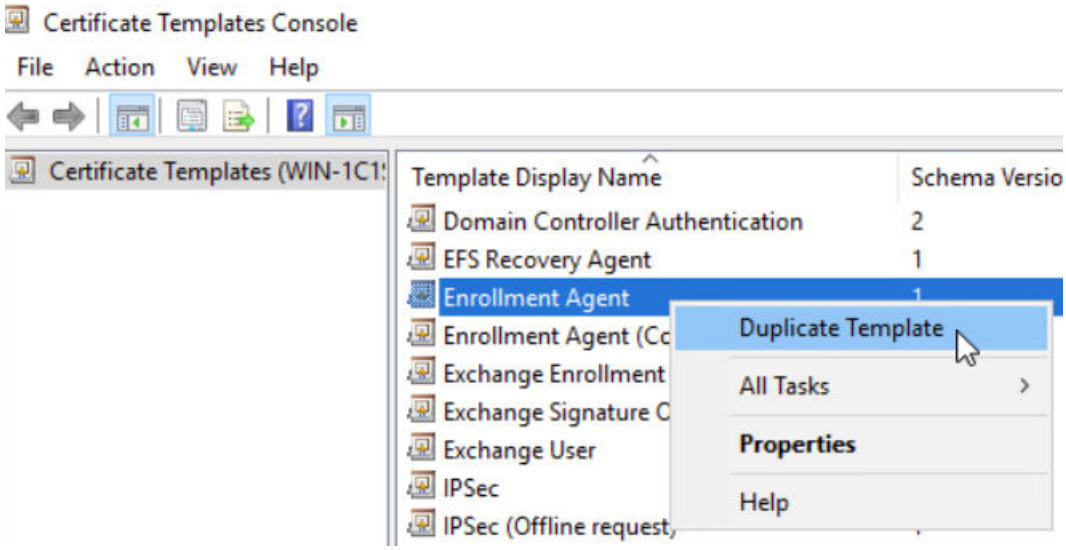
次のスクリーンショットは、Window Server 2016 を実行しているシステムでこの手順を示しています。



証明書テンプレート コンソールが表示されます。

d [登録エージェント] テンプレートを右クリックし、[テンプレートの複製] を選択します。

次のスクリーンショットは、Window Server 2016 を実行しているシステムでこの手順を示しています。



[新規テンプレートのプロパティ] ウィンドウが表示されます。

e　次のセクションの説明に従って、ウィンドウのタブに情報を入力します。

> **注：** 次のスクリーンショットは、Microsoft Windows Server 2016 Standard オペレーティング システムを実行している Microsoft Enterprise Certificate Authority を使用して撮られたものです。Microsoft Enterprise Certificate Authority が別のオペレーティング システム バージョンの Windows Server を実行している場合は、Windows システムのユーザー インターフェイスに若干の違いがある可能性があります。

[全般] タブ

重要： True SSO テンプレートの名前には ASCII 文字のみを使用します。この既知の問題により、True SSO テンプレート名に 非 ASCII 文字または拡張 ASCII 文字が含まれていると Horizon Cloud 環境で True SSO を正しく設定できません。

テンプレートの表示名

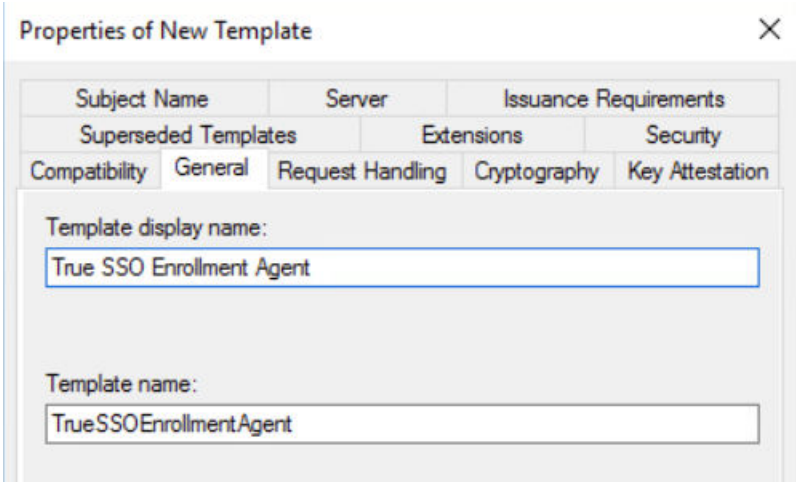
この新しいテンプレートが True SSO 登録エージェント用であることを示す名前を入力します（例：**`True SSO Enrollment Agent`**）。

テンプレート名

前の [テンプレートの表示名] に入力すると、ツールによってその名前がスペースなしの [テンプレートの表示名] の入力と一致するように自動的に入力されます。

たとえば、**テンプレートの表示名** に [True SSO EnrollmentAgent] と入力した場合、ツールはこの [テンプレート名] を自動的に `TrueSsoEnrollmentAgent` に設定します。

次のスクリーンショットは、[テンプレートの表示名] に **`True SSO Enrollment Agent`** と入力した後のこのタブを示しています。

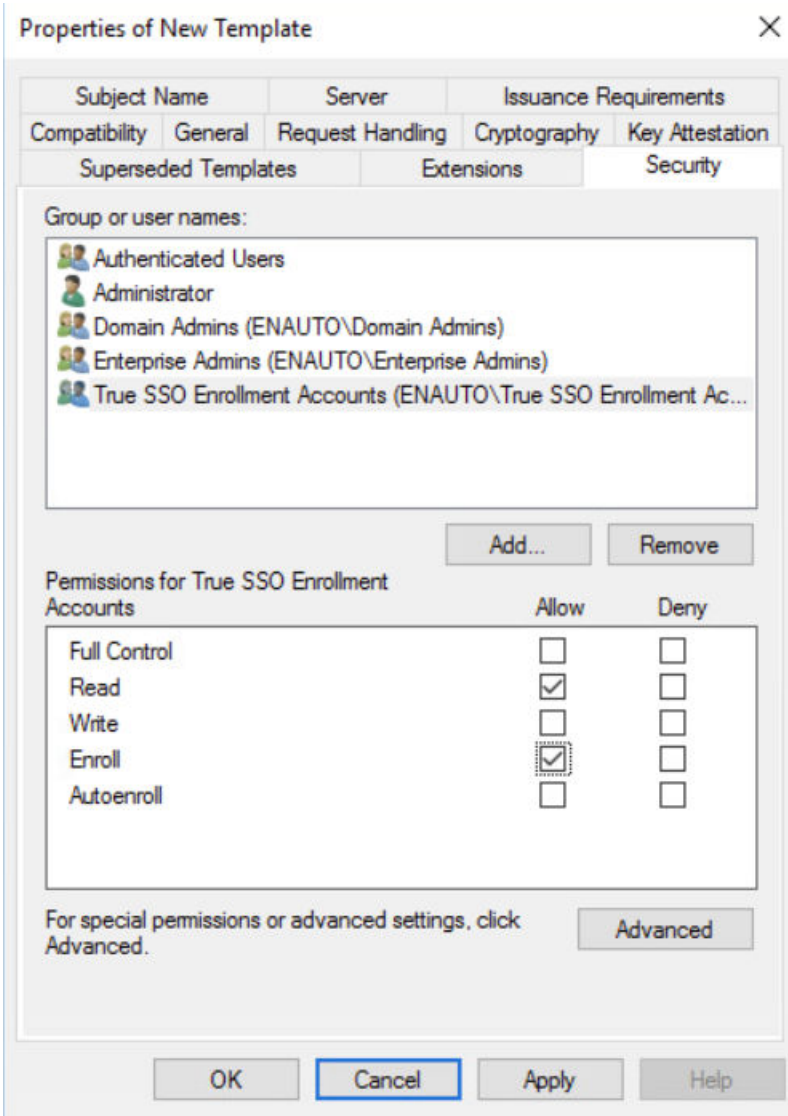


[セキュリティ] タブ

[セキュリティ] タブで、True SSO 登録アカウント用に作成した新しいユニバーサル セキュリティ グループに `Read` 権限と `Enroll` 権限を付与します。

1 [グループまたはユーザー名] セクションで、True SSO 登録アカウント用に作成したグループを追加します。

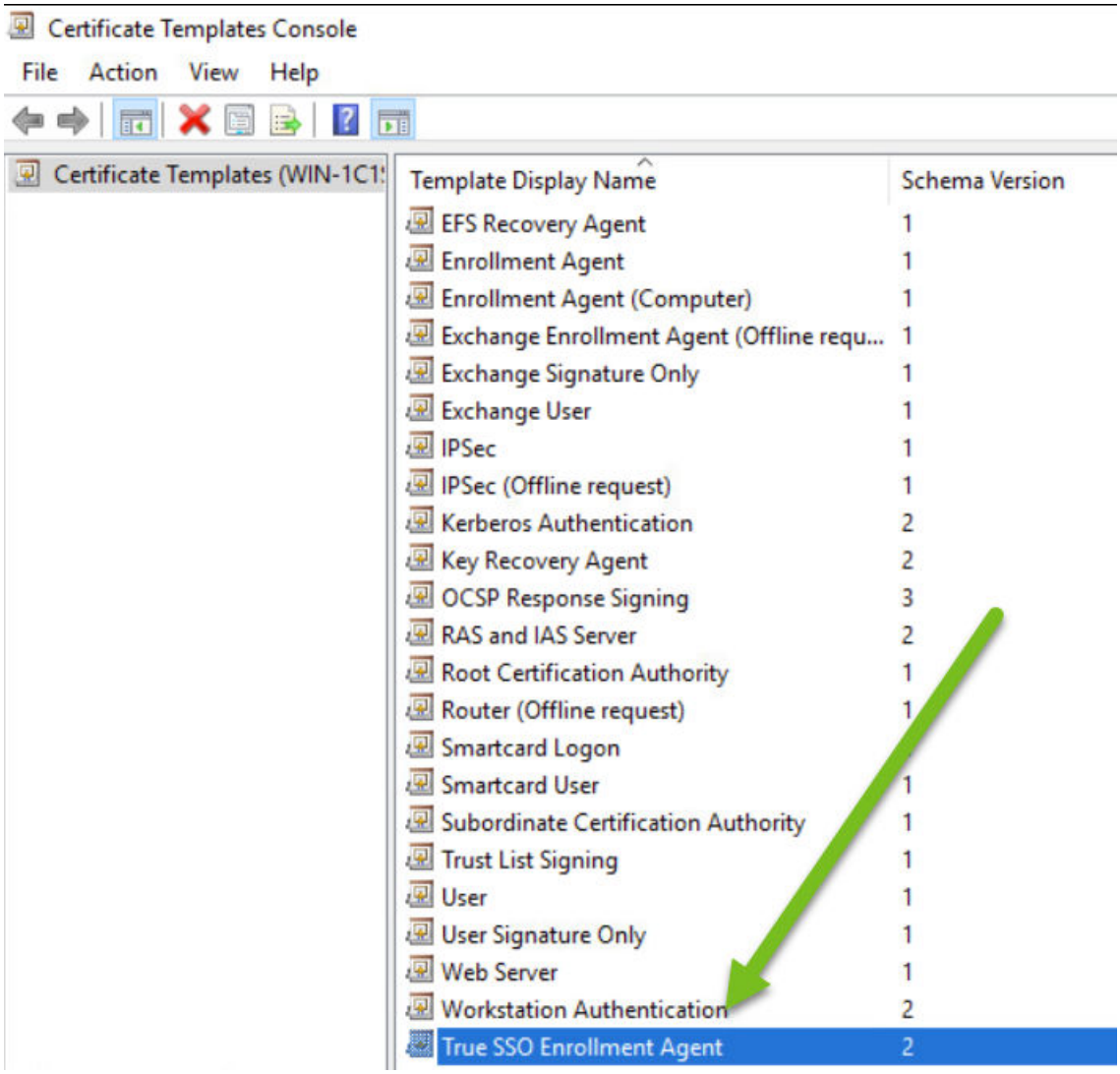
2 そのグループを選択し、[権限] セクションで `Read` 権限と `Enroll` 権限の [許可] を選択します。



f 新しい True SSO 登録エージェント テンプレートを保存するには、[新しいテンプレートのプロパティ] ウィンドウで [OK] をクリックします。

新しい True SSO 登録エージェント テンプレートが証明書テンプレート コンソール内にリストされ、指定した [テンプレート表示名] を使用して表示され、証明書要求エージェントとしての目的が表示されます。

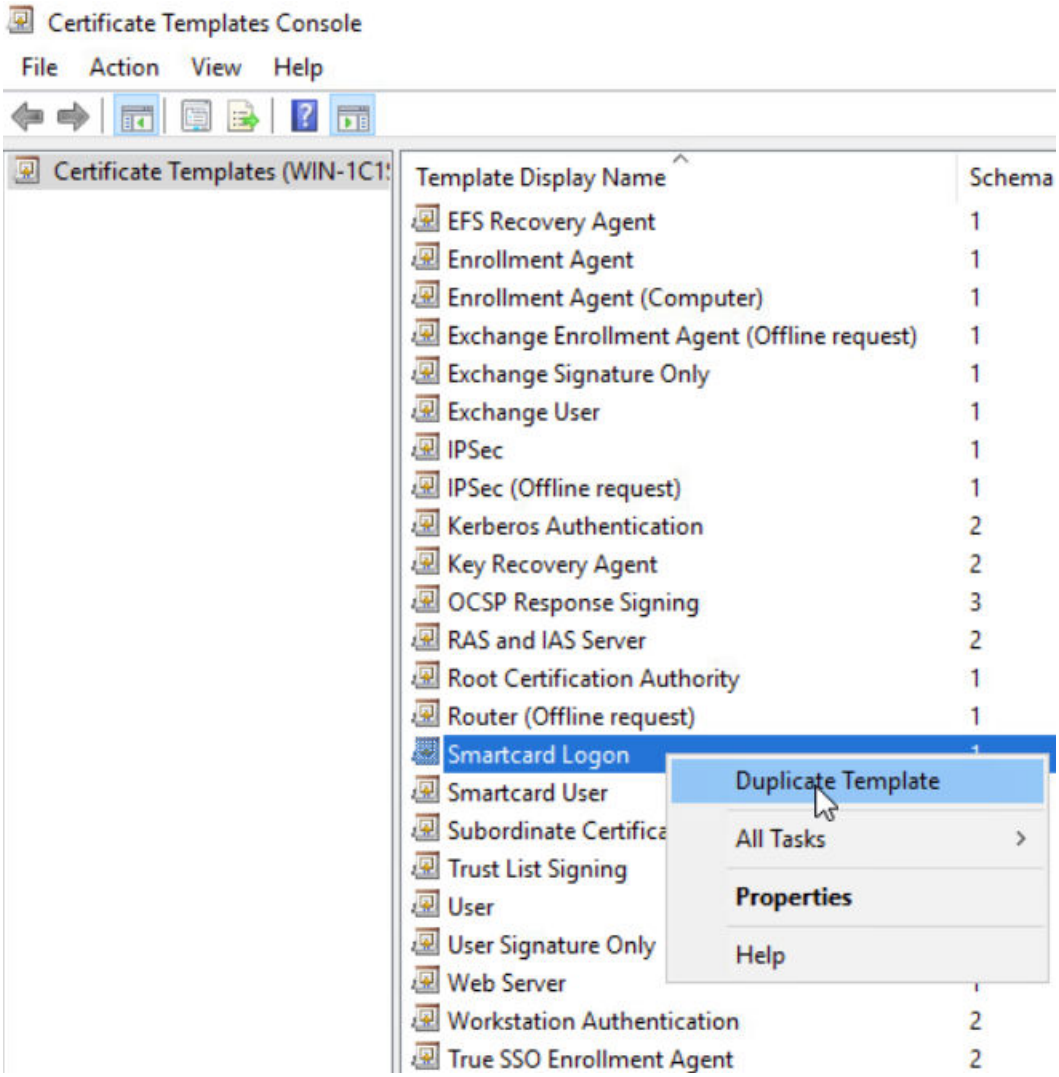
次のスクリーンショットは、新しくリストされたテンプレートを示しています。


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-1C1
Template Display Name
Schema Version
EFS Recovery Agent 1
Enrollment Agent 1
Enrollment Agent (Computer) 1
Exchange Enrollment Agent (Offline requ... 1
Exchange Signature Only 1
Exchange User 1
IPSec 1
IPSec (Offline request) 1
Kerberos Authentication 2
Key Recovery Agent 2
OCSP Response Signing 3
RAS and IAS Server 2
Root Certification Authority 1
Router (Offline request) 1
Smartcard Logon
Smartcard User 1
Subordinate Certification Authority 1
Trust List Signing 1
User 1
User Signature Only 1
Web Server 1
Workstation Authentication 2
True SSO Enrollment Agent 2

3 同じ証明書テンプレート コンソールで、True SSO スマートカード ログイン テンプレートを構成します。

a 証明書テンプレート コンソールで、リストされている [スマート カード ログオン] テンプレートを右クリックし、[テンプレートの複製] を選択します。

次のスクリーンショットは、Window Server 2016 を実行しているシステムでこの手順を示しています。



[新規テンプレートのプロパティ] ウィンドウが表示されます。

b 次のセクションの説明に従って、ウィンドウのタブに情報を入力します。

注意： 必ずこれらの事項に従います。従わないと、必要な値を設定できなくなり、手順をキャンセルしてやり直すことになります。この要件は、Windows システムの動作です。

- 次の箇条書きで説明するように、3 つのタブで必要な設定を決められた所定の順序で行うまでは、[プロパティ] ウィンドウの [適用] および [OK] をクリックしないでください。

  ウィンドウで適用または保存する前に、以下で説明する 3 つのタブの設定を構成するというこのガイダンスに従わない場合、Windows で [暗号化] タブの [プロバイダーのカテゴリ] が強制的に読み取り専用になりますが、この設定は後から True SSO に必要な [キー格納プロバイダー] 設定に変更することはできません。

  したがって、ウィンドウで適用または保存する前に、以下の 3 つのタブで構成を正確に正しい順序で完了する必要があります。

- これらのタブを、最初に構成を行うタブとして構成し、次の特定の順序で構成します。

  a [互換性] タブ

  b [全般] タブ

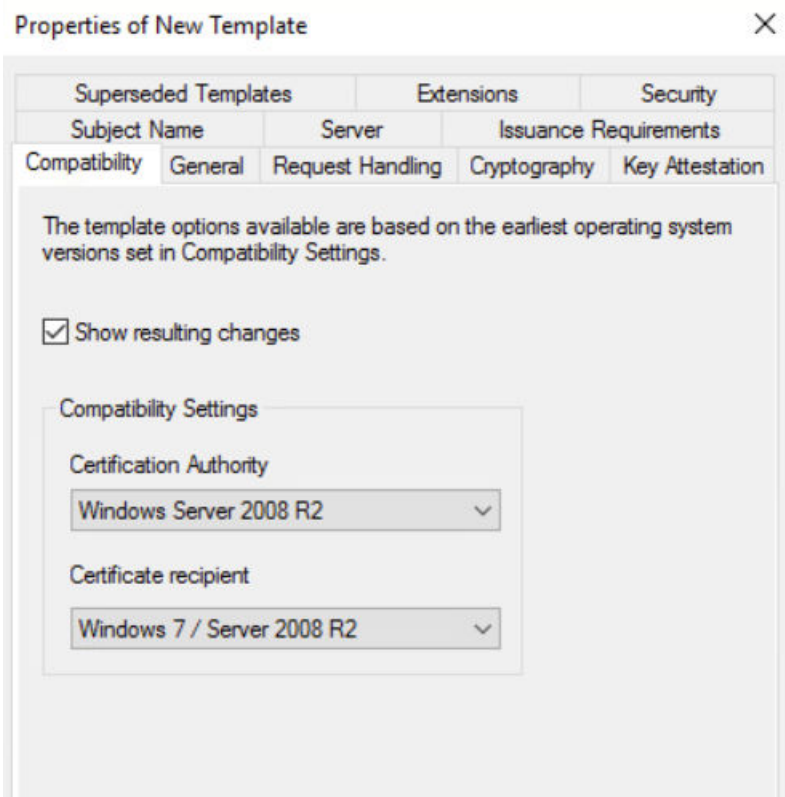
  c [暗号化] タブ

この順序が指定されている理由は、[互換性] タブで設定を変更するにつれて、システムによって関連するオ

[互換性] タブ

注： [互換性] タブでこれらの選択を行い、[暗号化] タブで適切なオプションを使用できるようにする必要があります。

- [変更の結果を表示] チェック ボックスをオンにします。
- [認証局]：Microsoft Windows がこの設定で提供しているオプションが表示されます。True SSO の要件を満たすには、[Windows Server 2008 R2] を選択するか、メニューに表示されるそれ以降のリリースのいずれかを選択します。
- [証明書の受信者]：Microsoft Windows がこの設定で提供しているオプションが表示されます。True SSO の要件を満たすには、[Windows 7 /Server 2008 R2] を選択するか、メニューに表示されるそれ以降のリリースのいずれかを選択します。



[全般] タブ

重要： True SSO テンプレートの名前には ASCII 文字のみを使用します。この既知の問題により、True SSO テンプレート名に 非 ASCII 文字または拡張 ASCII 文字が含まれていると Horizon Cloud 環境で True SSO を正しく設定できません。

テンプレートの表示名

この新しいテンプレートが True SSO で使用されることを示す名前（**`True SSO`** など）を入力します。

テンプレート名

前の [テンプレートの表示名] に入力すると、ツールによってその名前がスペースなしの [テンプレートの表示名] の入力と一致するように自動的に入力されます。

たとえば、**テンプレートの表示名** に [True SSO] と入力した場合、ツールはこの [True SSO] を自動的に テンプレート名 に設定します。

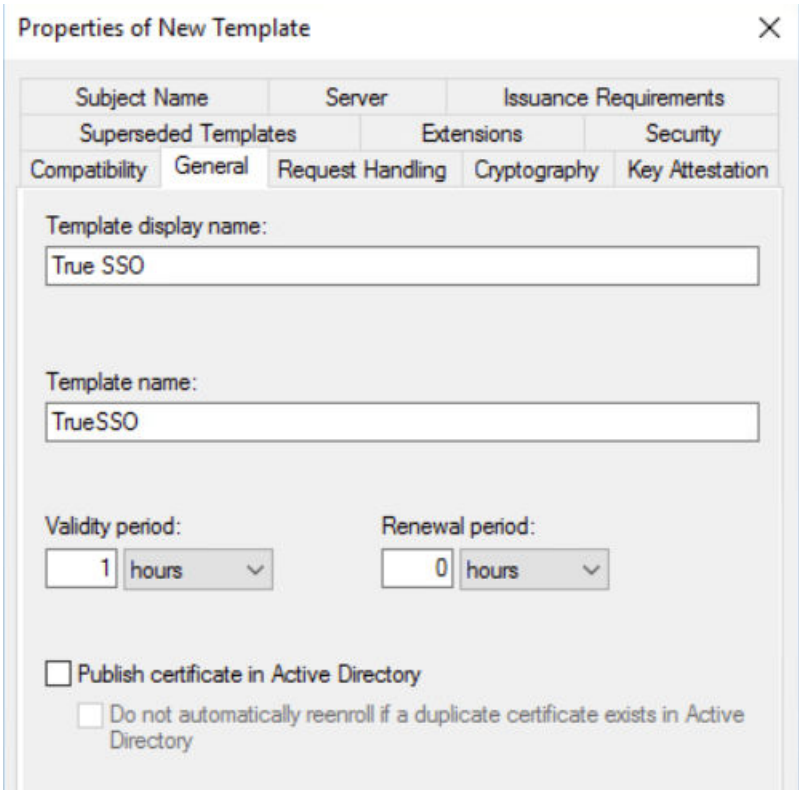
有効期間

1 時間（1 時間）

更新期間

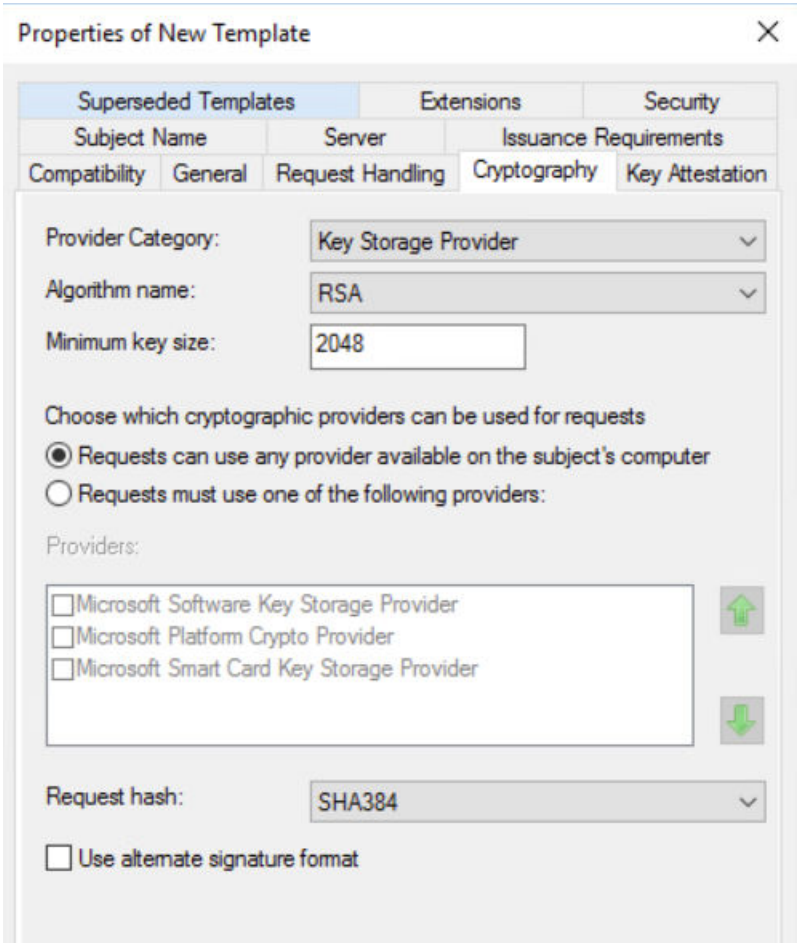
0 週間 (ゼロ週間)

次のスクリーンショットは、[テンプレート表示名] に **`True SSO`** として入力した後のこのタブを示しています。



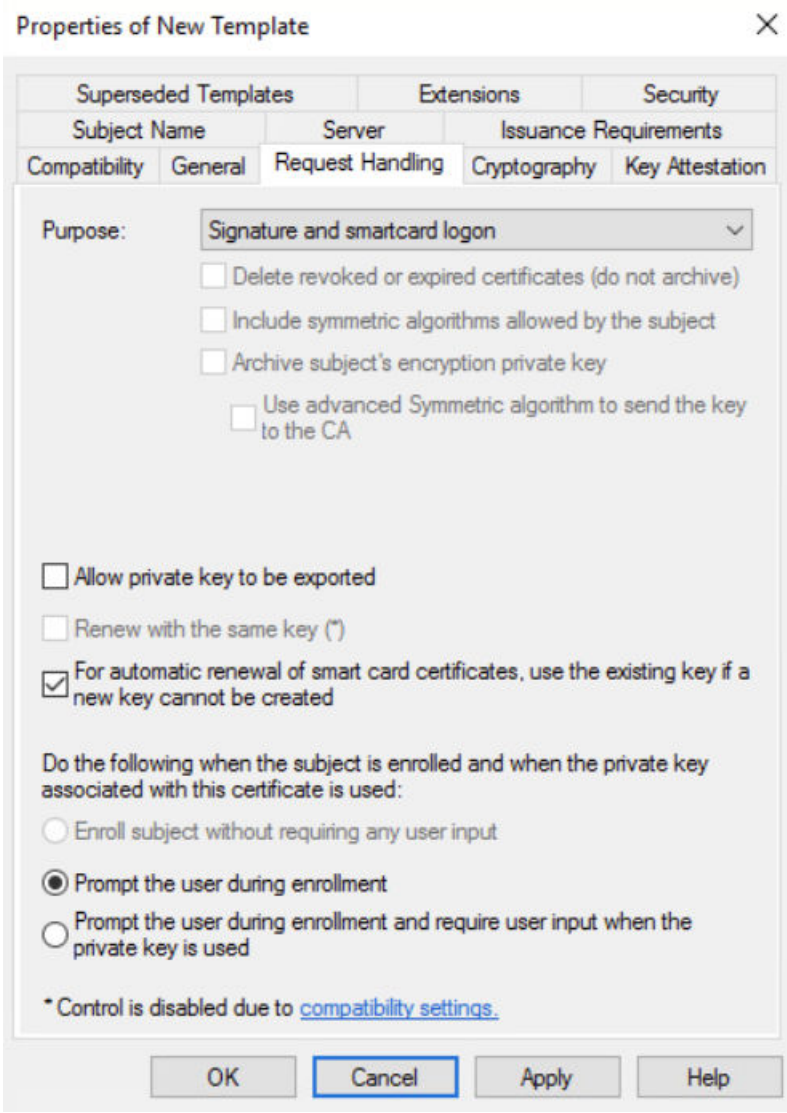
[暗号化] タブ

- [プロバイダのカテゴリ] - [キー ストレージ プロバイダ]
- [アルゴリズム名] - [RSA]
- [キーの最小サイズ] - [2048]
- [サブジェクトのコンピューターで利用可能な任意のプロバイダー] ラジオ ボタンを選択します。
- [ハッシュの要求] - [SHA384]



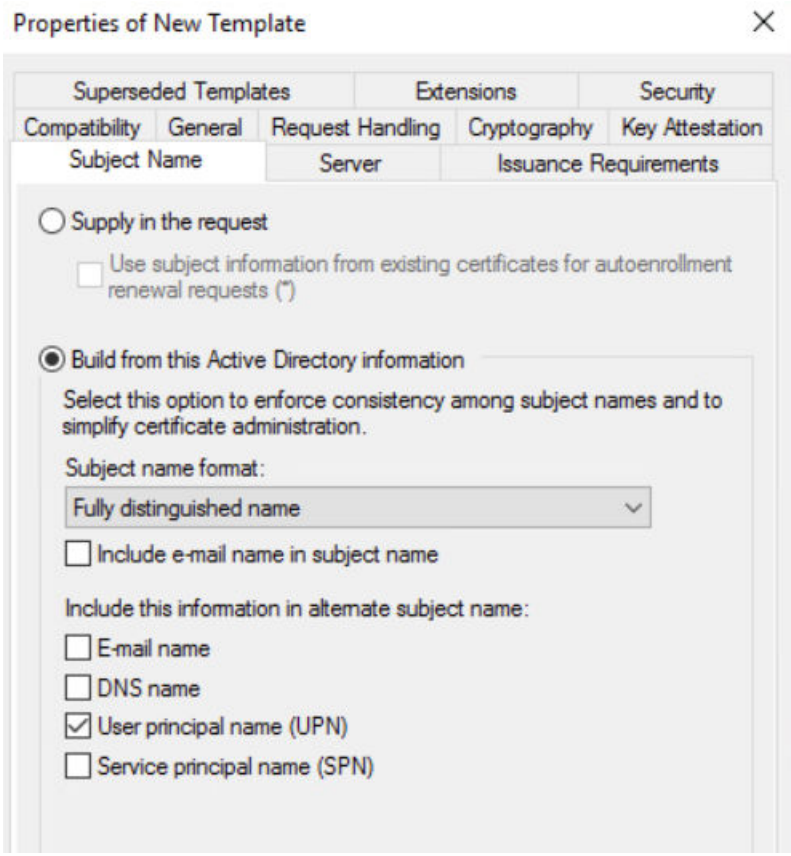
[要求の処理] タブ

- [目的] - [署名とスマートカード ログイン]
- [スマート カード証明書の自動書き換えで、新しいキーを作成できない場合は既存のキーを使用する] チェック ボックスをオンにします。
- [登録時にユーザーにプロンプトを表示] ラジオ ボタンをオンにします。



[サブジェクト名] タブ

- [Active Directory の情報から構築する] ラジオ ボタンをオンにします。
- [サブジェクト名の形式] - [完全識別名 (DN)]
- [ユーザー プリンシパル名 (UPN)] チェック ボックスをオンにします。



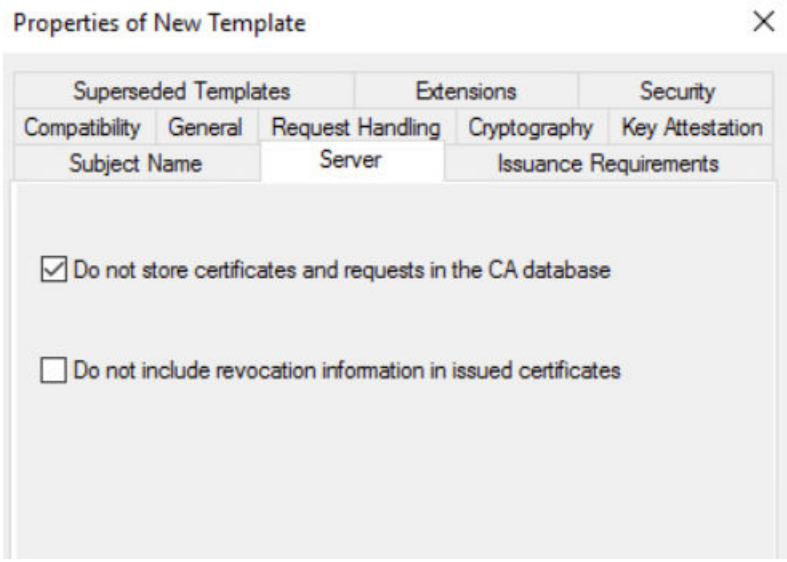
サーバ タブ

[CA データベース内に証明書および要求を保存しない] チェック ボックスをオンにします。

重要： [発行される証明書に失効情報を含めない] というラベルの付いた 2 番目のチェック ボックスを必ずオフにします。

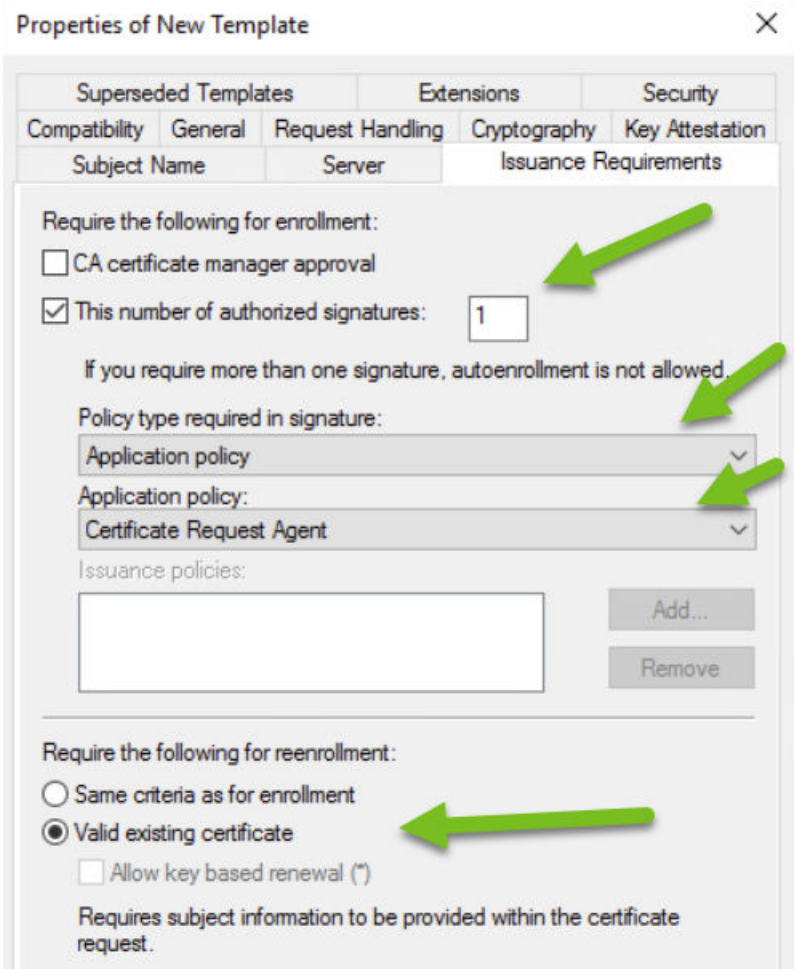
最初のチェック ボックスをオンにすると、[発行される証明書に失効情報を含めない] が自動的にオンになります。

2 番目のチェック ボックス [発行される証明書に失効情報を含めない] を必ずオフにします。



[発行の要件] タブ

- [登録には以下が必要] - [認証された署名の数] を選択して **1** を入力。
- [署名に必要なポリシー タイプ] - [アプリケーション ポリシー]
- [アプリケーション ポリシー] - [証明書要求エージェント]
- [次の項目を再登録の要件とする] - [既存の有効な証明書]

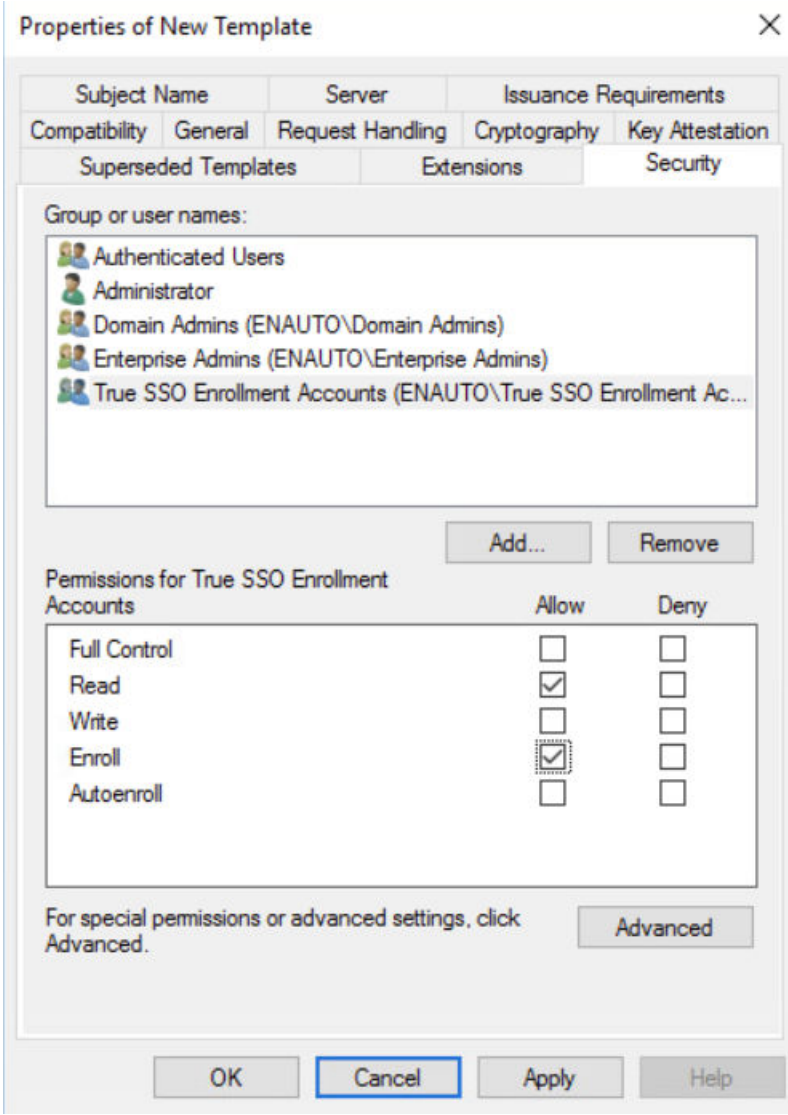


[セキュリティ] タブ

[セキュリティ] タブで、True SSO 登録アカウント用に作成した新しいユニバーサル セキュリティ グループに `Read` 権限と `Enroll` 権限を付与します。

1 [グループまたはユーザー名] セクションで、True SSO 登録アカウント用に作成したグループを追加します。

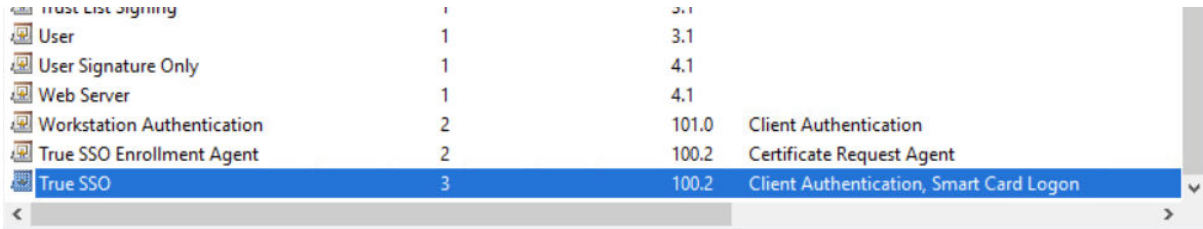
2 そのグループを選択し、[権限] セクションで `Read` 権限と `Enroll` 権限の [許可] を選択します。



c 新しい True SSO テンプレートの [プロパティ] ウィンドウで [OK] をクリックして、この新しい True SSO テンプレートの保存を完了します。

新しい True SSO テンプレートは、証明書テンプレート コンソール内にリストされ、指定した [テンプレートの表示名]を使用して表示され、クライアント認証、スマート カード ログインの目的も表示されます。

次のスクリーンショットは、新しくリストされたテンプレートを示しています。

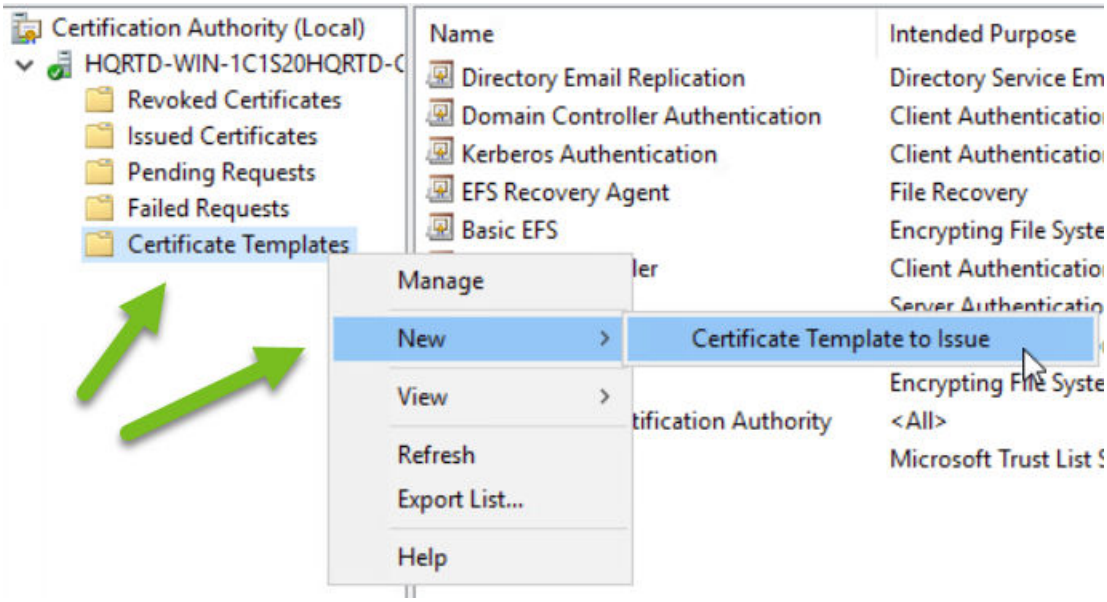


4 これで、証明書テンプレート コンソールを閉じて、認証局ツールに戻ることができます。

5 True SSO のテンプレートを発行します。

a 認証局ツールで、証明書テンプレート フォルダを右クリックし、[新規作成] - [発行する証明書テンプレート] を選択します。

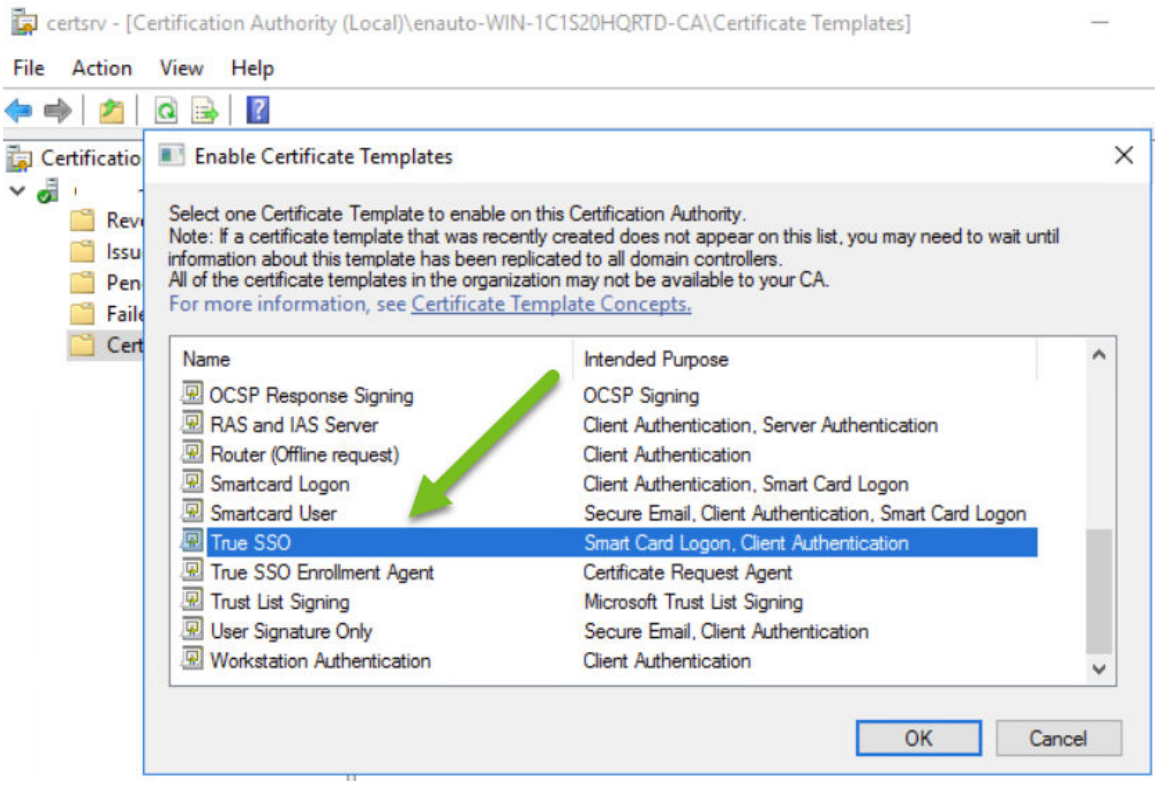
次のスクリーンショットは、Window Server 2016 を実行しているシステムでこの手順を示しています。



[証明書テンプレートを有効にする] ウィンドウが表示されます。

b 前の手順で作成した True SSO テンプレートを選択し、[OK] をクリックします。

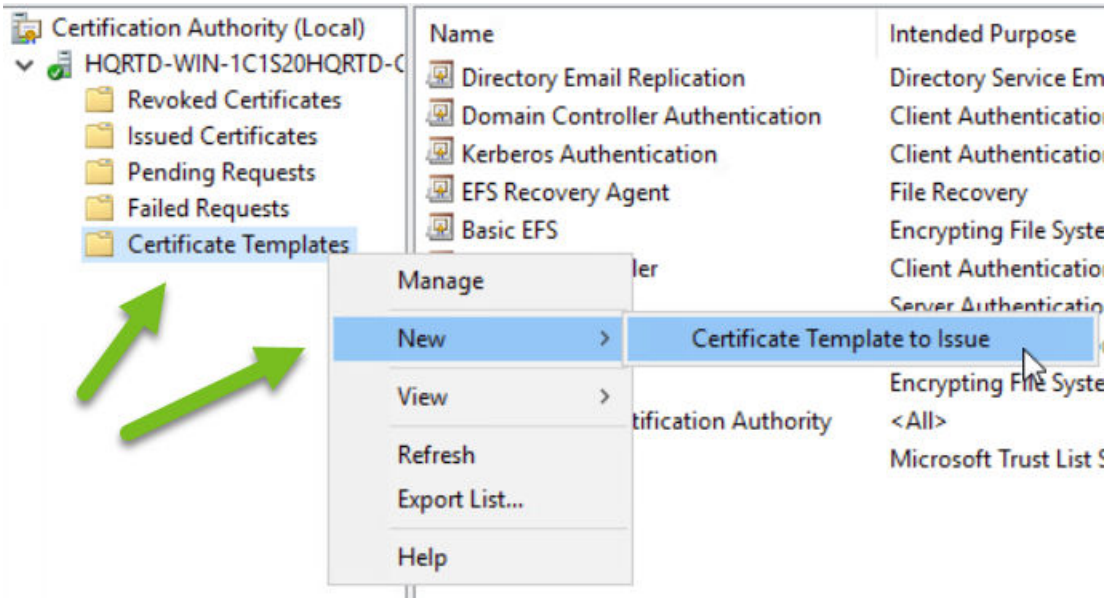
次のスクリーンショットは、Window Server 2016 を実行しているシステムでこの手順を示しています。



重要： これらのアクションは、True SSO 機能に使用するすべての Microsoft Enterprise Certificate Authority インスタンスで実行する必要があります。

6 True SSO 登録エージェント テンプレートに対して、同じ発行手順を繰り返します。

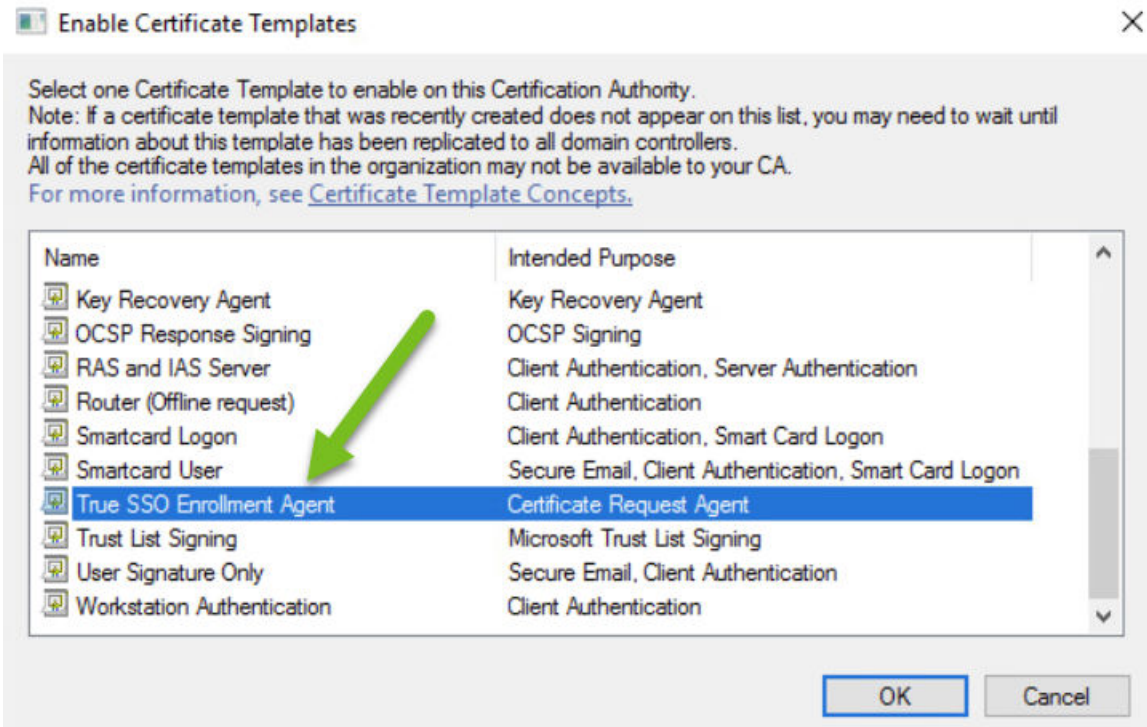
a 認証局ツールで、証明書テンプレート フォルダを右クリックし、[新規作成] - [発行する証明書テンプレート] を選択します。



[証明書テンプレートを有効にする] ウィンドウが表示されます。

b 上記の手順で作成した True SSO 登録エージェント テンプレートを選択し、[OK] をクリックします。

次のスクリーンショットは、Window Server 2016 を実行しているシステムでこの手順を示しています。



重要： これらのアクションは、True SSO に使用するすべての Microsoft Enterprise Certificate Authority インスタンスで実行する必要があります。

これで、Microsoft Enterprise Certificate Authority が設定され、True SSO 機能で使用するために必要な証明書テンプレートを使用して構成されました。

Horizon Edge で True SSO を使用するための Horizon Cloud Service - next-gen への SSO 構成の追加

このドキュメント ページでは、Horizon Edge で True SSO 機能の使用を構成する SSO 構成を追加する手順について説明します。Horizon Universal Console を使用して SSO 構成を追加し、その SSO 構成を Horizon Edge に関連付けます。

SSO を使用するデスクトップをユーザーが起動する各ドメイン フォレストに SSO 構成を追加します。

これらの手順は Horizon Universal Console を使用して実行します。

同じフォレストに複数の True SSO 構成を作成できます。ドメインは、1 つの True SSO 構成にのみ関連付けることができます（つまり、1 つの True SSO 構成にのみ追加されます）。

このシナリオでは、ユーザーがデスクトップまたはリモート アプリケーションを起動すると、システムは次の基準に基づいて、使用する True SSO 構成を優先順位で選択します。

1 ユーザーのドメインを含む True SSO 構成。

2 ユーザーのドメインと同じフォレストからの True SSO 構成。

注： Microsoft Azure で Horizon Edge により SSO を使用するためにサポートされる認証局タイプで説明されているように、True SSO 機能では、Horizon Universal Console は [Microsoft CA] ラベルを使用します。[Microsoft CA] ラベルを見たら、ラベルが True SSO 機能に関連付けられていることに注意してください。

前提条件

ユーザーまたはチームが次のタスクを完了していることを確認します。

- この SSO 構成で選択する Active Directory ドメインにドメイン登録アカウントを作成します。Active Directory ドメインの設定 画面で説明されているように、ドメイン登録アカウントは、True SSO 機能が Microsoft AD CS (Active Directory Certificate Services) から短期証明書を取得するために使用する登録サービス アカウントです。True SSO は認証に証明書を使用し、ユーザーに Active Directory 認証情報の入力を求めるプロンプトを表示しないようにします。コンソールでは、ドメイン登録アカウント、登録サービス アカウント、およびドメイン登録サービス アカウントという用語が同じ意味で使用されている場合があります。
- 少なくとも 2 つのドメイン参加エンタープライズ CA が構成されており、True SSO に使用できることを確認します。
- Active Directory ドメインにユニバーサル セキュリティ グループを作成し、Horizon Cloud を使用した True SSO に必要な証明書テンプレートの設定の説明に従って、それらのドメイン登録アカウントをそのグループに追加します。
- Horizon Cloud を使用した True SSO に必要な証明書テンプレートの設定の説明に従って、Microsoft Enterprise Certificate Authority で必要なテンプレートを作成する手順を完了します。

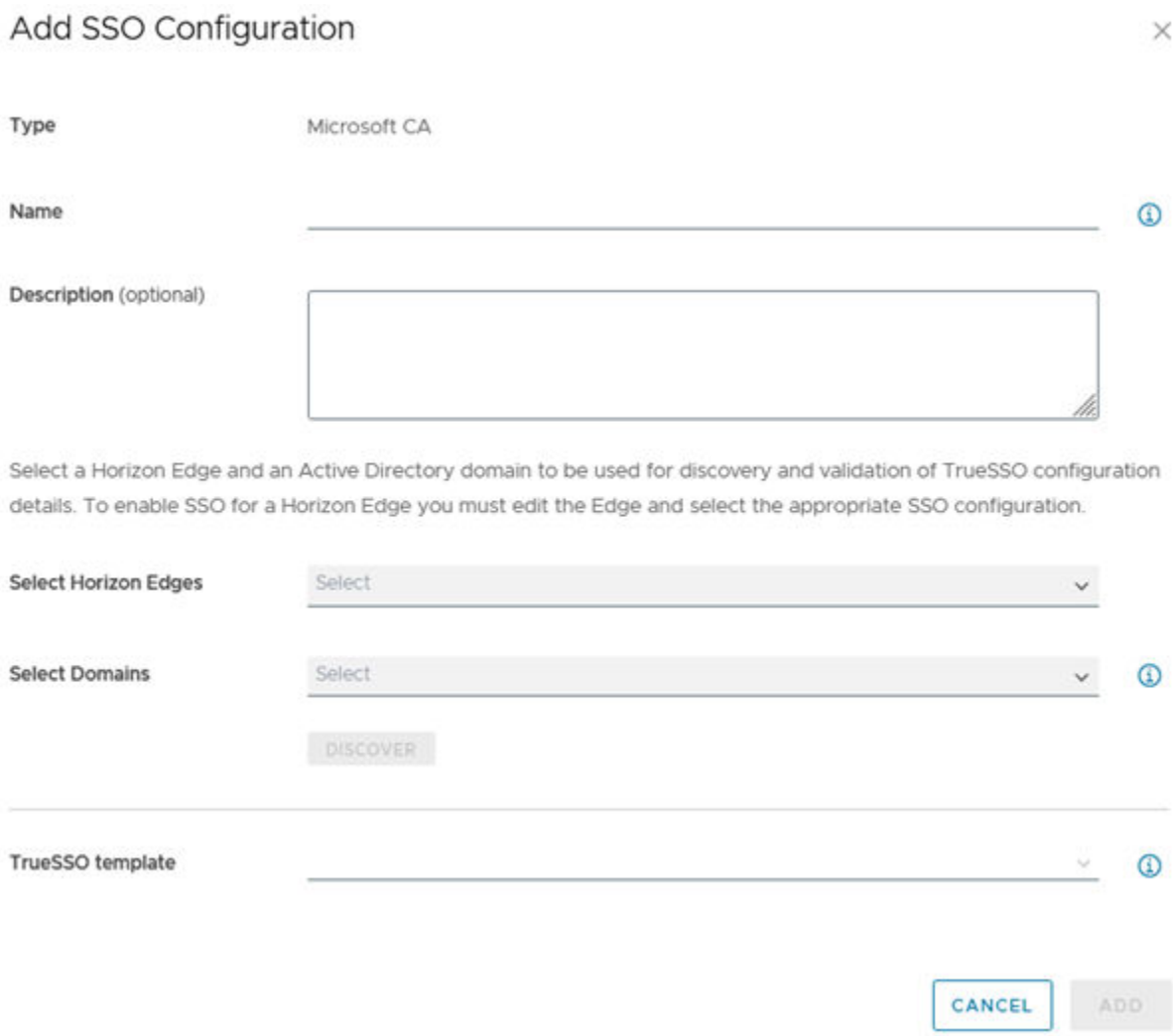
- この SSO 構成で選択する Active Directory ドメインの場合は、Active Directory ドメインの設定の説明に従って、Active Directory ドメイン登録の [ドメイン登録サービス アカウント] セクション内の登録アカウントを指定します。
- この True SSO 構成を適用する Horizon Edge を決定します。コンソールの [SSO 構成の追加] ユーザー インターフェイス フロー内で、次の手順で説明する Horizon Edge を選択します。

手順

1 ナビゲーション バーの [統合] をクリックします。

2 [ID とアクセス] タイルで [管理] をクリックします。

3 [SSO 構成] をクリックし、次に [追加] - [Microsoft CA] の順に選択して、[SSO 構成の追加] ページに移動します。



4 SSO 構成に一意の [名前] を追加します。

5 [Horizon Edge の選択] ドロップダウン メニューから Horizon Edge を選択します。

少なくとも 1 つの Horizon Edge を選択する必要があります。

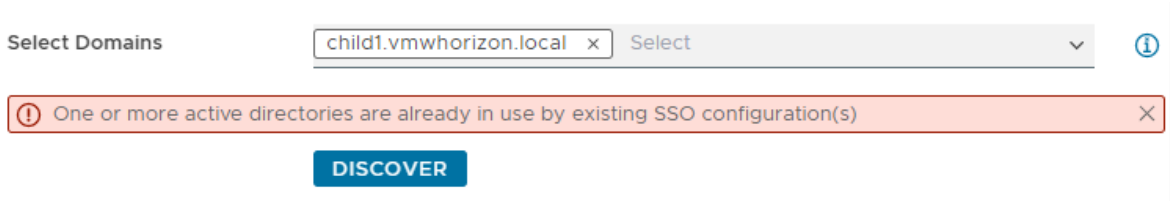
6 [ドメインの選択] ドロップダウン メニューから SSO 構成のドメインを選択し、[追加] をクリックします。

SSO 構成には複数のドメインを追加できます。ドメインは、同じ Active Directory フォレストに属している必要があります。

このメニューでは、コンソールに環境に登録されているすべてのドメインが一覧表示されます（コンソールの [ID とアクセス] ページの [ドメイン] タブに表示されます）。

ただし、この新しい SSO 構成レコードに選択する各ドメインは、システムにすでに保存されている別の SSO 構成内ですでに使用されているものにはしないでください。

別の SSO 構成でまだ指定されていないドメインを選択する必要があります。次のスクリーンショットに示すように、[検出] をクリックすると、ユーザー インターフェイスはこの事実を検証します。この文書の作成時点では、次のように検証メッセージが表示されます。



7 [検出] をクリックして、選択内容を検証します。

[検出] をクリックすると、システムは、このページの上部で説明されている次のような多くの前提条件を検証します。

- 選択したドメインのいずれかが別の SSO 構成ですでに使用されているか?
- 選択したドメインには、ドメイン登録（コンソールの [ID とアクセス] ページの [ドメイン]タブにリストされている登録）で登録サービス アカウントが指定されているか?
- システムは、True SSO の要件に従って、自分またはチームが構成した Microsoft Enterprise Certificate Authority で必要な証明書テンプレートを見つけられるか?

すべてのドメインでシステムの検証が成功した場合、ユーザー インターフェイスは選択した次のメニューを使用できるようにします。

8 [TrueSSO テンプレート] および [登録エージェント テンプレート] ドロップダウン メニューでは、デフォルトの選択を受け入れるか、いずれかまたは両方のメニューから別のテンプレートを選択します。

注： 選択した 2 つのテンプレートに共通の認証局インスタンスがある場合は、[認証局] ドロップダウン メニューに表示されます。

9 [追加] をクリックして、システムへの新しい SSO 構成の保存を完了します。

結果

システムは、選択した Horizon Edge に SSO 設定を送信します。

注： [SSO 構成] ページでは、True SSO 構成がページに一覧表示され、[タイプ] 列の値として「Microsoft CA」が設定されています。また、Microsoft CA 構成の場合、認証局モードと証明書の有効期限は適用されないため、[認証局モード] 列と [証明書の有効期限] 列は空白のままになります。

次のステップ

SSO 構成が完了したら、その SSO 構成を特定の Horizon Edge に関連付けることができます。[キャパシティ] - [Horizon Edge] を選択し、新しく追加した SSO 構成を関連付ける Horizon Edge を選択して、[編集] をクリックします。[Horizon Edge を編集] ウィザードで、ウィザードの各手順で [次へ] をクリックし、[Horizon Edge Gateway] セクションに移動し、[SSO を使用] トグルを選択して有効にします。新しく追加した SSO 構成の名前を選択し、必要に応じて [次へ] をクリックしてウィザードを完了します。

Horizon Edge が提供するエンド ユーザー デスクトップおよびリモート アプリケーションに対して True SSO の使用を指定できます。デスクトップおよびリモート アプリケーションでの SSO の使用の指定は、プール グループ レベルで設定されます。Horizon Universal Console [リソース] ナビゲーションを使用して関連するプール グループに移動し、関連するプール グループを編集して各プール グループで SSO を有効にします。

コンソールを使用して特定の Horizon Edge で設定された SSO 構成を確認するには、[キャパシティ] - [Horizon Edges] の順に移動し、Horizon Edge の名前を選択して、詳細ページを表示します。

Horizon Cloud Service - next-gen で SSO に VMware CA を使用する

VMware Certificate Authority (CA) を使用してエンド ユーザーにデスクトップおよびアプリケーションへのシングル サインオン (SSO) アクセスを提供するには、VMware CA を使用して、SSO の一時的なスマートカード証明書を発行します。透明性とセキュリティを確保するため、このプロセスには確立された Microsoft ユーティリティを使用する PowerShell スクリプトが含まれています。

次のリストには、VMware CA の構成に関する情報が記載されています。SSO を構成する場合は、以下のトピックで説明するように、コンテキストの中で同じ詳細情報の多くが表示されます。たとえば、Horizon Cloud Service - next-gen への VMware CA 向けの SSO 構成の追加には VMware CA バンドルをダウンロードする手順が記載されています。このバンドルには、Active Directory フォレストへの VMware SSO CA バンドルの公開の指示に従って SSO を構成するために実行する VMware PowerShell スクリプトが含まれています。

- VMware CA で SSO に必要な機能を有効にするには、次のいずれかの状況が Active Directory フォレストに適用される必要があります。
  - Active Directory フォレストに少なくとも 1 つのオンライン Microsoft Enterprise CA が構成されている。この場合、次の結果が発生します。
    - Microsoft Enterprise CA は、その CA 証明書と証明書失効リスト (CRL) をフォレストに自動的に公開する。
    - ドメイン コントローラが証明書の登録を自動的に実行する。
  - Active Directory フォレストがサードパーティの CA またはスタンドアローンの Microsoft CA を使用する。この場合、次の状況が適用される必要があります。
    - すべての CA 証明書を、`certutil` などのユーティリティを使用してフォレストに手動で公開する必要がある。
    - 失効情報は HTTP 経由で常に使用できる必要がある。
    - ドメイン コントローラは、クライアント認証、サーバ認証、スマート カード ログイン、および KDC 認証を許可する証明書を使用して発行する必要がある。
- VMware CA は、ルート CA または中間 CA として構成できます。ただし、公開鍵基盤 (PKI) のベスト プラクティスは、中間 CA を選択することです。

- ルート CA を使用する場合、VMware CA 証明書は 5 年間有効です。
- 中間 CA を使用する場合、発行元の CA によって VMware CA 証明書の有効期間が決まります。
- 中間 CA を使用する場合、VMware CA 証明書は Microsoft CA または任意のサードパーティ CA によって署名できます。
- サードパーティ CA を使用する場合は、ドメイン メンバー マシンが、VMware CA 証明書を検証するために必要なすべての証明書と失効情報にアクセスできることを確認します。
- VMware CA を信頼するには、Active Directory フォレストのさまざまな場所に VMware CA バンドルを公開する必要があります。
- VMware CA バンドルを公開するには、ドメイン メンバー マシンの適切な権限を持つ管理者として VMware PowerShell スクリプトを実行します。
- VMware PowerShell スクリプトは 1 回のみ実行する必要があります。Active Directory は公開された PKI データを、Active Directory フォレスト内のすべてのドメインのすべてのドメイン コントローラおよびデスクトップにレプリケートします。複雑な Active Directory 環境で `Repadmin` などのユーティリティを使用すると、SSO を試行する前に、異なるドメインまたはサイト内のドメイン コントローラ間で構成の名前付けコンテキストをタイムリーにレプリケートできます。
- PowerShell スクリプトは、完全な透明性のために Microsoft ユーティリティ `certreq` と `certutil` を使用します。PowerShell スクリプトを実行する前に、スクリプトを読んで、その動作を正確に確認できます。

VMware CA を使用し、複数のフォレストに適用できる SSO 構成用に Active Directory を準備する

Horizon Cloud に SSO を構成する場合は、VMware 認証局 (CA) の構成の詳細に応じて、後続の適切なタスクを実行する必要があります。

後続の手順の概要

SSO バンドルを作成する場合は、PowerShell スクリプトを使用して、バンドルが作成されたフォレストにバンドルを公開します。このアクションにより、SSO がバンドルのフォレストで確実に機能するようになります。

SSO を追加の信頼するフォレストと連携させるには、次のように、VMware CA の認証パスからのルート証明書と中間証明書を信頼するフォレストに公開する必要があります。

- ルート CA 証明書を信頼するフォレストに公開する必要があります。
- 中間 CA 証明書を信頼するフォレストに公開する必要があります。
- ルート CA 証明書を NTAuth ストアに公開する必要があります。
- 失効情報は、証明書チェーン全体で HTTP 経由で常に使用できる必要があります。

信頼されたルート証明機関にルート証明書を追加する

VMware CA 証明パスの終端にあるルート証明書は、Active Directory の信頼されたルート証明機関グループ ポリシーに追加する必要があります。

手順

1 信頼構成の一部であるすべての Active Directory フォレストで、信頼されたルート証明機関にルート証明書を追加します。

a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。

b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。

2 [コンピュータの構成] セクションを展開し、[Windows 設定] > [セキュリティ設定] > [公開鍵] の順に開きます。

3 [信頼されたルート証明機関] を右クリックして、[インポート] を選択します。

4 ウィザードの指示に従ってルート証明書（`rootCA.cer` など）をインポートし、[OK] をクリックします。

5 [グループ ポリシー] ウィンドウを閉じます。

結果

ドメイン内のすべてのシステムの信頼されたルート ストアに、ルート証明書がコピーされます。

次のステップ

中間証明機関（CA）がスマート カードのログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory で中間証明機関のグループ ポリシーに中間証明書を追加します。中間証明機関に中間証明書を追加するを参照してください。

中間証明機関に中間証明書を追加する

VMware CA 証明パスのすべての中間証明書は、Active Directory の中間証明機関グループ ポリシーに追加する必要があります。

手順

1 信頼構成の一部であるすべての Active Directory フォレストで、VMware CA 証明書チェーンに含まれるすべての中間証明書を中間証明機関に追加します。Active Directory サーバで、Group Policy Management プラグインに移動し、次の操作を行います。

a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。

b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。

2 [コンピュータの構成] セクションを展開し、[Windows Settings\Security Settings\Public Key] のポリシーを開きます。

3 [中間証明機関] を右クリックして、[インポート] を選択します。

4 ウィザードの指示に従って中間証明書（`intermediateCA.cer` など）をインポートし、[OK] をクリックします。

5 [グループ ポリシー] ウィンドウを閉じます。

結果

ドメイン内のすべてのシステムの中間証明機関ストアに、中間証明書がコピーされます。

Enterprise NTAuth ストアにルート証明書を追加する

VMware CA 証明パスの終端にあるルート証明書は、Active Directory の Enterprise NTAuth ストアに追加する必要があります。

手順

- Active Directory サーバで、`certutil` コマンドを使用して、証明書を Enterprise NTAuth ストアに発行します。

  例：**`certutil -dspublish -f` *`ルート CA 証明書へのパス`* `NTAuthCA`**

結果

CA がこの種の証明書の発行元として信頼されるようになります。

Horizon Cloud Service - next-gen への VMware CA 向けの SSO 構成の追加

VMware CA 向けの SSO 構成を追加して、Horizon Edge Gateway に展開できます。

SSO を使用するデスクトップをユーザーが起動する各ドメイン フォレストに SSO 構成を追加します。

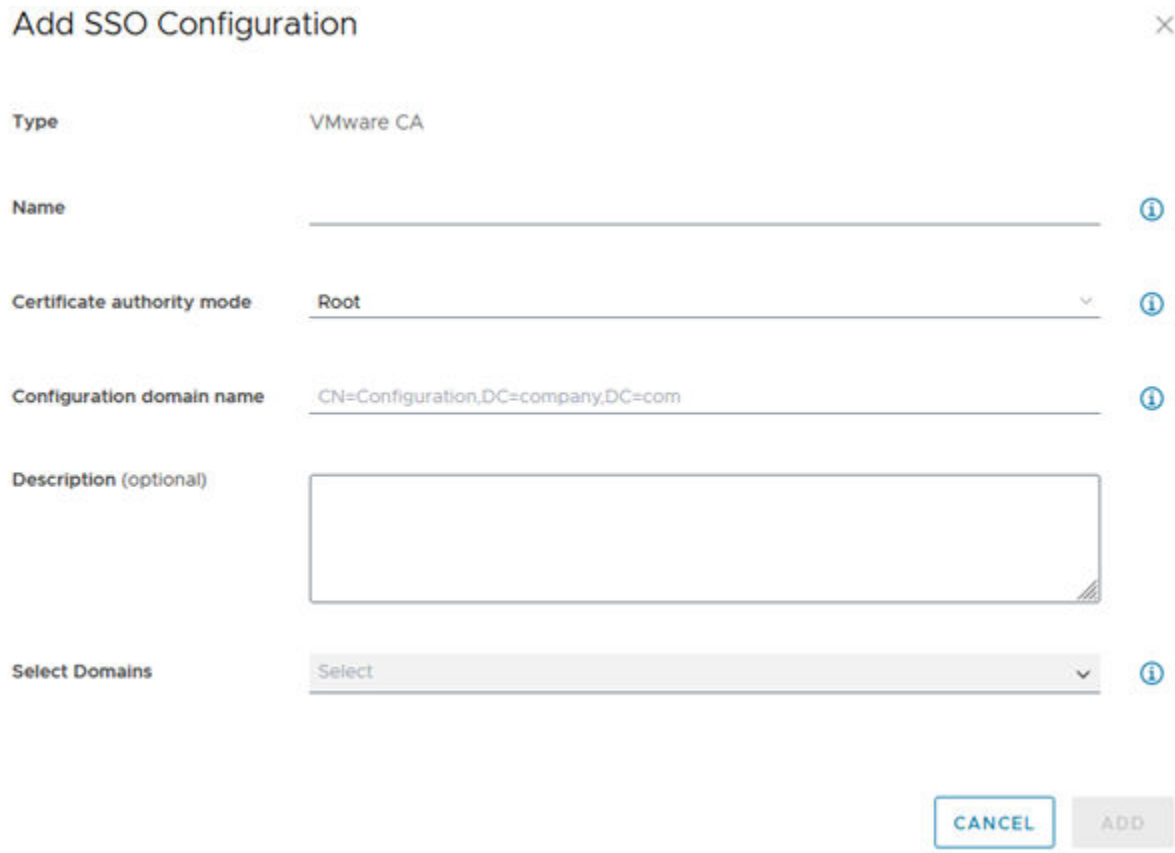
前提条件

VMware CA、ルート CA、または中間 CA に使用する認証局モードを決定します。Horizon Cloud Service - next-gen で SSO に VMware CA を使用するを参照してください。

手順

1. ナビゲーション バーの [統合] をクリックします。
2. [ID とアクセス] タイルで [管理] をクリックします。

3 [SSO 構成] をクリックし、次に [追加] - [VMware CA] の順に選択して、[SSO 構成の追加] ページに移動します。



4 SSO 構成に一意の [名前] を追加します。

5 [認証局] モード（[ルート] または [中間]）を選択し、ダウンロードして Active Directory サーバにインストールする認証局 (CA) バンドルのタイプを決定します。

ルート モードでは、自己署名のルート証明書を使用して CA バンドルが作成されます。中間モードでは、証明書署名リクエスト (CSR) ファイルを使用して CA バンドルが作成されます。PowerShell スクリプトにはユーザー インターフェイスが表示され、管理者は証明書を取得するために CSR が送信される Enterprise CA を選択できます。

6 [構成ドメイン名] を追加して、SSO 構成の Active Directory フォレストの構成の名前付けコンテキストを決定します。

[構成ドメイン名] は通常、CN=Configuration とフォレスト ルート ドメインの相対識別名で構成されます (CN=Configuration,DC=company,DC=com)。構成の名前付けコンテキストを特定するには、ドメインに参加しているマシンに接続し、PowerShell コマンド `"C:> Get-ADRootDSE -Server "`. を実行します。

7 SSO 構成の [ドメイン] を選択し、[追加] をクリックします。

SSO 構成には複数のドメインを追加できます。ドメインは同じ Active Directory フォレストに属している必要があります。各ドメインは、1 つの SSO 構成にのみ含めることができます。

8 SSO 構成を追加したら、そのメニュー（縦に並んだ 3 つのドット）をクリックし、認証局 (CA) バンドルをダウンロードして Active Directory にインストールします。

次のステップ

- ダウンロードしたバンドルを公開します。Active Directory フォレストへの VMware SSO CA バンドルの公開を参照してください。
- VMware SSO CA 証明書の有効期限が切れる前に、新しい CA バンドルを要求します。

  注： CA 証明書の有効期限が近づいていることを示す通知が Horizon Universal Console に表示されます。

  - CA 証明書の有効期限は、[SSO 構成] ページの [証明書の有効期限] 列で確認できます。
  - [SSO 構成] ページでは、SSO 構成のメニュー（縦に並んだ 3 つのドット）をクリックし、[新しい CA バンドルの生成] を選択することで、CA バンドルをいつでもリクエストできます。このアクションにより、CA バンドルが生成され、システムにダウンロードされます。Active Directory フォレストへの VMware SSO CA バンドルの公開を参照してください。
- SSO 構成が完了したら、その SSO 構成を特定の Horizon Edge に関連付けることができます。[キャパシティ] - [Horizon Edge] を選択し、新しく追加した SSO 構成を関連付ける Horizon Edge を選択して、[編集] をクリックします。[Horizon Edge を編集] ウィザードで、ウィザードの各手順で [次へ] をクリックし、[Horizon Edge Gateway] セクションに移動し、[SSO を使用] トグルを選択して有効にします。新しく追加した SSO 構成の名前を選択し、必要に応じて [次へ] をクリックしてウィザードを完了します。

Active Directory フォレストへの VMware SSO CA バンドルの公開

エンド ユーザーにデスクトップおよびアプリケーションへのシングル サインオン (SSO) アクセスを提供するには、対応する Horizon Edge Gateway インスタンスで SSO を管理します。

この手順により、エンド ユーザーは認証情報を一度入力した後でデスクトップおよびアプリケーションにアクセスできます。

VMware CA の構成の背景情報については、Horizon Cloud Service - next-gen で SSO に VMware CA を使用するを参照してください。

この手順を完了するには、必要に応じて Microsoft のドキュメントを参照してください。たとえば、エンタープライズ CA をインストールする場合は、認証局のインストールを参照してください。

前提条件

- Horizon Universal Console を使用して、認証局 (CA) バンドルを作成およびダウンロードします。Horizon Cloud Service - next-gen への VMware CA 向けの SSO 構成の追加を参照してください。
- VMware CA バンドルから抽出された PowerShell スクリプトを実行するには、この手順で説明するように、適切な権限があることを確認します。

この手順では、VMware PowerShell スクリプトを実行する必要があります。Enterprise Admins グループのメンバーとしてスクリプトを実行するなど、VMware PowerShell スクリプトを実行するためのオプションがいくつかあります。次のガイダンスでは、強力でない権限を使用することが示されますが、Enterprise Admins グループのメンバーとしてスクリプトを実行できます。ここでは、次の権限があることを確認することをお勧めします。

- Active Directory の「パブリック キー サービス」コンテナに対するフル コントロールの権限。
- Active Directory の「SubCA」証明書テンプレートに対する登録権限。

手順

1 ドメイン メンバー マシンに接続し、CA バンドル ファイルをサーバにアップロードして、ファイルの内容を解凍します。

適切な権限があれば、任意のドメイン メンバー マシンから PowerShell スクリプトを実行できます。

2 PowerShell を開き、コマンドを実行して、次のサブステップの説明に従ってプロンプトに応答します。

重要： 環境が複数のドメイン コントローラで構成されている場合、またはリモート マシンからバンドルをインストールする場合、CA 証明書をすべてのドメイン コントローラに伝達するのに数時間かかる場合があります。すべてのドメイン コントローラ インスタンスで `'gpupdate.exe /Target:Computer /Force'` を実行することで、実行時間を短縮できます。

a 次のコマンドを実行します。

```
Unblock-File -Path Path to ps1 file
```

b CA バンドルから抽出された `ps1` PowerShell スクリプトを実行し、プロンプトに応答します。

例：`PS C:\ca\VmwAuthEngine-CA_1> .\VmwAuthEngine-CA_1.ps1`

SSO 構成を中間 CA として追加した場合は、VMware CA CSR に署名するための MSFT エンタープライズ CA を選択するように求められます。ルート CA または中間 MSFT エンタープライズ CA を選択して、VMware CA CSR を処理できます。該当する場合は、適切なエンタープライズ CA を選択します。選択したエンタープライズ CA の [Subordinate Certification Authority] テンプレートを有効にする必要があります。

次に示すように、必要な確認プロンプトに **`Y`** で応答します。

```
Confirmation required Do you want to publish to AD?
```

```
N] No [Y] Yes [?] Help (default is "N"):Y
```

結果

想定される結果は、スクリプトがエラーなしで実行されることです。ただし、次のタイプのエラーが発生した場合は、提案されるトラブルシューティングの手順を実行してください。

```
2022-03-22T15:35:39 [INFO ] [VmwAuthEngine-CA-62351bb62ff3dd5966ad3575-1.ps1,67] certutil.exe
-dspublish -f C:\SSO-C\Vmw
AuthEngine-CA-62351bb62ff3dd5966ad3575-1.crl
error : 2022-03-22T15:35:39 [ERROR][-2147016563][] Failed to publish base CRL
```

```
At C:\SSO-C\VmwAuthEngine-CA-62351bb62ff3dd5966ad3575-1.ps1:303 char:5
+     error $retCode "Failed to publish base CRL"
+     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,error
```

次の `Get-ADRootDSE` コマンドを実行し、出力を確認して、SSO 構成の作成に使用される CA 構成ドメイン名が、`configurationNamingContext` プロパティから返されるものと一致するかどうかを確認します。

```
C:\>
        Get-ADRootDSE -Server dnsDomainName
```

例：`C:\> Get-ADRootDSE -Server horizonv2.local`

出力：

```
configurationNamingContext       :  "CN=Configuration,DC=horizonv2,DC=local"
        ...other
        output fields...
```

CA 構成ドメイン名が出力と一致しない場合は、Horizon Universal Console を使用して SSO 構成を編集します。特に CA 構成ドメイン名を修正できます。SSO 構成へのアクセスの詳細については、Horizon Cloud Service - next-gen への VMware CA 向けの SSO 構成の追加を参照してください。SSO 構成を編集するには、SSO 構成の横にある縦に並んだ 3 つのドットをクリックし、[編集] を選択します。ドメイン名を修正したら、更新された CA バンドルをダウンロードして公開できます。

次のステップ

Horizon Edge Gateway をデプロイしたら、SSO 構成ステータスが適切に設定されていることを確認します。Horizon Universal Console で、[リソース] - [キャパシティ] を選択し、構成した Horizon Edge Gateway インスタンスの名前をクリックし、構成を編集して [SSO を使用] オプションを有効にします。SSO 構成を選択して、Horizon Edge Gateway に関連付けます。保存してステータスが READY_TO_SERVE に設定されていることを確認します。これは、SSO がエンド ユーザーに対して機能していることを示します。

ID プロバイダの接続

ドメイン情報が Horizon Cloud Service - next-gen で正常に保存されたら、エンド ユーザー認証とアクセスのために ID プロバイダを接続します。

次の情報は、ID プロバイダの接続に対する次のタスクに適用されます。

Microsoft Entra ID が ID プロバイダの場合、グローバル管理者権限を持つユーザーは次の操作を行う必要があります。

- 要求された権限を承認する。
- 組織全体の同意書を提供する。

- Entra ID アプリケーションが組織のデータにアクセスすることについての同意書を提供する。

Workspace ONE Access が ID プロバイダの場合、管理者権限を持つユーザーは次の操作を行う必要があります。

- 要求された権限を承認する。
- 組織全体の同意書を提供する。

手順

1 ナビゲーション バーの [統合] をクリックします。

2 [ID とアクセス] タイルで [管理] をクリックします。

3 [ID とアクセス] ページで、ドロップダウン メニューの [Microsoft Azure]、[Workspace ONE Access クラウド]、および [オンプレミスの Workspace ONE Access] から [ID プロバイダ] を選択します。

[Microsoft Azure]

a エンド ユーザーが資格にアクセスできるように、[ブローカ URL] の [テナント サブドメイン] を追加します。

[グローバル管理者] でない場合は、[リンクを生成] をクリックしてリンクを生成し、管理者と共有して承認を要求します。

b [接続] をクリックします。

c ページの内容を確認し、[同意する] をクリックして Horizon Universal Console に移動する権限を付与します。

プロンプトに従って次の手順を実行します。

[Workspace ONE Access クラウド]

a エンド ユーザーが資格にアクセスできるように、[ブローカ URL] の [テナント サブドメイン] を追加します。

b `yourcompany.workspaceoneaccess.com.` の形式で [Workspace ONE Access テナントの FQDN] を追加します。

c [接続] をクリックして、Horizon Universal Console に移動します。

[オンプレミスの Workspace ONE Access]

a エンド ユーザーが資格にアクセスできるように、[ブローカ URL] の [テナント サブドメイン] を追加します。

b `yourcompany.workspaceoneaccess.com.` の形式で [Workspace ONE Access テナントの FQDN] を追加します。

c オンプレミスの Workspace ONE Access で構成されている OAuth [クライアント ID] を入力します。

d オンプレミスの Workspace ONE Access で構成されている OAuth [クライアント シークレット] を入力します。

e [接続] をクリックして、Horizon Universal Console に移動します。

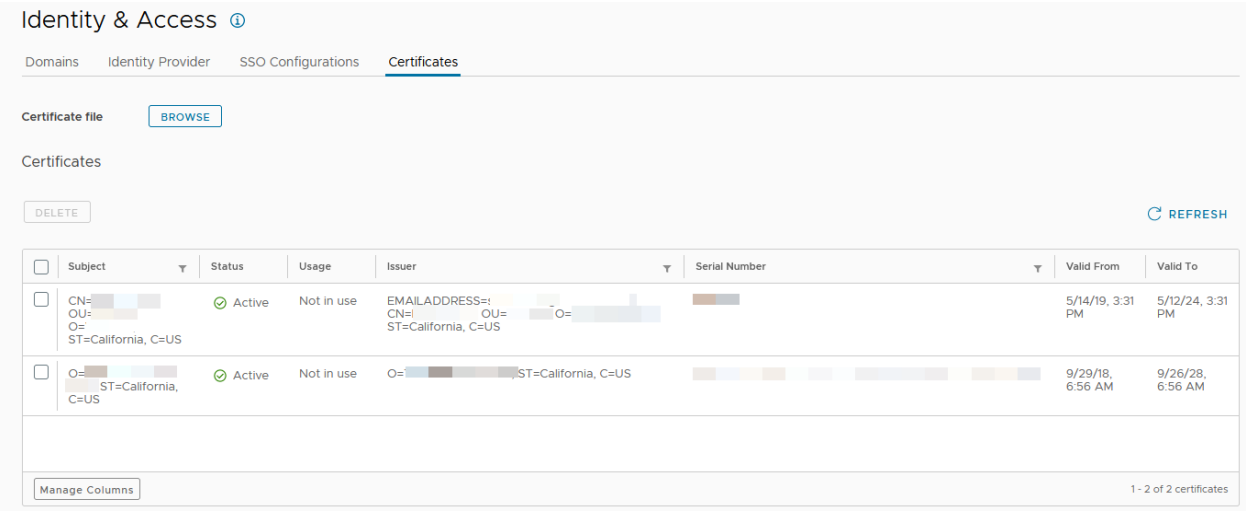
次のステップ

Horizon Edge を追加します。

LDAPS で使用する PEM 証明書の管理

Horizon Cloud Service - next-gen で LDAPS を使用するには、PEM でエンコードされたルート CA 証明書と中間 CA 証明書をアップロードする必要があります。これらの証明書は、後で [証明書] ページの Horizon Universal Console で管理できます。

PEM でエンコードされたルート CA 証明書と中間 CA 証明書は、Active Directory ドメインを構成するときにアップロードできます。これらの証明書は [証明書] ページで使用できます。このページには、左側のペインで [統合] をクリックし、[ID とアクセス] タイルで [管理] をクリックしてアクセスできます。



[証明書] ページでは、次の操作を実行できます。

- 既存のスナップショットを削除します。
- 証明書を追加します。

  証明書を追加するには、[参照] をクリックし、アップロードするシステム上の証明書を含む PEM でエンコードされたファイルを選択し、[証明書] ページに戻り、[アップロード] をクリックします。
- 列フィルタを使用して、既存の証明書を検索します。

注： [ステータス] 列を使用して、有効期限が間もなく切れる、またはすでに切れている証明書を確認し、新しい証明書をアップロードするか古い証明書を削除するかを判断します。

- [有効] - 証明書は有効で、まだ期限切れになりません。
- [まもなく期限切れ] - 証明書は 30 日以内に期限切れになります。
- [期限切れ] - 証明書の有効期限が切れています。

Horizon Cloud Service - next-gen での Dynamic Environment Manager の構成

Horizon Agent で使用される Dynamic Environment Manager を構成して、仮想マシンをカスタマイズできます。

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

手順

1 ナビゲーション バーの [設定] をクリックします。

2 [Dynamic Environment Manager] タイルの [管理] をクリックして、[Dynamic Environment Manager] ページに移動します。

3 [Dynamic Environment Manager] で、[追加] をクリックして Dynamic Environment 構成を追加します。

4 [Dynamic Environment Manager の構成の追加] ページで、構成の一意の名前を追加し、構成設定が保存されているファイル共有へのパスを指定します。

5 [保存] をクリックします。

また、Dynamic Environment Manager の構成を [編集] または [削除] することもできます。

ID プロバイダの設定

Horizon Cloud Service - next-gen は外部 ID プロバイダに依存しており、現在 Microsoft Entra ID と Workspace ONE Access をサポートしています。Horizon Cloud Service - next-gen で構成した ID プロバイダは、ユーザーがデスクトップにアクセスするときに必要な認証を実行します。

いずれの場合も、Microsoft Entra ID または Workspace ONE Access の場合は、オンプレミスの Active Directory を外部 ID プロバイダに接続する必要があります。

ID プロバイダがオンプレミスの Active Directory と統合されていない場合は、選択した ID プロバイダに応じて、以降の該当する手順を実行します。

ID プロバイダとしての Microsoft Entra ID の構成

Horizon Cloud Service - next-gen で、Microsoft Entra ID を ID プロバイダとして使用していて、Microsoft Entra ID がまだオンプレミスの Active Directory と統合されていない場合は、次の手順を実行します。

Microsoft Azure の登録タスクと同期タスクを完了します。

前提条件

- Horizon Cloud へのアクセス権があることを確認します。ログインを作成するには、4 章 Horizon Cloud Service - next-gen 管理者のオンボーディングを参照してください。
- オンプレミスの Active Directory サーバがサポートされていることを確認します。

手順

1 既存のテナントがない場合は、新しい Microsoft Azure テナントを作成します。「クイック スタート：Azure Active Directory で新しいテナントを作成する」など、Microsoft のドキュメントを参照してください。

2 グローバル管理者ロールを持つユーザーを Microsoft Azure に作成します。

3 オンプレミスの Active Directory を Microsoft Azure と同期します。

   a オンプレミスの Active Directory サーバで、ユーザーとグループを作成し、ユーザーをグループに割り当てます。

   すべてのユーザーがグループのメンバーであることを確認します。

   b Microsoft Azure をリンクするには、オンプレミスの Active Directory サーバに Microsoft Entra ID Connect をインストールします。インストールの手順については、「Azure AD Connect の前提条件」など、Microsoft のドキュメントを参照してください。

   c Microsoft Entra ID Connect の構成が完了したら、ユーザーとグループが Microsoft Entra ID で作成されていることを確認します。

次のステップ

必要な Active Directory ドメイン アカウントを作成します。Active Directory ドメイン バインドおよびドメイン参加アカウントの作成を参照してください。

Workspace ONE Access を ID プロバイダとして構成する

Horizon Cloud Service - next-gen では、Workspace ONE Access を ID プロバイダとして使用していて、Workspace ONE Access がまだオンプレミスの Active Directory と統合されていない場合は、次の手順を実行します。

前提条件

- Horizon Cloud へのアクセス権があることを確認します。ログインを作成するには、4 章 Horizon Cloud Service - next-gen 管理者のオンボーディングを参照してください。
- オンプレミスの Active Directory サーバがサポートされていることを確認します。
- Workspace ONE Access テナントがあることを確認します。

手順

1 オンプレミスの Active Directory を Workspace ONE Access と統合します。

   Workspace ONE Access ドキュメントの「VMware Workspace ONE Access とのディレクトリ統合」トピックを参照してください。

2 必要な Active Directory ドメイン アカウントを作成します。

   Active Directory ドメイン バインドおよびドメイン参加アカウントの作成を参照してください。

3 Horizon Cloud の ID プロバイダとして Workspace ONE Access を使用するために必要な次の構成タスクを実行します。

- Horizon Cloud と統合するための Workspace ONE Access ユーザー属性の構成 の一部である必要があります。
- Horizon Cloud と統合するための Workspace ONE Access People Search の構成 の一部である必要があります。

Active Directory ドメイン バインドおよびドメイン参加アカウントの作成

ID プロバイダを構成したら、オンプレミスの Active Directory に 2 つのドメイン バインドと 2 つのドメイン参加アカウントを作成します。後で、Horizon Universal Console を使用して、これらのアカウントの詳細を Horizon Cloud に提供します。

Horizon Cloud では、サービス アカウントとして使用する次の Active Directory アカウントの 2 つのインスタンスを指定する必要があります。

- AD ドメイン内の検索を実行するために使用するドメイン バインド アカウント。
- コンピュータ アカウントをドメインに参加させ、コンピュータ アカウントをドメインから削除し、Sysprep 処理を実行するために使用するドメイン参加アカウント

重要： これらのサービス アカウントに指定する Active Directory アカウントについては、次のガイドラインに従ってください。

- プライマリと補助の両方のドメイン バインド アカウントが期限切れになるか、アクセス不能になると、シングル サインオンは機能せず、新しいデスクトップに参加できません。プライマリまたは補助ドメイン バインド アカウントで [有効期限なし] を設定しない場合、両方に異なる有効期限を設定する必要があります。有効期限が近くなったら常に追跡しながら、有効期限の時刻に達する前に Horizon Cloud ドメイン バインド アカウント情報を更新する必要があります。
- プライマリ ドメインと補助ドメインの両方のドメイン参加アカウントが期限切れになるかアクセス不能になると、シングル サインオンが機能せず、新しいデスクトップに参加できなくなります。プライマリまたは補助ドメイン参加アカウントで [有効期限なし] を設定しない場合、両方に異なる有効期限を設定する必要があります。有効期限が近くなったら常に追跡しながら、有効期限の時刻に達する前に Horizon Cloud ドメイン参加アカウント情報を更新する必要があります。

ドメイン バインド アカウント - 必須の Active Directory 権限

ドメイン バインド アカウントには読み取り権限が付与されている必要があります。Horizon Cloud のサービスとしてのデスクトップ操作でエンド ユーザーへのデスクトップ仮想マシンの割り当てなどの操作を行う際など、Active Directory 組織単位 (OU) の Active Directory アカウントをすべて検索できる機能を使用されることが想定されます。ドメイン バインド アカウントには、Active Directory からオブジェクトを列挙する機能が必要です。ドメイン バインド アカウントには、Horizon Cloud での使用が予想されるすべての OU およびオブジェクトに対する次の権限が必要です。

- コンテンツの一覧表示
- すべてのプロパティの読み取り
- アクセス許可の読み取り

- tokenGroupsGlobalAndUniversal の読み取り（[すべてのプロパティの読み取り] 権限により暗黙に含まれる）

重要： 一般的に、ドメイン バインド アカウントには、Microsoft Active Directory デプロイで認証されたユーザーに通常付与される、設定済みのデフォルトの読み取りアクセス関連の権限が付与されている必要があります。標準の Microsoft Active Directory デプロイでは、Authenticated Users に通常付与されるデフォルト設定により、標準ドメイン ユーザー アカウントは、Horizon Cloud がドメイン バインド アカウントに必要な列挙を行うことができます。ただし、組織の Active Directory 管理者が通常ユーザーの読み取りアクセス権に関連する権限をロックダウンすることを選択した場合は、それらの Active Directory 管理者に、Horizon Cloud に使用するドメイン バインド アカウントの認証済みユーザーの標準デフォルト設定を保持するように要求する必要があります。

ドメイン参加アカウント - 必須の Active Directory 権限

ドメイン参加アカウントは、テナント レベルで構成されます。テナントのフリート内のすべてのポッドで、ドメイン参加関連のすべての操作のために、Active Directory 登録で構成されている同じドメイン参加アカウントがシステムによって使用されます。

システムは、ファームと VDI デスクトップ割り当ての [コンピュータの組織単位 (OU)] テキスト ボックスが Active Directory 登録のデフォルトの OU と異なる場合、Active Directory 登録ワークフロー（そのワークフローの [デフォルトの組織単位 (OU)] テキスト ボックス）で指定する OU 内、および作成するファームおよび VDI デスクトップ割り当てで指定する OU 内のドメイン参加アカウントに対する明示的な権限チェックを実行します。

下位の OU を使用するケースにも対応するため、ベスト プラクティスとして、これらの必須のアクセス権限をコンピュータの組織単位のすべての子孫オブジェクトに適用するように設定します。

重要：

- ここに挙げる AD 権限の一部は通常、Active Directory により、デフォルトで アカウントに割り当てられます。ただし、Active Directory のセキュリティ許可を制限している場合、Horizon Cloud で使用すると予想されるすべての OU およびオブジェクトの権限についての記述を、ドメイン バインド アカウントが必ず読むようにする必要があります。
- Microsoft Active Directory では、新しい組織単位 (OU) を作成するときに、システムは、新しく作成された OU およびすべての子孫オブジェクトの [すべての子オブジェクトの削除] 権限に `Deny` を適用する `Prevent Accidental Deletion` 属性を自動的に設定する場合があります。その結果、ドメイン参加アカウントに [コンピュータ オブジェクトの削除] 権限を明示的に割り当てた場合、新しく作成された OU の場合、Active Directory は、明示的に割り当てられた [コンピュータ オブジェクトの削除] 権限に上書きを適用した可能性があります。[誤削除の防止] フラグをオフにしても、Active Directory が [すべての子オブジェクトの削除] 権限に適用した `Deny` が自動的にオフにならない場合があるため、新しく追加された OU の場合、Horizon Universal Console でドメイン参加アカウントを使用する前に、OU およびすべての 子 OU の [すべての子オブジェクトの削除] に対して設定した `Deny` 権限を確認して手動でクリアする必要がある場合があります。

コンピュータ アカウントの再利用

ドメイン参加ユーザー アカウントには既存のコンピュータ アカウントを再利用するための権限を付与する必要があります。それには次の手順を使用します。

- 新しいユニバーサル セキュリティ グループを作成します。
- すべてのドメイン参加ユーザー アカウントを新しいセキュリティ グループに追加します。

- 関連するすべてのグループ ポリシー オブジェクト (GPO) について、[ドメイン コントローラ：ドメイン参加中にコンピュータ アカウントの再利用を許可する] を有効にします。
- [セキュリティの編集...] をクリックします。
- [信頼されたコンピュータ アカウント所有者のセキュリティ設定] ダイアログで、[追加...] をクリックします。
- 新しいセキュリティ グループを選択し、[OK] をクリックします。

各ドメインに対して次の手順を実行します。

Horizon Cloud と統合するための Workspace ONE Access ユーザー属性の構成

Horizon Cloud の ID プロバイダとして Workspace ONE Access を使用している場合は、Workspace ONE Access コンソールを使用して必須のユーザー属性を構成します。

この手順の目的は、Workspace ONE Access を Horizon Cloud の ID プロバイダとして正常に構成するために必須の追加の Workspace ONE Access 属性を追加し、それらの必須属性を Active Directory 属性にマッピングすることです。

userPrincipalName、objectGuid、sid、および netBios の Workspace ONE Access 属性は必須であり、次の手順で説明するように適切な Active Directory 属性にマッピングする必要があります。

前提条件

Workspace ONE Access コンソールでユーザー属性を構成するには、Workspace ONE Access Connector をインストールし、Active Directory とのディレクトリ統合を設定する必要があります。

手順

1 Workspace ONE Access コンソールにログインします。

2 [設定] - [ユーザー属性] をクリックします。

3 次のリストに示すようにカスタム属性を追加し、[保存] をクリックします。

> **注：** このリストに表示されているとおりに、大文字と小文字を区別して属性を正確に入力してください。

   - objectGuid
   - sid
   - netBios

   この統合には userPrincipalName も必須ですが、デフォルト属性のリストにすでに表示されているため、追加する必要はありません。

4 [統合] - [ディレクトリ] をクリックして、Workspace ONE Access 属性を Active Directory 属性にマッピングします。

   a Workspace ONE Access コンソールの [ID とアクセス管理] 領域の [管理] 部分を使用して、ディレクトリが構成されている画面に移動し、Horizon Cloud の資格を持つユーザーとグループを含むディレクトリの名前をクリックします。

   b そのディレクトリの画面で、[同期設定] タブをクリックし、[マップされた属性] ページに移動します。

   c 表示されているとおりに、Workspace ONE Access ユーザー属性を Active Directory 属性にマッピングします。

Workspace ONE Access 属性	Active Directory 属性
userPrincipalName	userPrincipalName
objectGuid	objectGUID
sid	objectSid
netBios	msDS-PrincipalName

5 [保存] をクリックします。

6 Horizon Cloud 環境に同期するすべてのユーザーとグループが選択されていることを確認します。

   Workspace ONE Access コンソールで、ユーザーとグループのリストを表示および編集するには、ディレクトリの [同期設定] 画面から、[ユーザー] タブおよび [グループ] タブに移動します。

7 Workspace ONE Access コンソールで、そのディレクトリのページに戻り、[同期] をクリックして、ユーザーとグループを Workspace ONE Access に同期し、すべての正しいユーザー属性を使用します。

Horizon Cloud と統合するための Workspace ONE Access People Search の構成

Horizon Cloud の ID プロバイダとして Workspace ONE Access を使用している場合は、Workspace ONE Access コンソールの People Search 機能が有効になっていることを確認します。これにより、Horizon Cloud のユーザー検索も有効になります。

Workspace ONE Access が Horizon Cloud の ID プロバイダである場合、ユーザー検索を Horizon Universal Console で使用できるようにするには、Workspace ONE Access People Search 機能を有効にする必要があります。

前提条件

Workspace ONE Access コンソールで People Search を有効にするには、Workspace ONE Access Connector をインストールし、Active Directory とのディレクトリ統合を設定する必要があります。

手順

1 Workspace ONE Access コンソールにログインします。

2 [統合] - [People Search] をクリックします。

3 [ディレクトリの選択] ページで、ディレクトリを選択します。

4 [ユーザー属性の選択] ページで、[businessUnit] 属性を選択し、プロンプトに従ってマッピングします。

5 [Workspace ONE Access の属性名] を [Active Directory の属性名] にマッピングするには、Active Directory の各属性名を選択します。

[managerDN 属性] には、カスタム属性を定義してマッピングすることもできます。

6 [次へ] をクリックします。

7 [ユーザー DN] テキスト ボックスで、デフォルトが適用される場合はそのまま使用します。デフォルトが適用されない場合は、ユーザー DN（**OU=Organization,DC=example,DC=com** など）を入力し、[保存して同期] をクリックします。

App Volumes の使用

App Volumes を使用して、アプリケーションを動的に配信および管理します。これらのアプリケーションは、エンド ユーザーが使用するために提供するものです。

注意: App Volumes ワークフローを実行する場合は、選択したドメインが選択した Horizon Edge からアクセス可能で、選択したパッケージャと同じドメインであることを確認します。選択した Horizon Edge が選択したドメインにアクセスできない場合、または選択したパッケージャが別のドメインに属している場合、予期しない結果が発生し、プロセスが失敗する可能性があります。

Horizon Cloud Service - next-gen で App Volumes アプリケーションを使用するための概要と前提条件

App Volumes アプリケーション機能を使用して、アプリケーションのライフサイクル全体を管理できます。これには、アプリケーションのパッケージ作成、更新、およびリタイアが含まれます。アプリケーションの資格をカスタマイズして、特定のバージョンのアプリケーションをエンド ユーザーに提供することもできます。

重要：

- コンソールに機能が表示され、表示されない場合は、アカウントの担当者に連絡して、ライセンスとテナント アカウントの構成で使用資格が付与されているかどうかを確認する必要があります。
- アプリケーション パッケージのインポートまたは削除、ファイル共有のプロビジョニング、ステージングから配信ファイル共有へのアプリケーション パッケージのレプリケーションなどの操作では、Horizon Edge デプロイを接続する必要があります。ファイル共有の詳細については、このページの「Horizon Edge 関連の前提条件」セクションを参照してください。

ゲスト OS のサポートについては、「製品の相互運用性マトリックス」を参照してください。

Horizon Cloud Service - next-gen の App Volumes 機能の概要

次の表は、Horizon Cloud Service - next-gen の VMware App Volumes 機能の概要を示しています。

機能領域	説明
デプロイ	■ 完全に自動化されたデプロイ。ストレージなどの App Volumes インフラストラクチャ コンポーネントの自動プロビジョニング。 ■ Microsoft Azure ファイル共有を管理する App Volumes モジュールをサポートする Edge インフラストラクチャ。 ■ ポッドの Horizon Edge のデプロイ時に、アプリケーションを保存および配信するための Microsoft Azure ファイル共有の自動プロビジョニング。
管理コンソール	■ App Volumes コンソールは、Horizon Universal Console にシームレスに統合されます。デスクトップとアプリケーションを同じコンソールで管理します。 ■ App Volumes Agent のインストール エクスペリエンスは、Horizon Cloud イメージ作成ワークフローにシームレスに統合されています。
App Volumes 4 Agent	オンプレミスおよび Microsoft Azure デプロイの両方に使用される統合され、パフォーマンス最適化されたエージェント。
パッケージ作成	■ Microsoft Azure ファイル共有を使用して提供される VHD ベースのパッケージをサポートしています。 ■ アプリケーション パッケージの作成は Horizon Cloud 内でネイティブに実行されます。コマンドライン ツールは不要です。 ■ ユーザーは、App Volumes を使用して、MSIX アプリケーション添付の VHD をインポートし、この新しいパッケージ形式を提供できます。
アプリケーション ライフサイクル管理	すでに App Volumes 4 オンプレミスの一部となっている SAM (Simplified Application Management) 機能をサポートします。管理者は、アプリケーションのライフサイクル全体（パッケージ作成、更新、リタイアなど）を管理できるようになりました。
アプリケーション割り当て	■ 管理者は、アプリケーションの資格をカスタマイズして、特定のバージョンのアプリケーションをエンド ユーザーに提供することができます。 ■ マルチ Edge アプリケーションの提供をサポートします。
ハイブリッド クラウドのサービス	オンプレミスの App Volumes ユーザーが、オンプレミスのデプロイから Microsoft Azure 上の Horizon Cloud にアプリケーション パッケージをインポートできるようになりました。オンプレミス パッケージを再利用します。Microsoft Azure 用にパッケージを作成し直す必要はありません。

App Volumes アプリケーション プロセスの概要

ユーザーが App Volumes アプリケーションを使用できるようにするには、次の 2 段階のプロセスがあります。

- Horizon Universal Console での App Volumes アプリケーションの追加。これを行うには、次の 2 つの方法があります。
  - 新しいアプリケーション パッケージを作成してインポートすることにより、App Volumes アプリケーションを追加します。

    アプリケーション パッケージがまだ作成されていない場合は、[パッケージの追加] オプションを使用して作成できます。これにより、App Volumes を使用してアプリケーション パッケージが作成され、自動的にインポートされます。Horizon Cloud Service - next-gen を使用した App Volumes アプリケーションの追加を参照してください。

    また、[アプリケーションの追加] 機能を使用してアプリケーションを作成するときに、アプリケーション パッケージを作成することもできます。
  - 既存のアプリケーション パッケージをインポートすることにより、App Volumes アプリケーションを追加します。

以前に App Volumes で作成されているアプリケーション パッケージがある場合は、[アプリケーションのインポート] オプションを使用してインポートできます。これは、アプリケーション パッケージを作成し直すことなく、オンプレミスのデプロイからアプリケーション パッケージを再利用できることを意味します。Horizon Cloud Service - next-gen を使用して既存のアプリケーション パッケージをインポートし App Volumes アプリケーションを追加するを参照してください。

- App Volumes アプリケーションの使用資格をユーザーに付与するための App Volumes 資格を作成します。Horizon Cloud Service - next-gen を使用した App Volumes アプリケーションの資格の作成を参照してください。

Horizon Cloud on Microsoft Azure 環境で App Volumes を使用するための要件と前提条件

重要： App Volumes アプリケーションにアクセスできなくなり、Horizon Cloud on Microsoft Azure 環境の App Volumes 機能のサポートが無効になるのを防ぐには、App Volumes 関連のストレージ アカウントのストレージ アカウント キーを、そのキーの有効期限切れ、変更、ローテーションを引き起こすような方法で操作しないようにする必要があります。

ストレージ アカウント キーが手動または Azure ポリシーを介してローテーションされると、App Volumes が依存するストレージ アカウントとファイル共有にアクセスできなくなります。この問題が発生した場合、環境内に保存されているストレージ キーが無効なため、App Volumes はエンド ユーザーにアプリケーションを配信できません。

Horizon Cloud on Microsoft Azure デプロイは指定された Azure サブスクリプションに存在しますが、デプロイの App Volumes 関連ストレージ アカウントは、Horizon Edge モジュール、Unified Access Gateway マシン、および Azure サブスクリプションにプロビジョニングされるその他のサービスによってデプロイされるリソースと同様に VMware によって管理されるコンポーネントです。すべての Horizon Cloud on Microsoft Azure デプロイには、App Volumes 関連のストレージ アカウントのデプロイが含まれます。

サービスが Horizon Edge をデプロイすると、サービスはこの App Volumes 関連のストレージ アカウントを Azure サブスクリプションにプロビジョニングします。このストレージ アカウントの目的は、App Volumes アプリケーション ファイルがプロビジョニングされるファイル共有を提供することです。

このストレージ アカウントのデータは、Microsoft 管理のキーを使用して Azure Storage によって自動的に暗号化されます。ユーザーまたは組織がこのストレージ アカウント キーの期限切れ、変更、ローテーションを行うと、ストレージ キーが無効になります。この問題が発生すると、App Volumes はファイル共有にアクセスできず、エンド ユーザーにアプリケーションを配布できなくなります。

App Volumes アプリケーションをインベントリに追加する前に、環境が次の前提条件を満たしていることを確認します。

Horizon Edge 関連の前提条件

- 環境にはゲートウェイ構成（Unified Access Gateway インスタンス）が必要です。また、Unified Access Gateway インスタンスで構成された Horizon Cloud on Microsoft Azure 環境の場合と同様に、Unified Access Gateway の FQDN マッピング手順を完了している必要があります。
- Azure サブスクリプションに、`[Preview] Storage Account public access should be disallowed` 定義が有効になっているポリシーが割り当てられていないことを確認します。

このような定義を持つポリシーが有効になっている場合、App Volumes サービスはデプロイ時にストレージ アカウントのファイル共有をプロビジョニングできません。

- これらのファイル共有はサービスによって生成され、App Volumes に必要です。

  ファイル共有を表示するには、Horizon Universal Console で [キャパシティ] ページに移動し、Horizon Edge をクリックして [App Volumes アプリケーション ストレージ] セクションまでスクロールします。

  ステージング ファイル共有

ステージング ファイル共有は、検出用の新しいアプリケーション パッケージをステージングし、アプリケーション インベントリにインポートするために使用される Azure ファイル共有です。アプリケーション パッケージは、既存の App Volumes 4.x デプロイからコピーできます。ファイル共有は、アプリケーションのパッケージングにも使用されます。

Horizon Edge がデプロイされると、1 つのファイル共有が自動的にプロビジョニングされます。

配信ファイル共有

配信ファイル共有は、ユーザーまたはグループに使用資格が付与されている既存のアプリケーション パッケージを配信するために使用される Azure ファイル共有です。デスクトップ プール仮想マシンは、このファイル共有からアプリケーション パッケージ ディスクをマウントします。

すべてのプロバイダに対して最初のプールが作成されると、6 つの配信ファイル共有が自動的にプロビジョニングされます。たとえば、1 つのプライマリ プロバイダと 4 つのセカンダリ プロバイダを持つ Horizon Edge の場合、App Volumes はすべてのセカンダリ プロバイダに対して 1 つのステージング ファイル共有と 6 つの配信ファイル共有をプロビジョニングします。その結果、合計 24 個のファイル共有がプロビジョニングされます。

注：

- プライマリ プロバイダを使用してプールを作成する場合、App Volumes は 1 つのステージング ファイル共有と 6 つの配信ファイル共有をプロビジョニングします。
- Horizon Edge 内で、Horizon Cloud サービスはステージング ファイル共有から配信ファイル共有にアプリケーション パッケージを自動的にレプリケートします。

構成要件

- Active Directory ドメインをマシン ID として構成する場合は、「Horizon Cloud Service - next-gen 環境での ID とアクセス管理」の説明に従って、Active Directory ドメインの登録ワークフローを完了していることを確認します。

  または、マシン ID として Azure Active Directory を選択することもできます。

- Horizon Cloud の Microsoft Azure での Horizon Cloud 環境のポートとプロトコルの要件を満たすだけでなく、TCP プロトコル トラフィック用のポート 445 も開く必要があります。ポート 445 は、Microsoft Windows の SMB ファイル共有にアクセスするための標準の SMB ポートです。アプリケーション パッケージは、Horizon Edge のプライマリ プロバイダ インスタンスによって識別されるリソース グループにある Microsoft Azure のファイル共有に格納されます。

イメージの要件

コンソールで [パッケージの追加] または [アプリケーションの追加] ワークフローを使用して、アプリケーション パッケージを作成して App Volumes アプリケーションを追加するには、コンソールのインベントリに次の条件を満たす公開イメージが必要です。

- クライアント タイプの Microsoft Windows 10 または Windows 11 オペレーティング システムを実行している。このクライアント タイプは、VDI タイプのオペレーティング システムと呼ばれる場合があります。クラウド内キャプチャ ワークフローは、VDI タイプのオペレーティング システムでのみ使用できます。クラウド内キャプチャ ワークフローは、マルチセッションまたは RDS タイプのオペレーティング システムでは使用できません。
- App Volumes Agent がインストールされている。
- オンデマンド パッケージ配信モードを使用するには、Horizon Agent インストーラ ビルド `23.1.0.21387799` 以降がインストールされていることを確認します。

特定のプールのイメージのエージェント バージョンを見つけるには、次の手順を実行します。

1 [リソース] - [プール] の順に進みます。

2 プール名をクリックします。

3 プールの詳細ページで、[全般設定] セクションに移動します。

4 [イメージ] ペインで、`Name` をメモします。

`Name` は、その特定のプールに使用されるイメージ名です。

5 イメージのリストを表示するには、[リソース] - [イメージ] に移動します。

6 イメージ バージョンとステータスを一覧表示する [バージョン] テーブルを表示するには、イメージ名のリンクをクリックします。

7 目的のイメージ バージョンのリンクをクリックします。

8 イメージ バージョンの詳細ページで、[イメージ コピー] テーブルに移動します。

9 `Agent Version` を表示します。

`Agent Version` は、イメージ バージョンにインストールされている Horizon Agent インストーラ ビルドを示します。

パッケージング要件

- App Volumes によってプロビジョニングされたストレージ アカウントにアクセスするためのファイアウォール ルールを構成している場合は、アプリケーションのパッケージ化に使用する Horizon Edge デプロイのプロバイダに関連付けられているすべてのサブネットを許可リストに登録してください。
- 自動更新の動作に問題があるため、パッケージ化する各アプリケーションの自動更新サービスを無効にする必要があります。
  - アプリケーションに自動更新サービスがある場合は、アプリケーションのプロビジョニング プロセス中に、Windows Services Manager などのサービスを無効にします。
  - アプリケーション プロビジョニング プロセス中に自動更新サービスを無効にできない場合や無効にしない場合は、未割り当てのアプリケーションの不完全なバージョンをユーザーが受け取るなどの問題が

発生した後で、レジストリを構成して基本イメージを変更します。このように構成することで、アプリケーション パッケージがユーザー仮想マシンにデプロイされるときに、目的のサービスが確実に開始されなくなります。具体的には、アプリケーション サービス名を svservice レジストリ構成 [DisableAppServicesList] に追加してレジストリを構成します。

Microsoft Azure の Horizon Edge デプロイ内の App Volumes アプリケーションで Microsoft Windows 10 または 11 Enterprise マルチセッション イメージを使用するためのベスト プラクティス

次のベスト プラクティスにより、ユーザーと管理者の使用環境の向上につながります。Horizon Cloud Service - next-gen の App Volumes アプリケーションで Microsoft Windows 10 または 11 Enterprise マルチセッション イメージを設定するも参照してください。

- 基本イメージに、プリンタ ドライバを使用してハードウェア プリンタをインストールします。
- Microsoft のドキュメント FAQ で説明されているように、Microsoft Windows 10 または 11 Enterprise マルチセッションは、以前は Microsoft Windows Server オペレーティング システムでのみ提供された複数の同時対話型セッションを許可する Remote Desktop Session Host (RDSH) タイプの仮想マシンです。Microsoft Windows 10 または 11 Enterprise マルチセッションは RDSH タイプのオペレーティング システムであるため、VDI 関連のワークフローではなく、Horizon Cloud RDSH に該当するワークフローが適用されます。したがって、これらのマルチセッション システムに基づいてエンド ユーザーにセッション デスクトップを提供するには、マルチセッション プール グループの作成の説明に従ってマルチセッション プール グループを作成します。
- アプリケーションをインストールしたり、同じ仮想マシン上のすべてのユーザー セッション間で共有しないファイルを作成したりするときに、ファイルをユーザー自身のプロファイルの場所に配置できることをユーザーに通知します。

Horizon Cloud Service - next-gen の App Volumes アプリケーションで Microsoft Windows 10 または 11 Enterprise マルチセッション イメージを設定する

Microsoft Azure の Horizon Cloud で App Volumes を使用して Microsoft Windows 10 または 11 Enterprise マルチセッション イメージを使用する場合は、セットアップ プロセス中に特定のアクションを実行する必要があります。まず、基盤となる Microsoft Windows Enterprise マルチセッション オペレーティング システムを作成し、App Volumes 割り当てを作成してユーザーにアプリケーションを提供します。次の手順の概要は、このプロセスを示しています。

その後に続く手順の背景情報については、Horizon Cloud Service - next-gen で App Volumes アプリケーションを使用するための概要と前提条件を参照してください。

次のリストの手順を実行する場合は、Microsoft Azure の Horizon Edge デプロイの App Volumes 機能で使用する Microsoft Windows 10 または 11 Enterprise マルチセッション イメージの構成に固有の手順を確認してください。

重要：

- マルチセッションのマシンでは、アプリケーション パッケージの分離は、そのパッケージを割り当てたユーザーが最後にログアウトした後に実行されます。ボリュームを接続解除するために、対応する仮想マシンをシャットダウンする必要はありません。
- システムのクラウド内キャプチャ ワークフローは、マルチセッションまたは RDS タイプのオペレーティング システムでは使用できません。このクラウド内キャプチャ ワークフローは、Horizon Universal Console を使用して実行されます。

  したがって、クラウド内キャプチャ ワークフローを使用して App Volumes アプリケーションを組織のインベントリに追加するには、クライアント タイプの Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムに基づくイメージを使用する必要があります。これは VDI タイプのオペレーティング システムと呼ばれることもあり、これをクラウド内キャプチャ ワークフローに使用します。次に、これらのアプリケーションがインベントリにある場合、Microsoft Windows 10 または 11 Enterprise マルチセッション イメージを使用してマルチセッション プールによってプロビジョニングされたセッションベースのデスクトップで使用できます。セッションベースのデスクトップを基盤となるデスクトップのエンド ユーザーに割り当てたら、それらのキャプチャした App Volumes アプリケーションを同じエンド ユーザーに割り当て、そのセッションベースのデスクトップ内で使用できるようにします。

ゲスト OS のサポートについては、「製品の相互運用性マトリックス」を参照してください。

1. App Volumes アプリケーションを Horizon Cloud インベントリに追加する

セッションベースのデスクトップの資格を付与したエンド ユーザーに App Volumes アプリケーションを割り当てる前に、テナントのインベントリにその App Volumes アプリケーションが含まれている必要があります。コンソールの [アプリケーションの追加] または [パッケージの追加] ワークフローまたは [アプリケーションのインポート] ワークフローを使用して、App Volumes アプリケーションを組織のインベントリに追加できます。

ただし、作成ワークフローは、マルチセッション タイプのオペレーティング システムでは使用できません。作成ワークフローを使用してアプリケーションをインベントリに追加する場合は、そのワークフローで使用し、その VDI タイプのオペレーティング システムからアプリケーションをキャプチャするために、クライアント タイプ（VDI タイプとも呼ばれる）の Microsoft Windows 10 または 11 オペレーティング システムが必要です。

- コンソールの [アプリケーションの追加] または [パッケージの追加] ワークフローを使用して、VDI タイプの Microsoft Windows 10 または 11 オペレーティング システムからインベントリにアプリケーションを追加します。手順については、Horizon Cloud Service - next-gen を使用した App Volumes アプリケーションの追加を参照してください。
- コンソールのインポート ワークフローを使用して、Horizon Cloud テナントの外部で手動でキャプチャし、Microsoft Azure ポータルを使用して Horizon Edge のステージング ファイル共有に手動でアップロードした App Volumes アプリケーションをインベントリに追加します。このワークフローは、主に一部のオンプレ

ミスの App Volumes インストールからの App Volumes パッケージがすでにあり、それらのパッケージを Horizon Cloud インベントリで再利用する場合に使用されます。Horizon Cloud Service - next-gen を使用して既存のアプリケーション パッケージをインポートし App Volumes アプリケーションを追加するを参照してください。

2. App Volumes アプリケーションの資格を新しいユーザーに付与する

作成したばかりの 1 つ以上の App Volumes アプリケーションを含む、新しいユーザーの App Volumes 資格を作成します。Horizon Cloud Service - next-gen を使用した App Volumes アプリケーションの資格の作成を参照してください。

重要： 管理者権限を必要とするサービスが Microsoft Windows 10 または 11 Enterprise マルチセッション アプリケーション パッケージにキャプチャされている場合、そのアプリケーション パッケージに割り当てられているすべてのユーザーにも管理者権限が必要です。

3. Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムの基盤となるデスクトップを作成し、ユーザーに資格を割り当てる

このプロセスの最初の部分には、次の手順が含まれています。

1 Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムのデスクトップ イメージを作成します。

注： イメージのベース仮想マシンを作成するときに、App Volumes Agent をインストールします。

Microsoft Azure Marketplace からのイメージの追加の詳細については、Microsoft Azure Marketplace からのイメージの追加を参照してください。

新しい Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システム デスクトップ イメージを使用してマルチセッション プール グループを作成します。マルチセッション プール グループの作成を参照してください。

2 新しいマルチセッション セッション プール グループの使用資格をエンド ユーザーに付与します。

Web クライアントの Horizon HTML Access を使用したデスクトップの起動を参照してください。

Horizon Cloud Service - next-gen を使用した App Volumes アプリケーションの追加

Horizon Universal Console のアプリケーションの追加ワークフローを使用して、アプリケーションを組織のインベントリに追加できます。アプリケーションの作成時にすぐにパッケージを追加するか、[パッケージの追加] ワークフローを使用して、後で既存のアプリケーションにパッケージを追加することができます。

注： 既存のアプリケーションにパッケージを追加する場合は、アプリケーションを再度作成する必要はありません。

- [アプリケーションの追加] ワークフローを初めて使用した後、キャプチャ デスクトップ仮想マシンでアプリケーション パッケージをキャプチャする手順を完了するまでは、同じユーザーが同じイメージに対してそのオプションを 2 回目に使用しようとしてはいけません。アプリケーション パッケージのキャプチャ手順を完了する前に、同じイメージに対してこのオプションを再度使用しようとすると、パッケージを作成する要求がすでに開始されていることを示すメッセージが表示されます。ただし、同じテナント内の別のユーザーは、最初のユーザーが完了したかどうかにかかわらず、そのイメージに対してパッケージの作成を開始できます。

  注： 同じ Horizon Edge または別の Horizon Edge で異なるイメージを選択すると、同じユーザーが複数のキャプチャを同時に実行できます。同じイメージで複数のキャプチャを同時に実行することはできません。

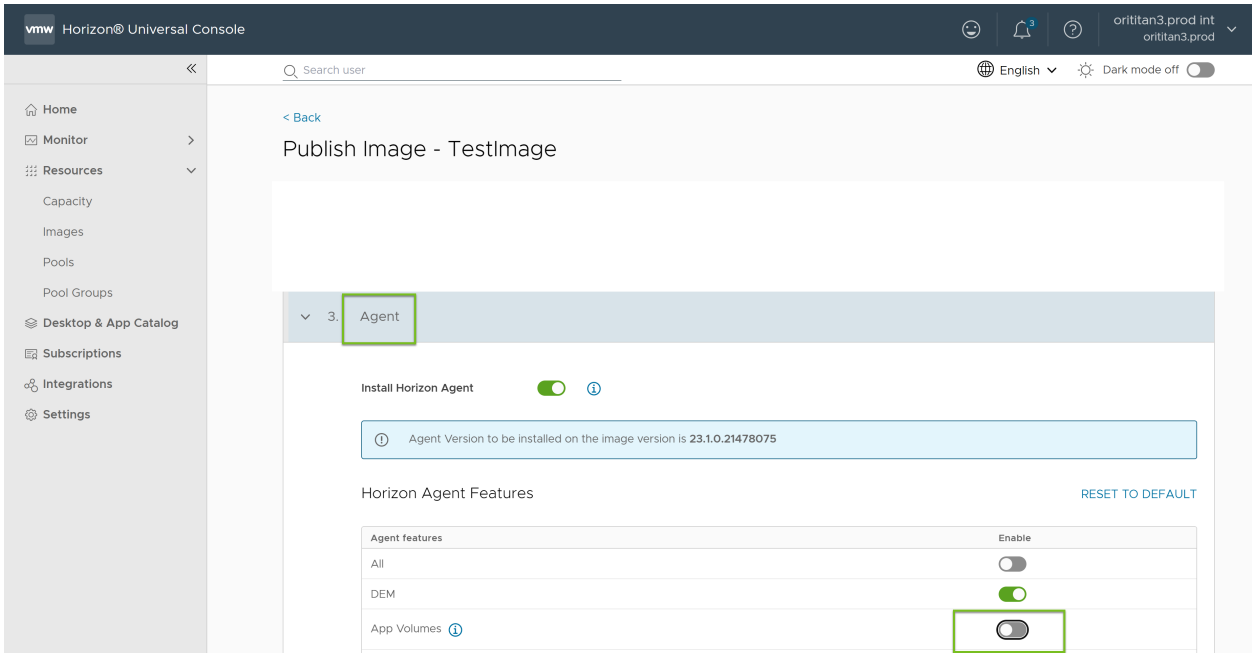
- 初めて [アプリケーションの追加] オプションをクリックしてキャプチャ プロセスを開始する場合、システムではキャプチャ デスクトップ仮想マシンの準備が完了してから `Desktop ready for application capture` ステータスに変更されるまで、最大で 10 分かかることがあります。この初めてのときの 20 分という時間は、システムがキャプチャ処理をサポートするためにデスクトップ割り当てと 2 台のデスクトップ仮想マシンを作成しているためです。最初のアプリケーション パッケージのキャプチャを完了してから新しいキャプチャ プロセスを開始すると、[アプリケーションの追加] オプションをクリックして、ステータスが `Desktop ready for application capture` に変更されるまでの時間が 10 分ほど短くなります。初回のようにキャプチャ デスクトップ割り当てを作成する必要がないので、初回以降の時間は短くなります。2 回目は、以前に使用されたキャプチャ デスクトップ仮想マシンが削除され、新しい仮想マシンが使用されます。

パッケージごとに 1 つの配信オプションがあります。このオプションを使用して、パッケージ配信モードを `Classic` または `On-demand` として構成できます。従来の配信では、割り当てられたアプリケーションは、コンピュータの起動時またはユーザー ログイン時にすぐにエンド ユーザーに配信されます。オンデマンド配信ではショートカットが表示されますが、ユーザーがショートカットを開くまでアプリケーションは配信されません。詳細については、Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージのパッケージ配信モードについてを参照してください。

前提条件

環境が Horizon Cloud Service - next-gen で App Volumes アプリケーションを使用するための概要と前提条件 に記載されているすべての前提条件を満たしていることを確認します。

重要： この追加ワークフローは、単一ユーザー、クライアント、または VDI タイプの Microsoft Windows オペレーティング システムのイメージでのみ使用でき、マルチセッション タイプのオペレーティング システムでは使用できません。以下のタスクの手順を開始する前に、App Volumes Agent がインストールされた使用可能なイメージが必要です。Microsoft Azure Marketplace からイメージを追加してイメージを公開する場合は、App Volumes トグル ボタンをオンにしていることを確認します。デフォルトでは、このトグルはオフになっています。このトグル ボタンは、イメージを公開するときに [エージェント] セクションにリストされます。



イメージを追加して公開するには、次世代 Horizon 制御プレーン を使用した Horizon イメージの管理を参照してください。

手順

1 Horizon Universal Console で、[デスクトップおよびアプリケーション カタログ] - [App Volumes] の順に移動します。

2 [追加] - [アプリケーション] の順にクリックします。

3 [アプリケーションを追加] ページで、[アプリケーション名] と [説明] を追加します。

4 Active Directory の使用可能なドメインから所有者を選択して [所有者の詳細] を追加します。

5 [パッケージの追加] トグルを選択します。

すぐにパッケージを追加することも、後で追加することもできます。パッケージを後で追加するには、[パッケージの追加] ワークフローを使用します。

6 [パッケージ名] および [説明] を追加します。

7 アプリケーションがパッケージ化される [Horizon Edge] を選択します。

8 パッケージをキャプチャするためにパッケージ仮想マシンが作成される [プロバイダ] を選択します。

9 [マシン ID] を選択します。

環境に登録されている `Azure Active Directory` または、構成済みの Active Directory ドメインのいずれかを選択できます。構成済みの Active Directory ドメインを選択する場合は、選択した Horizon Edge からドメインにアクセスできることを確認します。

注： `Azure Active Directory` の場合、Windows 11 および Windows 10 デバイスはすべてサポートされます。ただし、Microsoft Azure で実行されている Windows Server 2019 Home エディション以降の仮想マシンを除きます（サーバ コアはサポートされていません）。

10 アプリケーションをキャプチャするために仮想マシンが割り当てられている [パッケージャ] またはユーザーを選択します。

ユーザーのドメインは、選択した Active Directory ドメインと同じである必要があります。

11 [クラシック] と [オンデマンド] のいずれかの配信方法を選択します。

デフォルトでは、パッケージ配信は `Classic` です。パッケージを `On-demand` として構成すると、エンド ユーザーがアプリケーションを起動したときにのみパッケージの添付が行われます。

注： オンデマンド サポートのないバージョンの Horizon Agent インストーラ `23.1.0.21387799` 以前を使用して作成されたパッケージの場合、管理者は `On-demand` から `Classic` および `Classic` から `On-demand` に変更できます。ただし、App Volumes エージェントは、オンデマンドの動作のように既存のパッケージを仮想化することはできません。

12 パッケージのキャプチャに仮想マシンが使用する [イメージ] を選択します。

イメージに App Volumes Agent がインストールされていることを確認します。

13 パッケージのキャプチャに仮想マシンが使用する [イメージ バージョン] を選択します。

14 パッケージ用の仮想マシンの作成に使用される [デスクトップ モデル] を選択します。

15 [保存] をクリックします。

結果

- パッケージが追加されるとすぐに、パッケージのステータスは `Desktop provisioning is in progress` です。
- デスクトップ プロビジョニングが完了し、パッケージャに仮想マシンが割り当てられると、パッケージのステータスは `Ready for capture` になります。

次のステップ

アプリケーションを作成したら、次のいずれかのタスクを実行できます。

- このアプリケーションに別のパッケージを追加する場合、または後でパッケージを作成する場合は、「Horizon Cloud Service - next-gen を使用した既存の App Volumes アプリケーションへの新しいアプリケーション パッケージの追加」に記載されている手順を実行します。

- パッケージをすでに作成していて、アプリケーション パッケージをキャプチャする場合は、「Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージのキャプチャ」に記載されている手順を実行します。

Horizon Cloud Service - next-gen を使用した Horizon Edge デプロイ間での App Volumes アプリケーション パッケージの手動複製

複数の Horizon Edge デプロイがある場合、キャプチャまたはインポートされたアプリケーション パッケージを Horizon Edge 間で複製するには、送信元の Horizon Edge のファイル共有から宛先の Horizon Edge のファイル共有にパッケージを手動でコピーする必要があります。

前提条件

Horizon Cloud Service - next-gen で、複製するキャプチャまたはインポートされたアプリケーション パッケージを特定します。

手順

1 複製しようとするアプリケーション パッケージのファイル名を取得します。

a Horizon Universal Console で、[デスクトップおよびアプリケーション カタログ] - [App Volumes] の順に移動します。

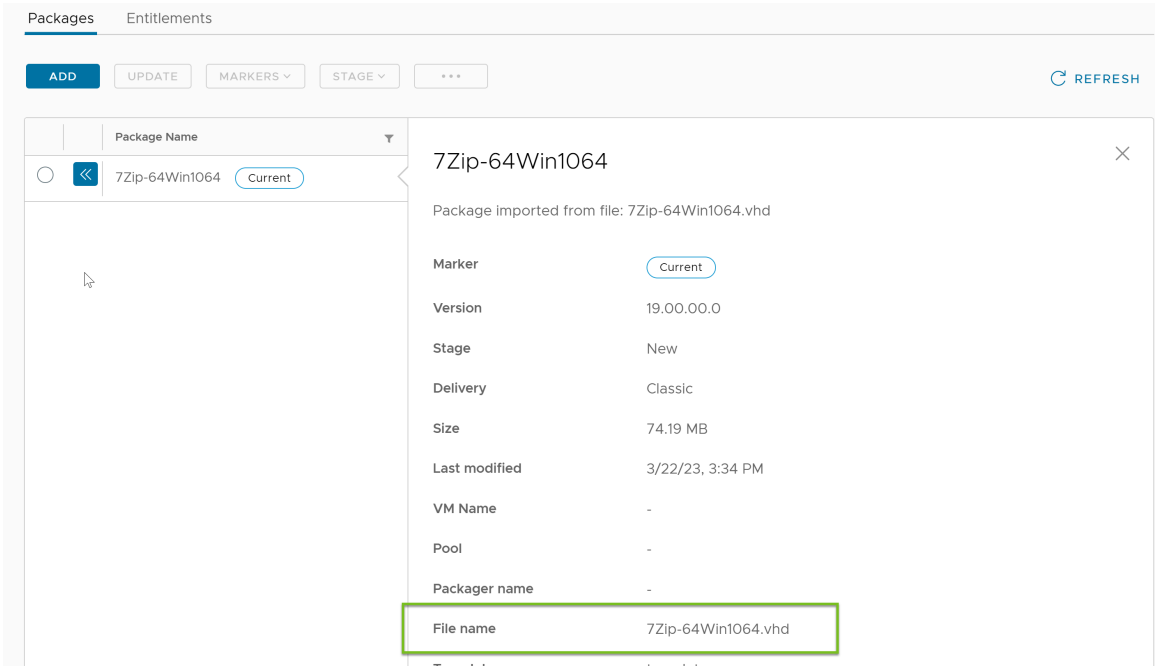
アプリケーションのリストが表示されます。

b 複製するパッケージがあるアプリケーションをクリックします。

c 目的のパッケージの左二重矢印アイコン  をクリックします。

パッケージの詳細画面が表示されます。

d ファイル名 (*filename*.vhd) を書き留めます。



2 Microsoft Azure ポータルに移動します。

3 前述のいずれかの手順で書き留めたアプリケーション ファイル名の `.vhd` および `.json` ファイルを含むステージング ファイル共有を見つけます。

4 `appvolumes/packages` からファイルをコピーします。

5 コピーしたファイルを宛先の Horizon Edge のステージング ファイル共有 (`appvolumes/packages`) にアップロードします。

App Volumes アプリケーション ストレージ アカウントの Azure プライベート エンドポイント

Azure プライベート エンドポイント ソリューションを使用して、ストレージ アカウントとファイル共有に安全にアクセスできます。Horizon Universal Console を使用して、新しい Horizon Edge をデプロイするとき、または既存の Horizon Edge のストレージ アカウントにプライベート エンドポイントを構成できます。

プライベート エンドポイントを構成し、サブネット（Edge Gateway 管理サブネットまたはカスタム サブネット）を選択する場合は、Azure ポータルで次の前提条件が設定されていることを確認します。

- 次の必須の権限は、サブスクリプション レベルで構成する必要があります。

  注： サービス プリンシパルを作成する場合、カスタム ロールにはここにリストされている権限が必要です。

  ```
  "Microsoft.Resources/deployments/*",
  "Microsoft.Resources/subscriptions/resourceGroups/read",
  "Microsoft.Network/virtualNetworks/read",
  "Microsoft.Network/virtualNetworks/subnets/read",
  "Microsoft.Network/virtualNetworks/subnets/write",
  "Microsoft.Network/virtualNetworks/subnets/join/action",
  "Microsoft.Network/privateEndpoints/read",
  "Microsoft.Network/privateEndpoints/write",
  "Microsoft.Network/privateEndpoints/delete",
  "Microsoft.Network/locations/availablePrivateEndpointTypes/read"
  ```

  これらの権限に関する詳細は、マイクロソフト社のドキュメントを参照してください。

- 次のコンポーネント間でネットワーク ピアリングを確立する必要があります。
  - プライベート エンドポイントが構成されているカスタム VNet と Edge Gateway 管理の VNet
  - プライベート エンドポイントが構成されているカスタム VNet と、(既存または新規の) 各デスクトップ プールの VNet。

  ネットワーク ピアリングを使用すると、Edge Gateway 管理とデスクトップ プールは、プライベート エンドポイントを介してストレージ アカウントおよびファイル共有と安全に通信できます。

プライベート エンドポイントのステータス

プライベート エンドポイントのステータスは次のとおりです。

接続済み

新規または既存の Horizon Edge デプロイ用にプライベート エンドポイントを構成すると、プライベート エンドポイントのステータスは `Connected` になります。

構成されていません

既存のストレージ アカウントにプライベート エンドポイントが構成されていない場合、または構成されたプライベート エンドポイントが削除された場合、プライベート エンドポイントのステータスは `Not Configured` になります。

このようなストレージ アカウントの場合、プライベート エンドポイントは [プライベート エンドポイントの構成] オプションを使用して構成できます。このオプションは、各 Horizon Edge の [App Volumes アプリケーション ストレージ] セクションにある [Azure ストレージ アカウント] 表で使用できます。

新しい Horizon Edge をデプロイするときにプライベート エンドポイントを構成するには、「Microsoft Azure Edge のデプロイ」を参照してください。既存の Horizon Edge のプライベート エンドポイントを構成するには、「Horizon Edge の詳細」を参照してください。

Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージのパッケージ配信モードについて

ユーザーによるビジネスクリティカルなアプリケーションの使用頻度が高くない場合があります。そのようなアプリケーションを、必要な場合にのみユーザーに配信できるようになりました。このセルフサービスに似た機能により、パッケージの作成時に各アプリケーション パッケージの配信モードを設定したり、パッケージの編集時にこのモードを変更したりすることができます。

パッケージ配信モードには、`Classic` と `On-demand` の 2 種類があります。デフォルトでは、パッケージ配信モードは `Classic` に設定されています。

デフォルト（従来）の動作では、割り当てられたアプリケーションは、コンピュータの起動時またはユーザー ログイン時に、アプリケーションがエンド ユーザーによってすぐに要求されない場合でも、エンド ユーザーに配信されます。ユーザーがアプリケーションを必要としている場合にのみアプリケーションを配信するために、オンデマンド配信モードを使用できます。

管理者がパッケージの配信モードに `On-demand` を選択すると、[起動] メニューまたはデスクトップでアプリケーションのショートカットのみがエンド ユーザーに表示されます。エンド ユーザーがショートカットを開くと、アプリケーション ボリュームがエンド ユーザーに配信され、仮想化されて起動されます。仮想化時に、アプリケーションの App Volumes オンデマンド ショートカットがアプリケーションのショートカットに置き換えられます。アプリケーションの起動に数秒程度の時間がかかる場合は、アプリケーションの提供が進行中であることを示すメッセージ ボックスがエンド ユーザーに表示されます。

オンデマンド アプリケーション パッケージの配信基準

アプリケーション パッケージをオンデマンドでエンド ユーザーに配信するには、次のような適格性基準があります。

- Horizon Agent インストーラ ビルド `23.1.0.21387799` 以降がインストールされていることを確認します。

  以前のバージョンの Horizon Agent インストーラを使用してインストールされたエージェント コンピュータにエンド ユーザーがログインし、エンド ユーザーに `on-demand` でアプリケーションを使用する資格が付与されている場合、エンドユーザーにパッケージは配信されません。

- パッケージ化プロセス中にインストールされるアプリケーション プログラムにはショートカットが必要です。

オンデマンドで配信されるアプリケーション パッケージの特性

オンデマンドで配信されるアプリケーション パッケージの特性には、次のようなものがあります。

- ユーザーに割り当てられたアプリケーションのショートカットは、そのユーザーにのみ表示されます。
- オンデマンドで配信されるアプリケーションのパッケージ添付ファイルは、エンド ユーザーがアプリケーションのシミュレーションされたショートカットを起動した後にのみ発生します。
- ファイル タイプの関連付け

  既存のパッケージの場合、管理者はパッケージを更新して、パッケージ内のファイル タイプの関連付けデータをキャプチャする必要があります。

  - コンテキスト メニュー項目を表示する一部のアプリケーション（7-Zip など）の場合、App Volumes エージェントではアプリケーションを配信するためのエントリ ポイントのみを表示します。コンテキスト メニューでエンド ユーザーに表示されるエントリ ポイントは、パッケージ化中に [VMware App Volumes - パッケージのファイナライズ] ウィンドウで構成された名前です。アプリケーションがエンド ユーザーに配信されると、このエントリ ポイントはアプリケーション固有のメニュー項目に置き換えられます。
  - 本質的に動的である OLE と COM、プレビュー ハンドラー、TypeLib は、ユーザーがアプリケーションのオンデマンド ショートカットを起動するまでは使用できません。
  - エンド ユーザーは、アプリケーション パスを使用して、オンデマンドでアプリケーションを提供できます。

    例：エンド ユーザーは winword.exe を使用して Microsoft Word アプリケーションを開くことができます。この場合、winword.exe がアプリケーション パスです。アプリケーション パスの使い方の詳細については、マイクロソフト社のドキュメントを参照してください。
  - 管理者が、カスケードされたサブメニューと、ショートカット、ファイル タイプの関連付け、アプリケーション パスなどのその他の機能を備えたアプリケーションをオンデマンドとして構成した場合、エンド ユーザーは、アプリケーション パッケージが配信された場合にのみカスケードされたサブメニューを表示できます。
  - パッケージ化中、App Volumes は、パッケージ マシンで使用されるオペレーティング システムの言語で静的テキストを保存します。パッケージが多言語をサポートしており、エンド ユーザーのエージェント コンピュータで使用されている OS 言語がパッケージ化コンピュータで使用されている言語と異なる場合、エンド ユーザーには、アプリケーション名、ツール チップ、ファイルの説明、およびその他のテキスト要素がパッケージ化マシンで使用されている OS 言語で表示される可能性があります。

パッケージの作成方法の詳細については、Horizon Cloud Service - next-gen を使用した App Volumes アプリケーションの追加を参照してください。

Horizon Cloud Service - next-gen を使用した既存の App Volumes アプリケーションへの新しいアプリケーション パッケージの追加

アプリケーション パッケージを作成し、このパッケージを既存の App Volumes アプリケーションに追加できます。

注： 既存のアプリケーションにパッケージを追加する場合は、アプリケーションを再度作成する必要はありません。代わりに、App Volumes タブに表示されるアプリケーションのリストから既存のアプリケーションを選択し、このタスクに記載されている手順に従ってパッケージの作成を続行します。

[パッケージの追加] ワークフローを初めて使用した後、キャプチャ デスクトップ仮想マシンでアプリケーション パッケージをキャプチャする手順を完了するまでは、同じユーザーが同じイメージに対してそのオプションの 2 回目の使用を試みることはできません。アプリケーション パッケージのキャプチャ手順を完了する前に、同じイメージに対してこのオプションを再度使用しようとすると、パッケージを作成する要求がすでに開始されていることを示すメッセージが表示されます。ただし、同じテナント内の別のユーザーは、最初のユーザーが完了したかどうかにかかわらず、そのイメージに対してパッケージの作成を開始できます。

注： 管理者は、同じイメージまたは異なるイメージで複数のキャプチャを同時に実行できます。イメージは、同一または別の Horizon Edge 上に配置できます。

初めて [パッケージの追加] オプションをクリックしてキャプチャ プロセスを開始する場合、システムではキャプチャ デスクトップ仮想マシンの準備が完了してから [アプリケーション キャプチャのためのデスクトップ準備完了] ステータスに変更されるまで、最大で 10 分かかることがあります。この初めてのときの 20 分という時間は、システムがキャプチャ処理をサポートするためにデスクトップ割り当てと 2 台のデスクトップ仮想マシンを作成しているためです。最初のアプリケーション パッケージのキャプチャを完了してから新しいキャプチャ プロセスを開始すると、[パッケージの追加] オプションをクリックしてから、ステータスが [アプリケーション キャプチャのためのデスクトップ準備完了] に変更されるまでの時間が 10 分ほど短くなります。初回のようにキャプチャ デスクトップ割り当てを作成する必要がないので、初回以降の時間は短くなります。2 回目は、以前に使用されたキャプチャ デスクトップ仮想マシンが削除され、新しい仮想マシンが使用されます。

パッケージごとに 1 つの配信オプションがあります。このオプションを使用して、パッケージ配信モードを `Classic` または `On-demand` として構成できます。従来の配信では、割り当てられたアプリケーションは、ユーザー ログイン時にすぐにエンド ユーザーに配信されます。オンデマンド配信ではショートカットが表示されますが、ユーザーがショートカットを開くまでアプリケーションは配信されません。詳細については、Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージのパッケージ配信モードについてを参照してください。

手順

1. Horizon Universal Console で、[デスクトップおよびアプリケーション カタログ] - [App Volumes] の順に移動します。
2. [追加] - [パッケージ] の順にクリックします。
3. このパッケージを追加する必要がある既存のアプリケーションを選択します。
4. [パッケージ名] と [説明] を入力します。
5. アプリケーションがパッケージ化される [Horizon Edge] を選択します。
6. パッケージをキャプチャするためにパッケージ仮想マシンが作成される [プロバイダ] を選択します。
7. パッケージのキャプチャに仮想マシンが使用する [イメージ] を選択します。

   イメージに App Volumes Agent がインストールされていることを確認します。
8. パッケージのキャプチャに仮想マシンが使用する [イメージ バージョン] を選択します。
9. パッケージ用の仮想マシンの作成に使用される [デスクトップ モデル] を選択します。

10 [マシン ID] を選択します。

環境に登録されている `Azure Active Directory` または、構成済みの Active Directory ドメインのいずれかを選択できます。構成済みの Active Directory ドメインを選択する場合は、選択した Horizon Edge からドメインにアクセスできることを確認します。

注： `Azure Active Directory` の場合、Windows 11 および Windows 10 デバイスはすべてサポートされます。ただし、Windows Server 2019 Home エディションと、Azure で実行されている新しい仮想マシンを除きます（サーバ コアはサポートされていません）。

11 アプリケーションをキャプチャするために仮想マシンが割り当てられている [パッケージャ] またはユーザーを選択します。

ユーザーのドメインは、選択した Active Directory ドメインと同じである必要があります。

12 [クラシック] と [オンデマンド] のいずれかの配信方法を選択します。

デフォルトでは、パッケージ配信は `Classic` です。パッケージを `On-demand` として構成すると、エンド ユーザーがアプリケーションを起動したときにのみパッケージの添付が行われます。

注： オンデマンド サポートのないバージョンの Horizon Agent インストーラ `23.1.0.21387799` 以前を使用して作成されたパッケージの場合、管理者は `On-demand` から `Classic` および `Classic` から `On-demand` に変更できます。ただし、App Volumes エージェントは、オンデマンドの動作のように既存のパッケージを仮想化することはできません。

13 [保存] をクリックします。

結果

- パッケージが追加されるとすぐに、パッケージのステータスは `Desktop provisioning is in progress` です。
- デスクトップ プロビジョニングが完了し、パッケージャに仮想マシンが割り当てられると、パッケージのステータスは `Ready for capture` になります。

次のステップ

アプリケーション パッケージをキャプチャするには、「Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージのキャプチャ」に記載されている手順を実行します。

Horizon Cloud Service - next-gen を使用した App Volumes アプリケーションの削除

アプリケーションは、必要に応じて削除できます。アプリケーションを削除すると、関連付けられたパッケージも削除されます。

アプリケーションに資格がある場合、そのアプリケーションは削除できません。まず、アプリケーションの資格を解除してから、削除操作を実行する必要があります。アプリケーションから資格を削除する方法の詳細については、「Horizon Cloud Service - next-gen を使用した App Volumes 資格の削除」を参照してください。

前提条件

アプリケーションに資格がないことを確認します。

手順

1 Horizon Universal Console で、[デスクトップおよびアプリケーション カタログ] - [App Volumes] の順に移動します。

2 目的のアプリケーションを選択し、[削除] をクリックします。

3 [アプリケーションを削除] ウィンドウで、[削除] をクリックします。

Horizon Cloud Service - next-gen を使用して既存のアプリケーション パッケージをインポートし App Volumes アプリケーションを追加する

インポート機能を使用して、別の Horizon Edge デプロイで作成された App Volumes アプリケーション パッケージを現在のデプロイで使用できます。また、この機能を使用して、パッケージにアプリケーション属性がない場合やパッケージがインベントリから欠落している場合に、パッケージを再インポートすることもできます。

Microsoft Azure Storage Explorer の操作の詳細については、Storage Explorer のドキュメントを参照してください。

前提条件

次の点に注意してください。

- 環境が Horizon Cloud Service - next-gen で App Volumes アプリケーションを使用するための概要と前提条件 に記載されているすべての前提条件を満たしていることを確認します。
- ファイアウォールを介してステージング ファイル共有にアクセスできるアドレスの許可リストに、クライアント IP アドレスを追加します。Microsoft Azure ポータルで、ストレージ アカウントのネットワーク セキュリティ設定を含むページに移動します。[ファイアウォール] セクションで、クライアント IP アドレスを追加するオプションを有効にします。

  Microsoft Azure Storage Explorer で適切なファイル共有に移動すると、このファイル共有の場所を確認できます。Horizon Edge のステージング ファイル共有を特定するには、[リソース] - [キャパシティ] の順に移動し、Horizon Edge の名前をクリックして、[App Volumes アプリケーション ストレージ] セクションに移動します。
- インポートするアプリケーション パッケージの JSON ファイルと VHD ファイルは、Horizon Edge の `appvolumes/packages` の下にあるステージング ファイル共有に含まれている必要があります。

  ヒント: アプリケーション パッケージのインポートに必要な JSON ファイルと VHD ファイルは、`7Zip.json` および `7Zip.vhd` のようになります。JSON および VHD ファイルのソースの一部は、スタンドアローン キャプチャおよび別の Horizon Edge のファイル共有です。

注: ファイル共有のファイルにアクセスするには、Microsoft Azure ポータルでストレージ アカウントのファイアウォール ルールの更新が必要になる場合があります。

手順

1 Horizon Universal Console で、[デスクトップおよびアプリケーション カタログ] に移動します。

2 [デスクトップおよびアプリケーション カタログ] ページで、[App Volumes] をクリックします。

3 [追加] - [アプリケーションのインポート] の順にクリックします。

4 [インポート] ページで、アプリケーション パッケージを Horizon Universal Console にインポートするサイトと Horizon Edge を選択します。

5 使用事例に応じて、対応する [インポート] オプションを使用します。

オプション	使用事例
新しいパッケージ	このオプションは、選択した Edge のステージング ファイル共有から App Volumes インベントリに新しいアプリケーション パッケージをインポートする場合に使用します。
すべてのパッケージ	所有者やショートカットなどのアプリケーション属性が欠落している場合や、パッケージがすでにインポートされているがインベントリから欠落している場合は、このオプションを使用してアプリケーション パッケージを再インポートします。

6 [インポート] をクリックします。

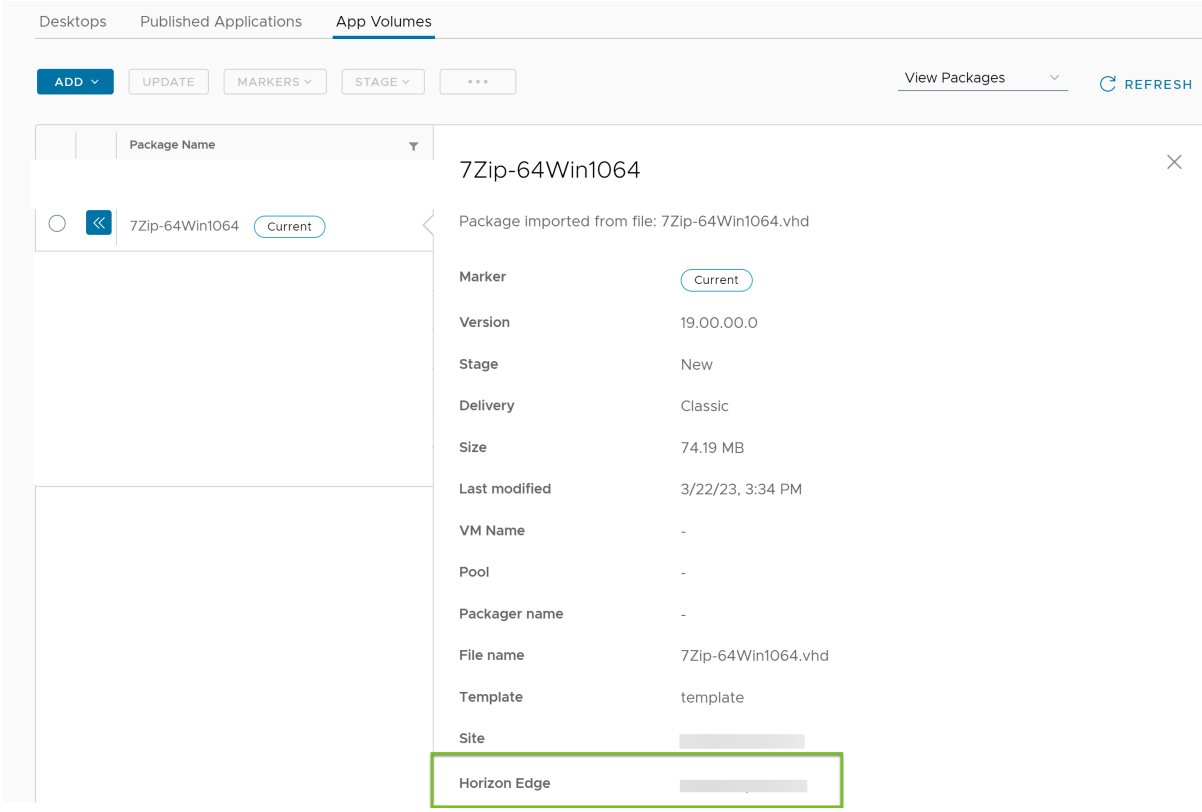
インポートが正常に完了すると、Horizon Universal Console の [App Volumes] タブにアプリケーション パッケージが表示されます。新しいアプリケーションを表示するには、ページの更新が必要になる場合があります。

結果

- インポートされると、JSON データは Horizon Universal Console で更新されます。

  重要： ステージングおよび配信ファイル共有から JSON または VHD ファイルを直接削除しないでください。アプリケーション パッケージを削除するには、常に Horizon Universal Console を使用します。

- アプリケーション パッケージがインポートされている Horizon Edge を表示するには、パッケージに移動し、パッケージの詳細を展開して、Horizon Edge 情報を探します。



追加の Horizon Edge デプロイに対して再度インポートを実行する場合 (VHD および JSON ファイルをインポート元とする各 Horizon Edge にコピー/転送した後)、アプリケーションは複数の Horizon Edge デプロイで使用可能になります。この場合、[パッケージの詳細] ウィンドウの Horizon Edge 情報には、Horizon Edge デプロイの数が表示されます。すべてのデプロイを表示するには、[表示] をクリックします。ページのテーブルに Horizon Edge デプロイの詳細が表示されます。

Horizon Cloud Service - next-gen を使用した App Volumes アプリケーションでのアプリケーション パッケージの管理

Horizon Cloud Service - next-gen 内で App Volumes アプリケーション パッケージを管理できます。

Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージのライフサイクル ステージの変更

App Volumes アプリケーション パッケージにはさまざまなステージがあります。これらのステージは、パッケージの配信状態に関する情報を提供します。管理者は、アプリケーション パッケージを正常にキャプチャした後に、パッケージのステージを変更できます。

パッケージのキャプチャに成功すると、パッケージのステータスが `Ready` になり、パッケージのステージが自動的に `New` に設定されます。ここで、パッケージのステージを変更できます。

注： パッケージのステージが `Unpackaged` になっている場合、パッケージのライフサイクルは変更できません。

パッケージがアプリケーションに追加されたが、まだキャプチャされていない場合、パッケージのステージは自動的に `Unpackaged` に設定されます。パッケージのステータスは `Ready for capture` になります。

パッケージのライフサイクル ステージは次のとおりです。

新規

パッケージをテストする準備ができました。

テスト済み

パッケージのテストが完了し、パッケージを公開する準備が整いました。

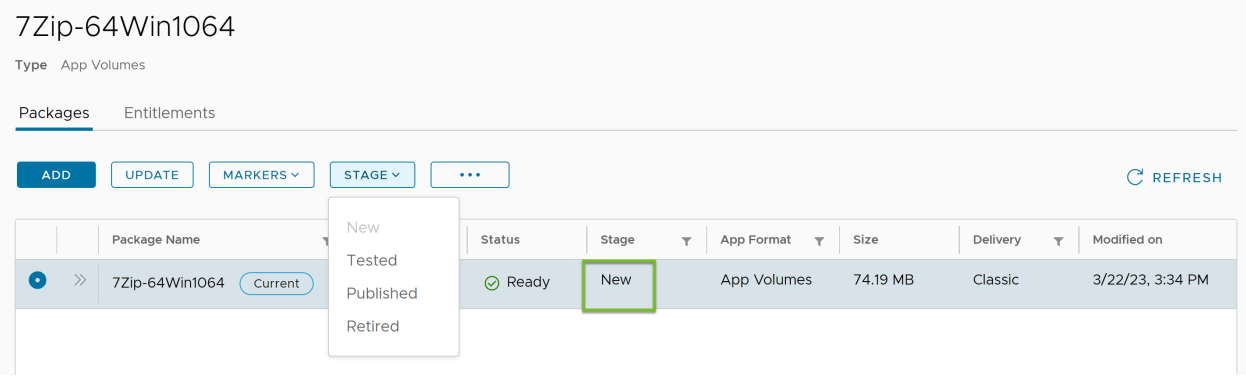
公開済み

パッケージは、パッケージに割り当てられているユーザーに対して公開されています。

離脱

パッケージは不要になったか、更新されていません。

離脱ステージのパッケージを含むアプリケーションにエンティティを割り当てることもできます。



前提条件

パッケージがキャプチャされ、パッケージのステータスが `Ready` になっていることを確認します。

アプリケーション パッケージをキャプチャするには、Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージのキャプチャを参照してください。

手順

1. Horizon Universal Console で、[デスクトップとアプリケーション カタログ] - [App Volumes] の順に移動します。
2. [パッケージの表示] をクリックします。
3. 目的のパッケージを選択します。
4. [ステージ] をクリックし、目的のライフサイクル ステージをクリックします。

   更新されたパッケージのステージは、パッケージのリストを含むページの [ステージ] 列に表示されます。

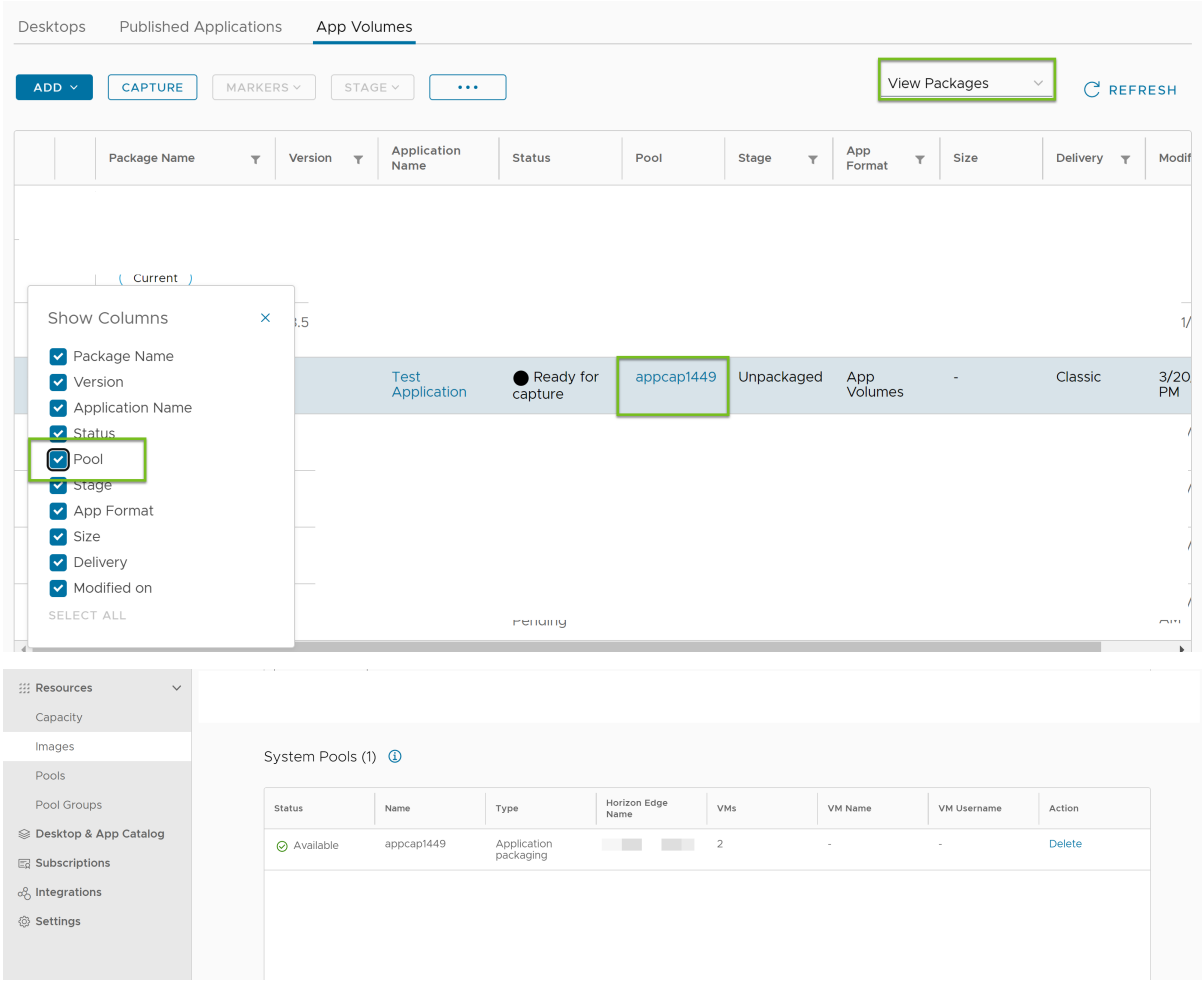
Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージのキャプチャ

各 App Volumes パッケージには、アプリケーションの実行に必要な 1 つ以上のプログラムが格納されています。1 つのパッケージを複数のユーザーおよびユーザー グループに配信できます。アプリケーション パッケージをキャプチャするには、次のワークフローを使用します。

キャプチャ プロセスを初めて開始するときは、キャプチャ デスクトップ仮想マシンがアプリケーションのキャプチャに使用できるようになるまで、最大で 10 分かかります。この 20 分間に、システムがキャプチャ プロセス VDI デスクトップ システム プールと、キャプチャ デスクトップ仮想マシンに使用される 2 台のデスクトップ仮想マシンを作成しています。システムが基盤となるシステム プールと仮想マシンを作成するには、最大で 20 分かかる場合があります。

- システムは、Horizon Edge ごとに 1 つのユーザー、1 つのイメージにつきプールを 1 つ作成します。このため、1 つまたは複数のプールを作成する場合があります。
- 各システム プールに 2 台のデスクトップがあるため、1 つ目の完了後に 2 つ目のキャプチャをすばやく開始できます。
- これらのプールは `appcaptureXXX` パターンに従って名前が付けられます。ここで、`XXX` はランダムに生成された番号になります。
- パッケージ化プロセスに使用されるイメージを更新する場合は、更新する前にこれらのプールを削除する必要があります。

  キャプチャ デスクトップ仮想マシンで使用されるイメージは、[リソース] - [イメージ] ページに表示されます。特定のパッケージのキャプチャ デスクトップ仮想マシンで使用されるイメージを簡単に識別するには、パッケージのリスト（[パッケージの表示]）ページに移動します。[列の管理] ボタンをクリックし、`Pool` を選択します。[プール] 列で、目的のパッケージのプール名をクリックします。対応するイメージ ページが表示されます。このページには、そのパッケージのキャプチャ デスクトップ仮想マシンで使用されるイメージが示され、プール情報はイメージ ページの [システム プール] セクションに表示されます。



- 近い将来に追加のキャプチャを実行する予定がない場合は、これらのシステム プールを削除して、理由もなく環境内に存在しないようにすることができます。削除した場合、次回キャプチャを実行したときに、システムは新しいものを作成するまでに最大で 20 分かかります。

  注： 前述のイメージ ページのナビゲーション情報を使用して、目的のパッケージのイメージに移動します。[システム プール] セクションに移動し、目的のプールを削除します。

注： キャプチャに失敗した場合は、[監視] - [アクティビティ ログ] の順に移動して、システム アクティビティ イベントを表示できます。

これで、[アプリケーション] ページのリストにアプリケーション パッケージのエントリが作成されます。このリストエントリの [ステータス] をポイントすると、キャプチャ仮想マシンのステータスが示されます。ステータスが `Desktop ready for application capture` の場合は、手順に従ってキャプチャ デスクトップ仮想マシンにログインし、アプリケーション パッケージのアプリケーションのインストールを開始できます。

注： 1 時間以内にキャプチャを開始しない場合、キャプチャ デスクトップ仮想マシンは App Volumes サービスによって自動的にパワーオフされます。このパワーオフにより、組織の電源管理コストを節約できます。ただし、管理者のユーザー エクスペリエンスは変わりません。キャプチャの準備ができたら、キャプチャ デスクトップ仮想マシンを引き続き使用して、次の手順に進むことができます。

前提条件

キャプチャするパッケージのステータスが `Ready for capture` になっていることを確認します。

手順

1 Horizon Universal Console で、[デスクトップとアプリケーション カタログ] - [App Volumes] の順に移動します。

2 [パッケージの表示] をクリックします。

3 キャプチャするパッケージを選択します。

4 [キャプチャ] をクリックします。

5 パッケージ仮想マシンに接続するには、VMware Horizon® Client™ またはブラウザのいずれかを選択します。

6 プロンプトに従って、パッケージャ仮想マシンを起動します。

パッケージャ仮想マシンが開き、「**処理中の App Volumes パッケージ**」情報が表示されます。

Horizon Universal Console で、パッケージのステータスが `Capture in progress` になります。

7 パッケージャ仮想マシンで、アプリケーションをダウンロードしてインストールします。

8 アプリケーションをインストールしたら、[処理中の App Volumes パッケージ] ダイアログ ボックスで [OK] をクリックします。

9 [インストール完了の確認] ダイアログ ボックスで、[はい] をクリックします。

10 （オプション）[VMware App Volumes - パッケージのファイナライズ] ウィンドウで、パッケージャのメモを追加します。

11 [完了] をクリックします。

12 [再起動が必要] ダイアログ ボックスで [OK] をクリックします。

パッケージ仮想マシンが再起動します。

13 以前に使用したパッケージャ認証情報を使用して再度ログインします。

14 [パッケージング成功] ダイアログ ボックスで [OK] をクリックします。

結果

キャプチャが完了すると、パッケージ仮想マシンはパッケージャから割り当て解除され、仮想マシンは削除されます。プール テンプレートのサイズは `1` です。

パッケージのステータスが `Ready` になりました。パッケージのライフサイクル ステージは `New` です。

次のステップ

パッケージのライフサイクルの変更、パッケージの `Current` マーカーの設定、パッケージの資格の作成などのパッケージ管理操作を実行できます。

これらのパッケージの管理操作の詳細については、Horizon Cloud Service - next-gen を使用した App Volumes アプリケーションでのアプリケーション パッケージの管理を参照してください。

Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージの移動

アプリケーション間でパッケージを移動できます。アプリケーション間で同様のパッケージ要件が存在する場合は、移動機能を使用できます。

前提条件

- 移動するパッケージに資格または CURRENT マーカーがないことを確認します。

  資格または CURRENT マーカーを含むパッケージは移動できません。パッケージに資格または CURRENT マーカーがある場合は、資格またはマーカーを削除して、パッケージの移動操作を再度実行します。

- パッケージがキャプチャされ、ステータスが Ready になっていることを確認します。

  パッケージは、パッケージ キャプチャ後にのみ移動できます。アプリケーション パッケージのキャプチャ方法についての詳細は、Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージのキャプチャを参照してください。

手順

1. Horizon Universal Console で、[デスクトップとアプリケーション カタログ] - [App Volumes] の順に移動します。
2. [パッケージの表示] をクリックします。
3. 移動操作を行うパッケージを選択します。
4. 横方向の省略記号アイコン をクリックして、[移動] をクリックします。
5. [パッケージの移動] ウィンドウの [アプリケーション] ドロップダウン ボックスで宛先のアプリケーションを選択します。
6. [保存] をクリックします。

   パッケージが宛先のアプリケーションに移動します。
7. パッケージの移動を確認するには、宛先のアプリケーションに移動し、そのアプリケーションのパッケージのリストを表示します。

Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージの編集

パッケージの名前、説明、配信モードなどのプロパティを変更するために、パッケージの編集機能を使用してパッケージを編集できます。

Ready ステータスのパッケージにのみ [メモ] フィールドがあります。

パッケージを編集するときに、[メモ] フィールドを使用して、パッケージ仮想マシンに追加されたメモが表示されます。このテキスト フィールドに追加された情報は、アプリケーション キャプチャの前にこのフィールドに存在する情報を上書きします。App Volumes Manager でこのテキスト フィールドを変更すると、メタデータのみが更新され、元のパッケージ仮想ディスク ファイルやパッケージの JSON ファイルは更新されません。

手順

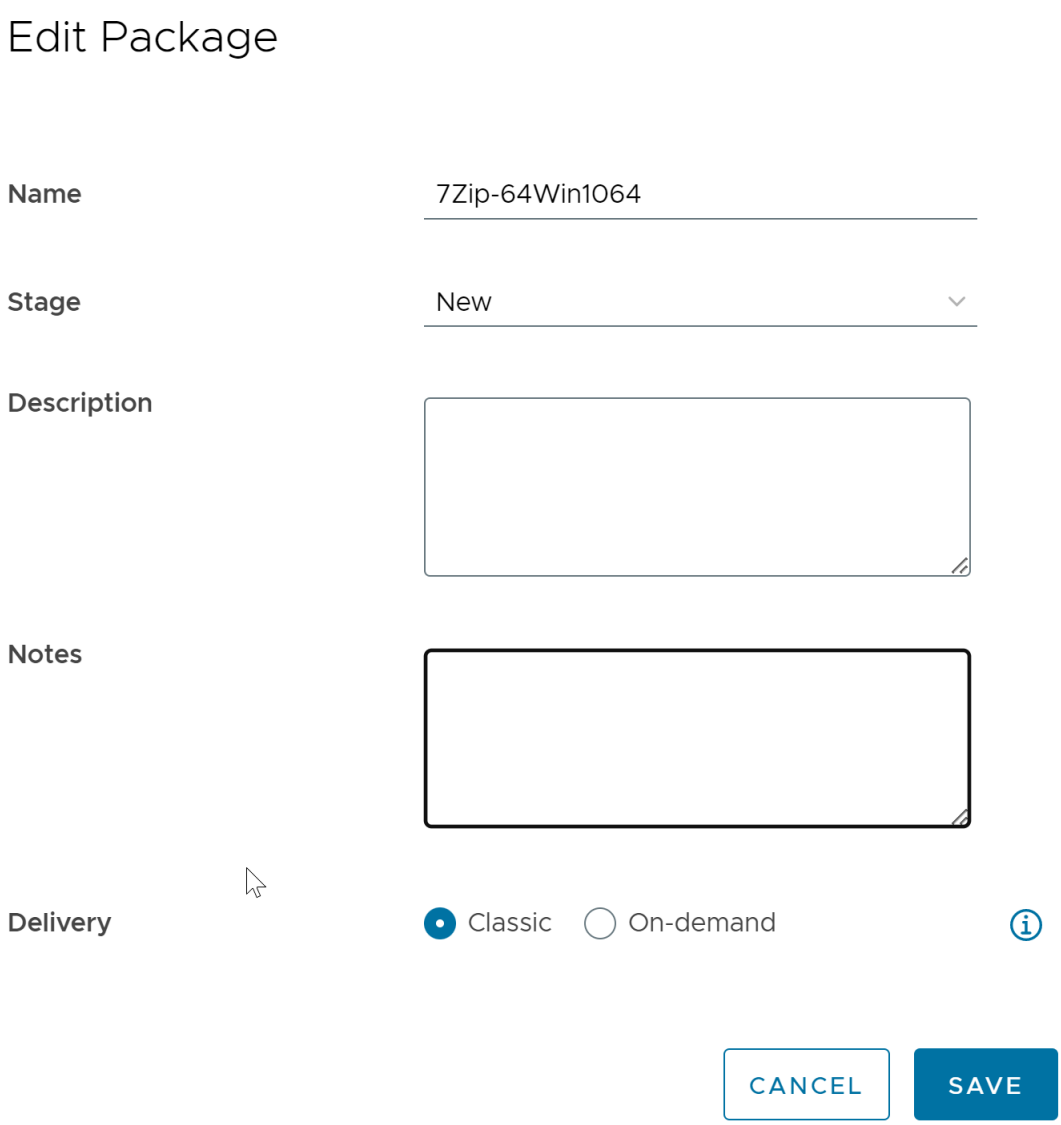
1. Horizon Universal Console で、[デスクトップおよびアプリケーション カタログ] - [App Volumes] の順に移動します。

2 [パッケージの表示] をクリックします。

3 編集するパッケージを選択します。

4 省略記号ボタン をクリックし、[編集] をクリックします。

5 [パッケージの編集] ウィンドウで、目的のプロパティを編集します。



6 [保存] をクリックします。

パッケージが編集されました。

App Volumes アプリケーションの資格のシナリオについて

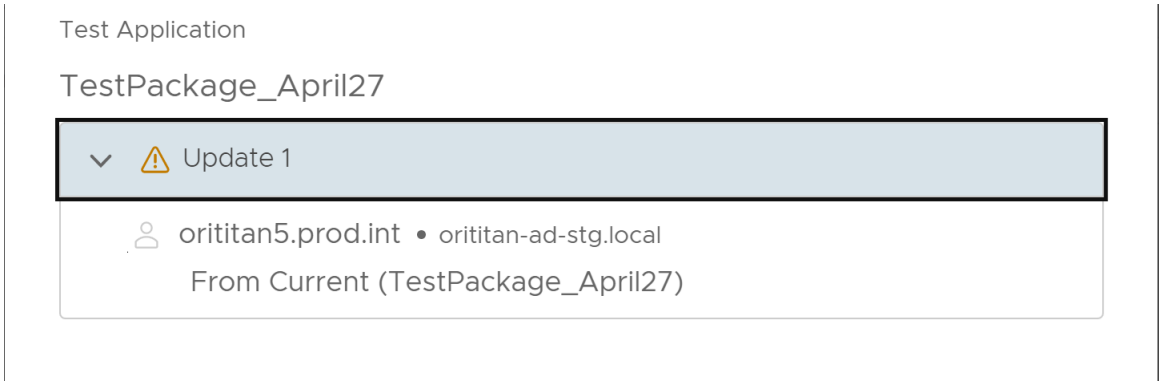
新たに選択したアプリケーション パッケージの資格を作成する場合は、既存の資格の更新または新しい資格のいずれかになります。新たに選択したアプリケーション パッケージが既存のアプリケーション パッケージと同じ場合、ユーザーまたはユーザー グループの資格は変わりません。

資格のシナリオ

更新

選択したパッケージによって、ユーザーまたはユーザー グループの既存の資格が置き換えられます。したがって、資格は既存の資格の更新と見なされます。

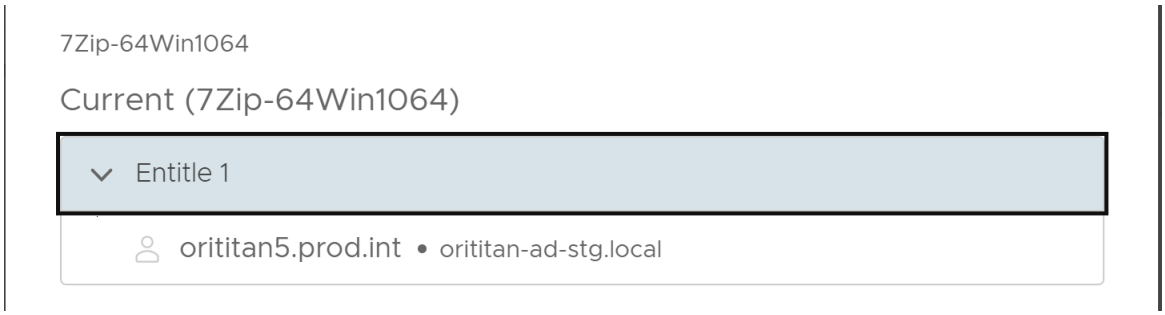
次の図の orititan5.prod.int は、`Current (Testpackage_April27)` という資格が付与されたユーザーです。`TestPackage_April27` を選択すると、この資格によって `Current (Testpackage_April27)` が置き換えられます。したがって、このシナリオは更新と見なされます。



新規（資格付与）

選択したパッケージは、ユーザーまたはユーザー グループに対する新しい資格です。

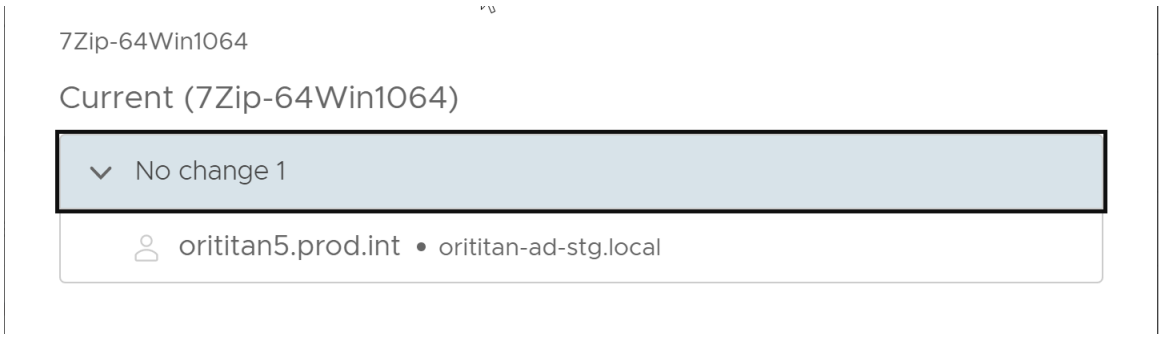
次の図の `Current (7Zip-64Win1064)` は、ユーザー orititan5.prod.int に対する新しい資格です。



変更なし

選択したパッケージにはユーザーまたはユーザー グループに対する資格がすでに付与されているため、資格は変更されません。

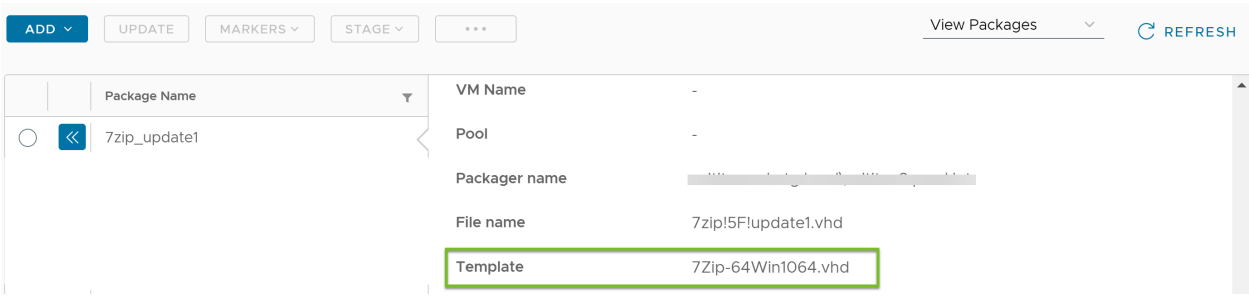
次の図では、資格に対して `Current (7Zip-64Win1064)` が再度選択されていますが、ユーザー orititan5.prod.int には同じパッケージの資格がすでに付与されています。したがって、資格に変更はありません。



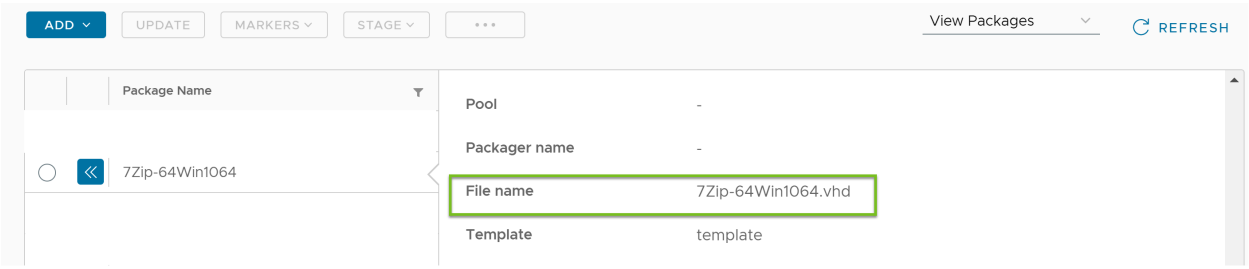
Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージの更新

既存のパッケージを更新して、既存のパッケージの新しいバージョンを作成できます。既存のパッケージはテンプレートとなるか、新しいバージョンのパッケージの基本パッケージとして機能します。

次のスクリーンショットでは、`7zip_update1` は更新されたパッケージで、`7Zip-64Win1064.vhd` はテンプレートで、これは既存のパッケージのファイル名です。



次のスクリーンショットでは、`7Zip-64Win1064` は既存のパッケージで、ファイル名は `7Zip-64Win1064.vhd` です。



前提条件

更新するパッケージがパッケージ化プロセスを完了し、パッケージのステータスが `Ready` になっていることを確認します。

手順

1 Horizon Universal Console で、[デスクトップおよびアプリケーション カタログ] - [App Volumes] の順に移動します。

2 [パッケージの表示] をクリックします。

3 更新するパッケージを選択します。

4 [更新] をクリックします。

5 [パッケージの更新] ウィンドウで、必要な情報を追加します。

6 [保存] をクリックします。

結果

更新されたパッケージがパッケージの一覧に表示されます。

Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージの削除

パッケージが不要になった場合は、パッケージを削除できます。

前提条件

パッケージを削除する前に、必ずパッケージのマーカーおよび資格を削除してください。

手順

1 Horizon Universal Console で、[デスクトップおよびアプリケーション カタログ] - [App Volumes] の順に移動します。

2 [パッケージの表示] をクリックします。

3 削除するパッケージを選択します。

4 省略記号ボタンをクリックし、[削除] をクリックします。

5 [パッケージの削除] ウィンドウで、[削除] をクリックします。

削除されたパッケージは、パッケージの一覧から削除されます。

> **注：** パッケージが `Delete Failed` ステータスの場合は、パッケージの削除を再試行します。
>
> パッケージがこのステータスになる理由の 1 つとして、1 人以上のユーザーがデスクトップにログインしていて、現在このアプリケーション パッケージを使用していることが考えられます。

Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージへの CURRENT マーカーの設定

アプリケーションに複数のパッケージがあり、アプリケーションの最新バージョンをユーザーまたはユーザー グループに配布する場合は、パッケージに `CURRENT` マーカーを設定できます。ユーザーまたはユーザー グループは、マーカーが 1 つのパッケージから削除され、もう一方のパッケージに設定されている場合でも、マーカーを含むパッケージ バージョンを常に受信するように構成できます。

`CURRENT` マーカーをパッケージに設定する場合に考慮する事項を次に示します。

- `CURRENT` マーカーを使用して設定されたパッケージでは、移動操作と削除操作を実行できません。

  いずれかの操作を実行するには、このマーカーをパッケージから削除する必要があります。

- アプリケーション内の 1 つのパッケージのみを `CURRENT` として設定できます。

前提条件

CURRENT としてマークするパッケージがパッケージ化プロセスを完了し、パッケージのステータスが Ready になっていることを確認します。

手順

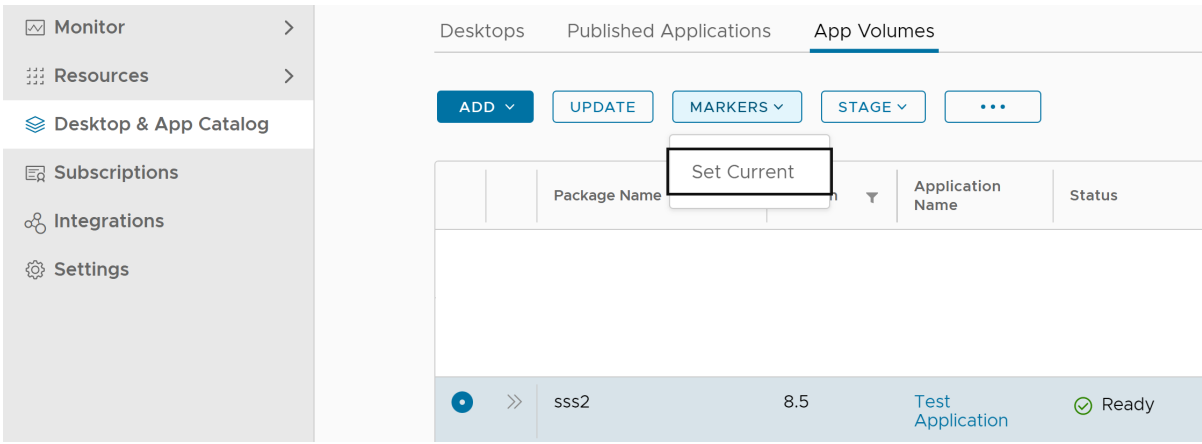
1 Horizon Universal Console で、[デスクトップおよびアプリケーション カタログ] - [App Volumes] の順に移動します。

2 CURRENT マーカーを設定するパッケージがあるアプリケーションをクリックします。

このアプリケーションのパッケージのリストが表示されます。

3 パッケージを選択します。

4 [マーカー] - [現在の設定] の順にクリックします。



5 [現在の設定] ダイアログ ボックスで、[設定] をクリックします。

パッケージ名が CURRENT マーカーとともに表示されます。

次のステップ

これで、このパッケージの資格をユーザーまたはユーザー グループに付与できるようになりました。資格の作成の詳細については、Horizon Cloud Service - next-gen を使用した App Volumes アプリケーションの資格の作成を参照してください。

VMware Horizon® Cloud Service™ - next-gen - App Volumes アプリケーション パッケージへの CURRENT マーカーの設定解除

Current とマークされたアプリケーション パッケージが最新バージョンでなくなった場合は、パッケージの Current マーカーを削除できます。同じアプリケーションの別のパッケージにマーカーを設定すると、このアクションにより、以前のパッケージのマーカーが自動的に設定解除されます。

アプリケーションは、Current としてマークされたパッケージを 1 つだけ持つことができます。

マーカーがパッケージから削除されると、資格は Current パッケージの受信を停止します。マーカーを別のパッケージに移動すると、資格は自動的に Current に設定されたパッケージの受信を開始します。

手順

1 Horizon Universal Console で[デスクトップおよびアプリケーション カタログ] - [App Volumes] の順に移動します。

2 [パッケージの表示] をクリックします。

3 Current マーカーの付いたパッケージを選択します。

4 [マーカー] - [現在のものを削除] をクリックします。

5 [現在のものを削除] の確認ウィンドウで、[削除] をクリックします。

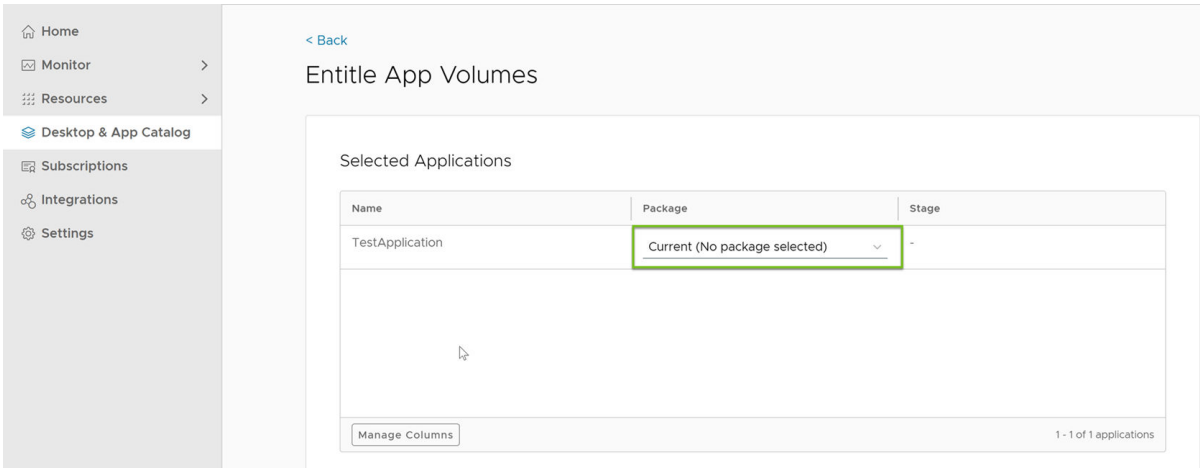
これで、パッケージに Current マーカーがなくなります。

Horizon Cloud Service - next-gen を使用した App Volumes アプリケーションの資格の作成

App Volumes アプリケーション パッケージをエンド ユーザーに提供するには、ユーザーまたはユーザー グループにアプリケーションの使用資格を付与する必要があります。

アプリケーションの資格を作成する場合に考慮する事項は次のとおりです。

- アプリケーションの資格は、単一または複数のユーザーまたはユーザー グループに付与できます。
- 資格は、特定のパッケージ バージョンまたはパッケージにまだ設定されていない CURRENT マーカーに基づいて作成できます。CURRENT マーカーを選択すると、アプリケーションにユーザーまたはユーザー グループの資格が付与されます。後でこのアプリケーションのパッケージが作成され、CURRENT とマークされると、ユーザーまたはユーザー グループはこのパッケージを受け取ります。



- マーカーベースの資格の場合、ユーザーまたはユーザー グループは常に CURRENT バージョンのパッケージを受け取ります。管理者が CURRENT マーカーを別のパッケージに設定すると、ユーザーまたはユーザー グループは次回のログイン時に、CURRENT マーカーを持つ新しいパッケージを受け取ります。

- アプリケーションにパッケージがない場合でも、アプリケーションにユーザーまたはユーザー グループの資格を付与できます。

アプリケーション パッケージをユーザーまたはユーザー グループに配信するには、パッケージのステータスを `Ready` にする必要があります。

複数のアプリケーションをユーザーまたはユーザー グループに同時に割り当てることもできます。

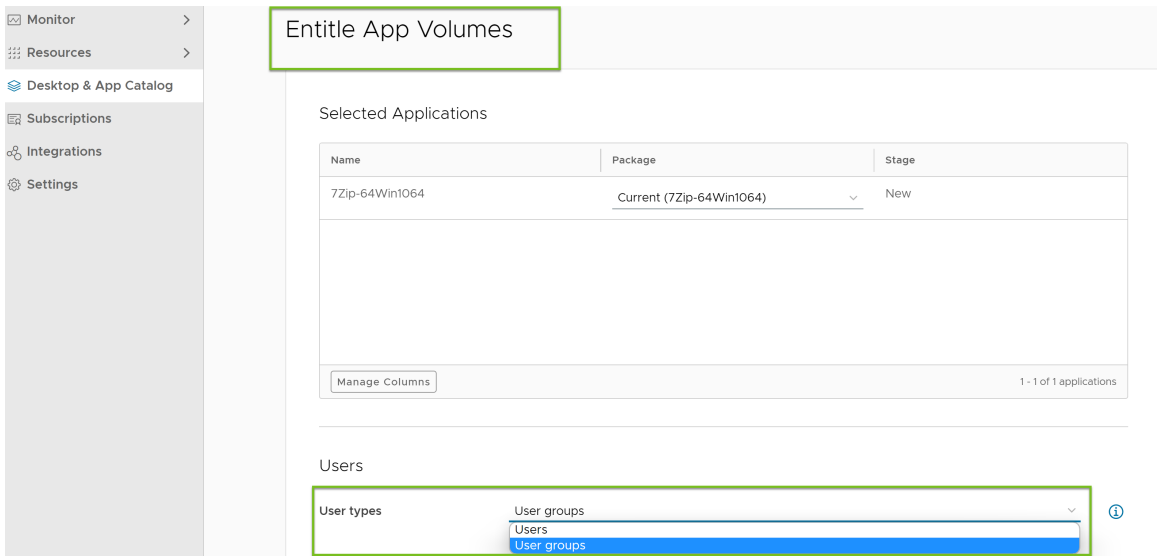
前提条件

アプリケーションをキャプチャした後、パッケージは `Ready` ステータスになります。詳細については、Horizon Cloud Service - next-gen を使用した App Volumes アプリケーション パッケージのキャプチャを参照してください。

App Volumes の資格を作成する前に、まずフローティング VDI デスクトップ割り当てを作成する必要があります。Microsoft Windows 10 および Windows 11 オペレーティング システムの処理が必要になるため、この割り当てには、少なくとも 2 基の vCPU と 4 GB の RAM を提供する VMware 推奨のデスクトップ モデルが必要です。

手順

1. Horizon Universal Console で、[デスクトップおよびアプリケーション カタログ] - [App Volumes] の順に移動します。
2. ユーザーまたはユーザー グループに資格を付与するアプリケーションを選択します。
3. [資格] - [資格を付与] の順にクリックします。
4. [App Volumes の資格を付与] ページで、次の手順を実行します。
   a. 目的のパッケージを選択します。
   b. [ユーザー タイプ] を選択します。
   c. 前の手順で選択したユーザー タイプに応じて、ユーザーまたはユーザー グループを追加します。



5 [保存] をクリックします。

アプリケーションのすべての資格が [資格] タブに表示されます。

a [デスクトップとアプリケーション カタログ] - [App Volumes] の順に移動します。

b アプリケーションをクリックします。

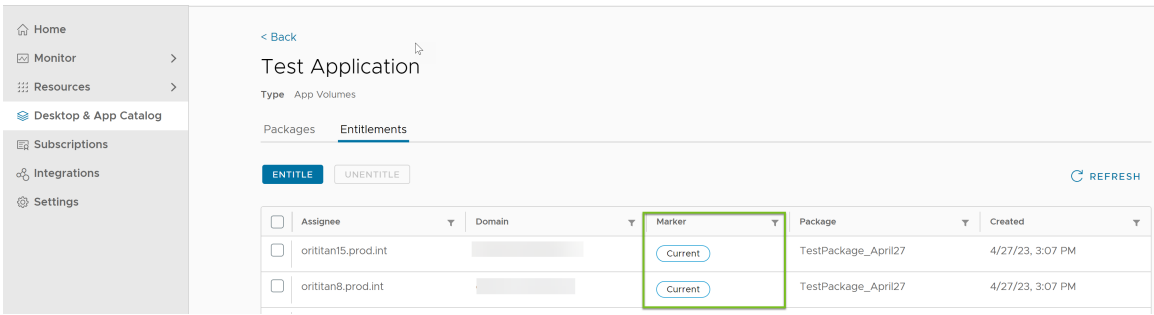
c アプリケーションの詳細ページで、[資格] タブをクリックします。

アプリケーションに関連付けられているすべての資格がページに表示されます。

注： Horizon Cloud Service first-gen では、各割り当てに複数のアプリケーションを割り当てることができ、これを複数のユーザーまたはユーザー グループに割り当てることができます。したがって、[割り当て] ページには、すべてのアプリケーションとそれに対応するユーザーまたはユーザー グループが表示されます。

ただし、VMware Horizon® Cloud Service™ - next-gen では、アプリケーション資格ページに表示されるのは、その特定のアプリケーションのアプリケーション パッケージに関連付けられているユーザーまたはユーザー グループのみです。

特定のユーザーまたはユーザー グループに対して `CURRENT` マーカーを含むパッケージが選択されている場合、このページの [マーカー] 列には、そのユーザーまたはユーザー グループの資格に対して `CURRENT` が表示されます。



Horizon Cloud Service - next-gen を使用した App Volumes 資格の削除

アプリケーションから資格を削除することで、アプリケーションの資格を変更できます。資格を削除するには、[資格を解除] ボタンを使用します。

手順

1 Horizon Universal Console で、[デスクトップおよびアプリケーション カタログ] - [App Volumes] の順に移動します。

2 目的のアプリケーションを選択します。

3 [資格] - [資格を解除] - [ ] の順にクリックします。

4 [アプリケーションの資格を解除] ウィンドウで、割り当て先を選択します。

5 [資格を解除] をクリックします。

結果

[デスクトップおよびアプリケーション カタログ] ページでは、アプリケーションの [資格] 列に 0 が表示されます。これは、このアプリケーションのすべての資格が削除されたためです。

Horizon Cloud Service - next-gen と Workspace ONE Intelligent Hub の統合

認証情報を入力しなくても、Workspace ONE Intelligent Hub からデスクトップとアプリケーションにアクセスできます。

前提条件

- アクセス テナントは、オフラインで作成されるか、現在のアクセス ワークフローを使用して作成されます。
- ID プロバイダに接続すると、WORKSPACE ONE Access が ID プロバイダとして選択されます。詳細については、ID プロバイダの接続を参照してください。
- Horizon Client バージョン 8.10 以降が使用されます。

手順

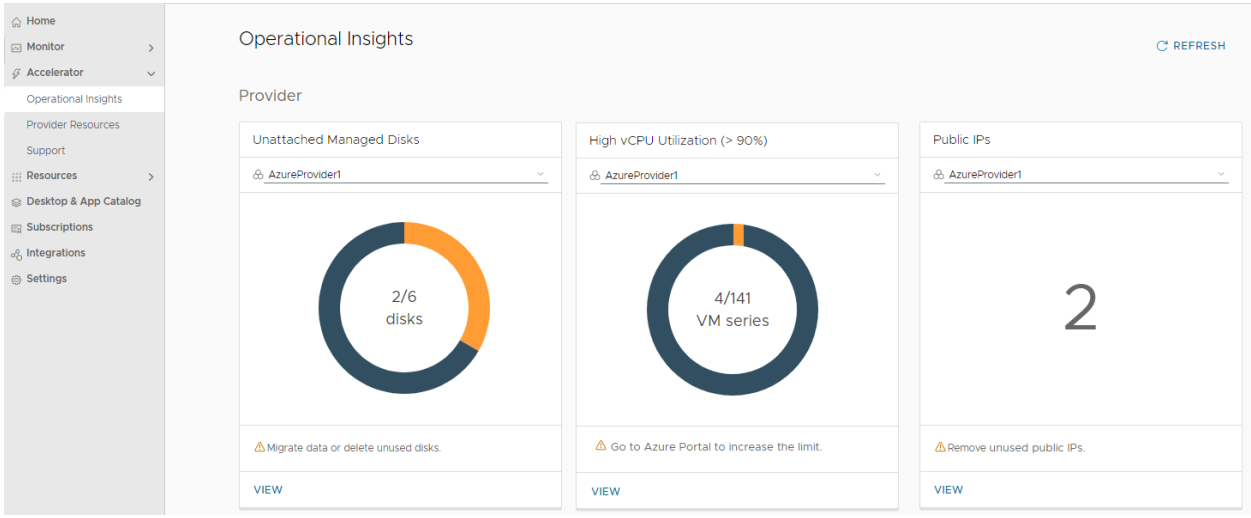
1. Horizon Universal Console にログインします。
2. [ホーム] ページで、[統合] をクリックします。
3. [統合] ページで、[Workspace One Intelligent Hub] タイルの [管理] をクリックします。
4. [Workspace One Intelligent Hub] ページで、トグルを選択して [Intelligent Hub] を有効にします。

   これで、資格が Workspace ONE Intelligent Hub のエンドユーザーに表示されるようになりました。

   注： この機能では、Windows、Mac、Linux、および HTML Access クライアントのみがサポートされます。

Horizon Accelerator - はじめに

このドキュメント ページでは、VMware Horizon Accelerator (VHA) SaaS サービスを開始する方法について説明します。下部のリンクから、より詳細な情報を含むページに移動できます。



簡単な紹介

Horizon Accelerator は、Horizon ユニバーサル ライセンス サブスクリプションのアドオン SKU です。

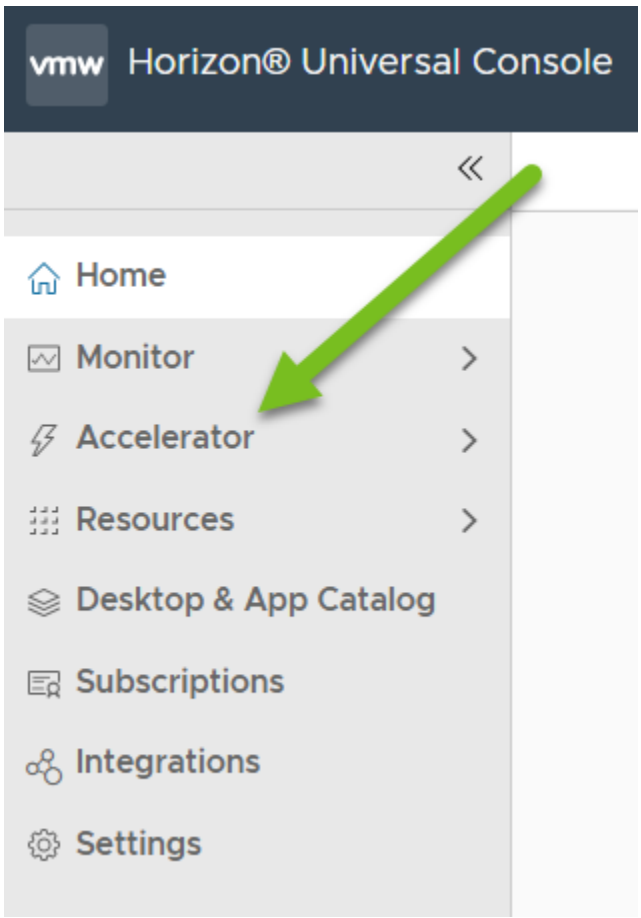
Horizon Accelerator では、Horizon Cloud Service - next-gen 環境に対する Day 0 から Day 2 の継続的なサポートが提供され、お使いの環境についてのインサイトと可視性を得ることができます。

Horizon Accelerator を使用すると、価値の提供までの時間を短縮し、VDI 環境の複雑さと学習曲線を排除できます。専用 VDI の専門知識が IT スタッフを補強し、Day 0 から Day 2 までの運用の負担を軽減します。

Horizon Universal Console 内の VHA Control Center にある Horizon Accelerator 機能にアクセスします。

要件

next-gen 環境に関連付けられているライセンスによって Horizon Accelerator を使用する資格が付与されると、次のスクリーンショットに示すように、Horizon Universal Console はコンソールのナビゲーションに [Accelerator] を自動的に表示します。



新機能がクラウド制御プレーンにリリースされると、自動的に使用可能になります。

環境に関連付けられているライセンスを確認するには、コンソールの [サブスクリプション] ページを使用します。Horizon Universal Console を使用した Horizon ライセンスの追跡を参照してください。Horizon Accelerator を使用するには、環境に以下が必要です。

- アドオン SKU を提供する Horizon サブスクリプション。Horizon サブスクリプションについては、VMware Horizon サブスクリプション比較マトリックスを参照してください。
- Horizon Accelerator ライセンス。
- 4 章 Horizon Cloud Service - next-gen 管理者のオンボーディング Horizon Cloud Service - next-gen にオンボーディング済みです。

VMware Horizon Accelerator (VHA) Control Center

このコントロール センターを使用すると、次世代環境で構成されたプロバイダ内のリソースに対するインサイトと可視性を獲得できると同時に、各プロバイダのユーザー インターフェイスまたはポータルにログインして各リソースを確認する必要がなくなります。

運用に関するインサイト

[運用に関するインサイト] ビューには、運用コストを削減するために調整できる、プロバイダ内のリソースに対する実行可能なインサイトと画面上のガイダンスが表示されます。

各リソース関連の領域には、存在する可能性のある問題が強調表示され、最適化の機会が示されます。

インフラストラクチャ リソースのインサイト

[プロバイダ リソース] ビューは [運用に関するインサイト] ビューと連携して機能し、プロバイダ リソースを可視化します。

プロバイダ リソースの状態を可視化するこの機能は、プロバイダのポータルにアクセスできない可能性がある次世代環境の管理者にとって特に有益です。

[プロバイダ リソース] ビューには、リソース データをダウンロード可能なファイル形式にエクスポートするための機能があります。更新機能を使用すると、見たい瞬間のデータを取得できます。

Horizon Pros Desk

Horizon Pros Desk には、専用の Horizon デリバリ エキスパートのチーム、Horizon Pros が配属されています。Horizon Pros は次のサービスを提供します。

- 年中無休のサポート
- 専用 VDI の専門知識
- Day 0 から Day 2 の最適化を含む完全なライフサイクル サポート、および標準アーキテクチャ、ベスト プラクティスなどのガイダンス。
- Horizon のデプロイ タイプ全体にわたる、エキスパートによるガイダンス

注： Horizon Pros Desk の機能は、Microsoft Azure デプロイとオンプレミス デプロイの両方に対して提供されます。

クラウド デプロイのための VMware の 24 時間サポートについては、vmware.com サイトの『VMware Production Support for Cloud Products PDF』を参照してください。

詳しい情報

上記の機能の詳細については、次のリンクを使用してください。

Horizon Accelerator - 運用に関するインサイト

このドキュメント ページでは、Horizon Cloud Service - next-gen 環境のために使用されるプロバイダ リソースの運用に関するインサイトを提供する Horizon Accelerator Control Center の機能について説明します。

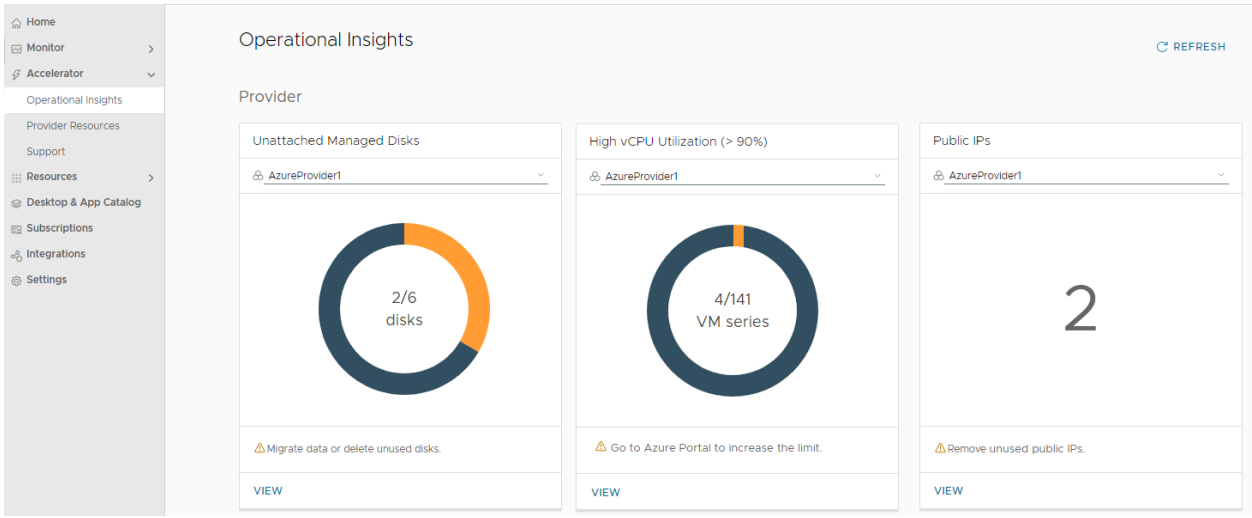
この機能は、Horizon Accelerator アドオン ライセンスがある場合に Horizon Universal Console で使用できます。

現在、この機能は Microsoft Azure キャパシティ プロバイダで使用できます。

概要

[運用に関するインサイト] ビューには、運用コストを削減するために調整できる、プロバイダ内のリソースに対する実行可能なインサイトと画面上のガイダンスが表示されます。

次のスクリーンショットは、[Accelerator] - [運用に関するインサイト] のユーザー インターフェイスの場所を示しています。このスクリーンショットは、Microsoft Azure プロバイダが各ゲージに対して選択された場合のこのビューも示しています。



各リソース関連の領域には、存在する可能性のある問題が強調表示され、最適化の機会が示されます。

各ドリルダウン ビューでは、プロバイダ リソースの詳細を確認し、問題を修正するためのガイダンスを参照できます。

リソース インサイト - Microsoft Azure プロバイダ

現在のリリースでは、[運用に関するインサイト] には、次世代環境で構成された Microsoft Azure プロバイダから使用される次のリソースのインサイトが提供されます。

表示されるゲージはそれぞれ、ゲージの上部で選択された特定のリソース プロバイダと特定のリソース タイプに対応するデータを提供します。

ヒント: Microsoft Azure の場合、プロバイダは Azure サブスクリプションに基づいています。表示されるデータは、選択したプロバイダに関連付けられているサブスクリプションにあるリソースに固有です。

ゲージおよび詳細ビューごとに、システムは Azure API がその特定のリソース タイプに対して提供する特性に応じて情報を取得します。

未接続の管理対象ディスク

このゲージは、選択したプロバイダに存在する未接続の管理対象ディスクの数に関するインサイトを提供します。

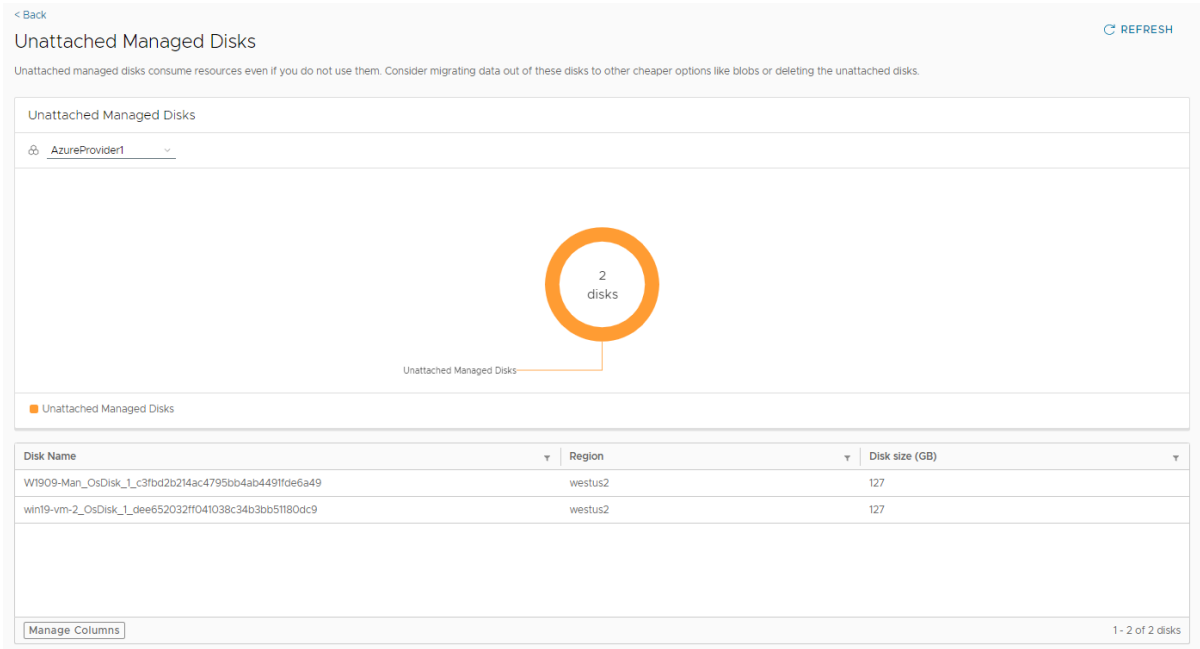
ゲージは、選択したプロバイダ内の管理対象ディスクの全体的なリストを反映し、それらのディスクのどのサブセットが仮想マシンに接続され、どのサブセットが仮想マシンに接続されていない（未接続のディスク）かを示します。

Microsoft Azure のドキュメントで説明されているように、Azure 管理対象ディスクは、Azure 仮想マシンで使用するように設計された高性能ストレージです。

Azure サブスクリプションでは管理対象ディスクごとにコストが発生するため、未接続のディスクの存在は実用的なインサイトになります。

- [推奨される解決策] - 未接続の管理対象ディスクは、ディスクが使用されていない場合でもリソースを消費します。これらの未接続のディスクから必要なディスク上のデータを BLOB ファイルなどのより低コストのオプションに移行することを検討してください。データの移行が完了したら、使用されていないディスクを削除します。
- [表示] - 未接続の管理対象ディスクのリストを名前、リージョン、ディスク サイズ別に表示します。

次のスクリーンショットは、ドリルダウン ビューを示しています。



Azure vCPU 使用率が高い (> 90%)

このゲージは、プロバイダのコンピューティング割り当ての増加が必要になる可能性のある仮想マシン シリーズについてのインサイトを提供します。

ゲージは、選択したプロバイダの Azure コンピューティング割り当ての現在の使用率と、どの仮想マシン シリーズの vCPU 使用率が 90% 以上であるかを反映します。

90% を超える使用率は実行可能なインサイトとなり、指定された Azure リージョンでその仮想マシン シリーズの追加割り当てをリクエストして、必要が生じる前にプロバイダに割り当てが確実に存在するように対処することにつながります。

- [推奨される解決策] - vCPU 使用率が 90% 以上の仮想マシン シリーズについて、割り当てを増やすことを検討します。仮想マシン シリーズの割り当ての増加は、[割り当て] ブレードを使用して Azure ポータルで行われ、[コンピューティング] および関連する Azure リージョンでフィルタリングされます。
- [表示] - vCPU 使用率が 90% 以上の Azure 仮想マシン シリーズの一覧を表示します。この表示から、割り当ての増加を要求する特定の仮想マシン シリーズを決定できます。

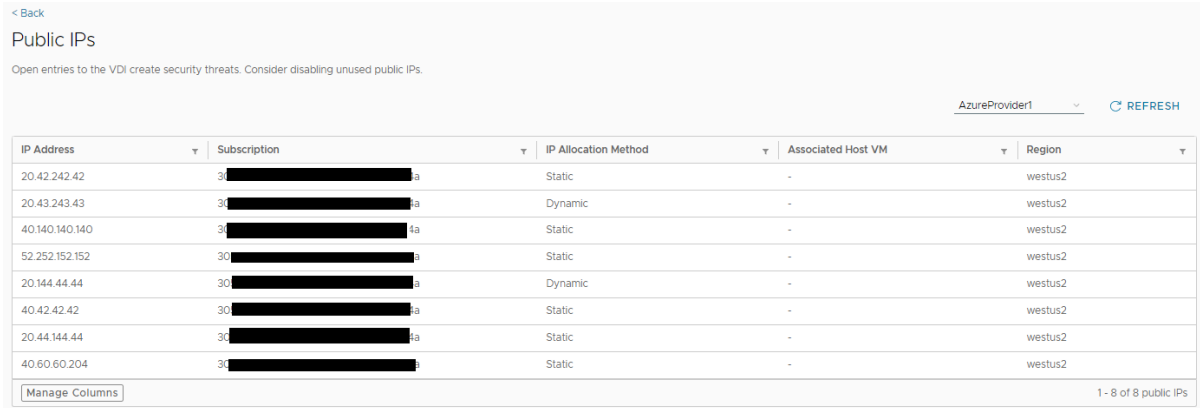
パブリック IP アドレス

セキュリティの観点から見ると、外部から仮想デスクトップ インフラストラクチャ (VDI) へのオープン エントリの数を制限することがベスト プラクティスです。

VDI の Unified Access Gateway インスタンスと Horizon Edge Gateway インスタンスにはパブリック IP アドレスが必要ですが、この運用に関するインサイトにより、プロバイダのネットワークで有効になっている他のすべてのパブリック IP アドレスが検出され、レビュー用のリストが提供されます。

- [推奨される解決策] - 不要なパブリック IP アドレスまたは未使用のパブリック IP アドレスを確認して無効にします。
- [表示] - パブリック IP アドレスのリストと、IP アドレスや関連する仮想マシンなどの関連情報を表示します。

次のスクリーンショットは、ドリルダウン ビューを示しています。プライバシーのため、一部の値はマスキング処理されています。



UI アクション - フィルタ、列の管理、更新

各セクションでは、これらの標準アクションについて説明します。

フィルタ

各列見出しには、フィルタリング アイコンが表示されます。

更新

ゲージ ビューから詳細ビューにドリルダウンすると、システムは選択したリソース プロバイダからデータを取得して、そのデータを表示します。表示されるデータは最新のデータです。

しばらくの間データを表示していて、最新のデータの取得を希望する場合は、[更新] をクリックして、最新のデータが表示されるようにします。

列の管理

この機能を使用して、列の表示と非表示を切り替えます。

Horizon Accelerator - プロバイダ リソース

このドキュメント ページでは、Horizon Cloud Service - next-gen 環境で使用されるプロバイダ リソースを表示するための Horizon Accelerator Control Center 機能について説明します。

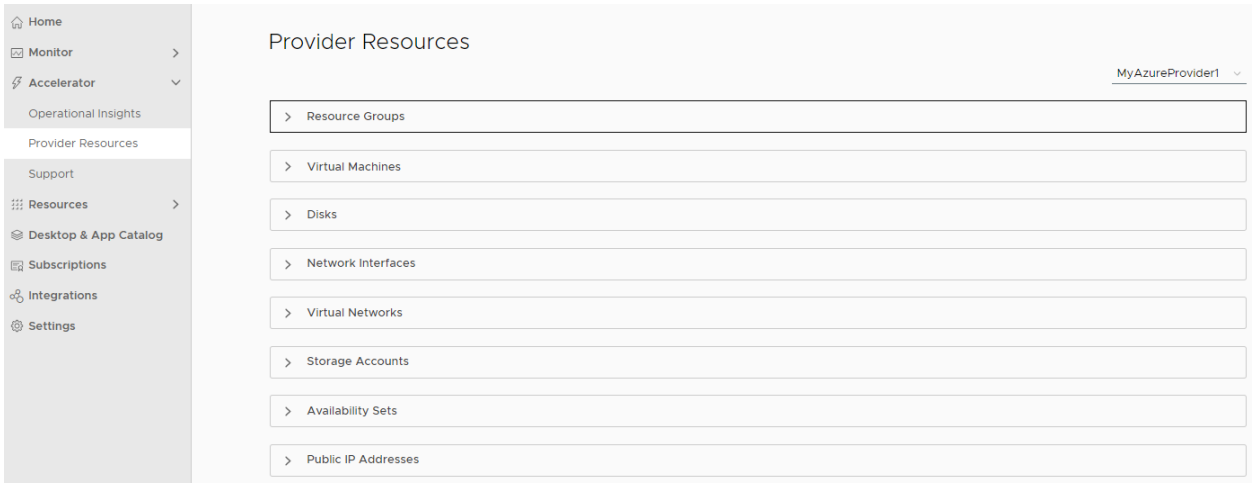
この機能は、Horizon Accelerator アドオン ライセンスがある場合に Horizon Universal Console で使用できます。

現在、この機能は Microsoft Azure キャパシティ プロバイダで使用できます。

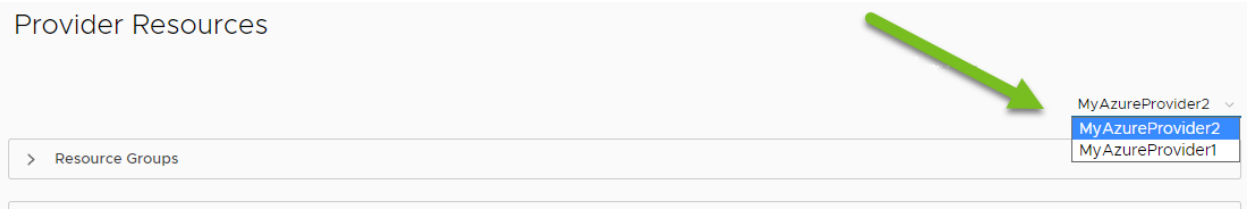
概要

Horizon Accelerator Control Center を使用すると、次世代環境で使用されるプロバイダ リソースを可視化すると同時に、各プロバイダのユーザー インターフェイスまたはポータルにログインして各リソースを確認する必要がなくなります。

次のスクリーンショットは、コンソール内のこの [プロバイダ リソース] ビューの場所（[Accelerator] - [プロバイダ リソース]）および Microsoft Azure プロバイダに対するこのビューの表示方法を示しています。



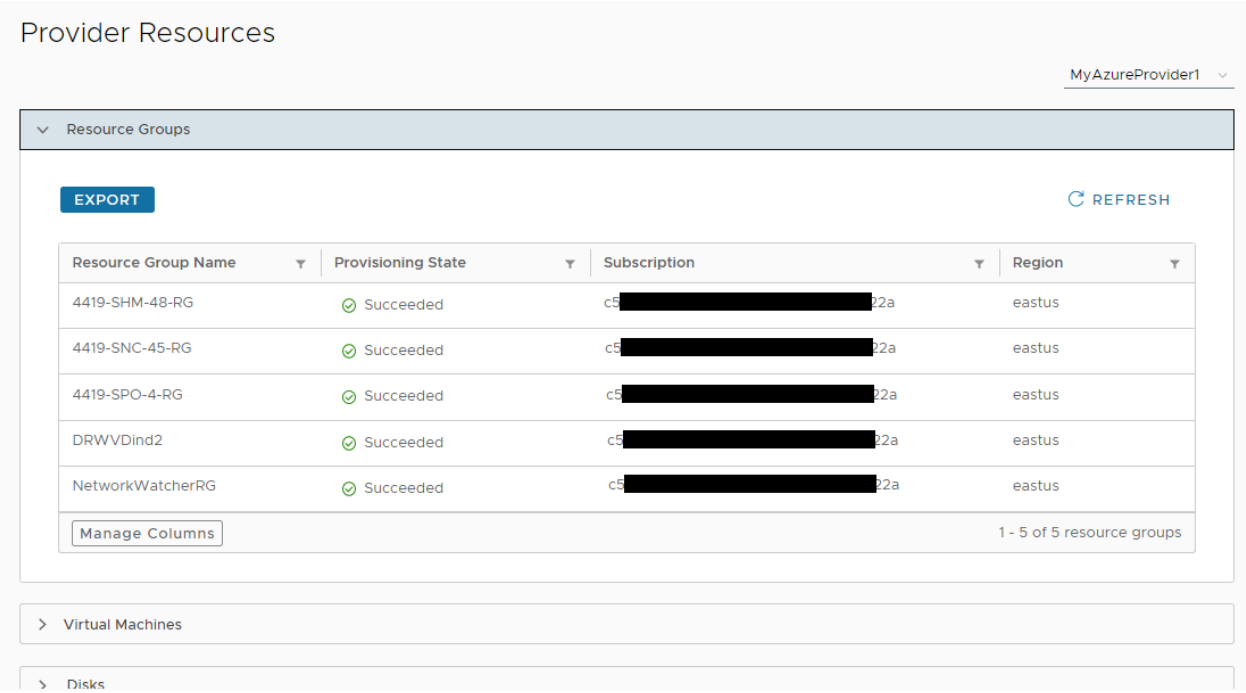
このビューの右上にあるプロバイダ選択リストには、次世代環境で構成された各プロバイダが反映されます。このリストを使用すると、特定のプロバイダのリソースを簡単に選択して表示できます。



各リソース タイプに関する情報を表示するには、そのセクションを展開します。

セクションを展開すると、システムはデータを取得して、最新情報が表示されます。

次のスクリーンショットは、展開されたセクションの例を示しています。サブスクリプション情報は、プライバシーに配慮してマスキング処理されています。



Microsoft Azure プロバイダ - リソース タイプ

現在のリリースでは、[プロバイダ リソース] ビューには、次世代環境で構成された Microsoft Azure プロバイダから使用される次のリソースのデータが表示されます。

これらのリソース タイプごとに、ユーザー インターフェイスでカテゴリを展開すると、システムは Azure API を呼び出して、Microsoft Azure とリソースが存在するサブスクリプションから最新情報のデータを取得します。

表示されるリソース タイプごとに、システムは [プロバイダ リソース] ビューの右上のリストで選択された特定のリソース プロバイダに対応するデータを提供します。

ヒント: Microsoft Azure の場合、プロバイダは Azure サブスクリプションに基づいています。表示されるデータは、右上の選択リストで選択したプロバイダに関連付けられているサブスクリプションにあるリソースに固有です。

リソース タイプごとに、システムは Azure API がその特定のリソース タイプに対して提供する特性に応じて情報を取得します。たとえば、Azure はリソース グループにプロビジョニング状態の特性を提供しますが、Azure はその特性をネットワーク インターフェイスには提供しません。

その結果、各リソース タイプのユーザー インターフェイス セクションには、Azure へのシステムの API 呼び出しがそのリソース タイプに対して返す内容に基づく列とフィルタが含まれています。

表示される列は、Azure がリソース タイプに関連付ける特性です。

Azure が特定の特性の特定の値を定義してサポートしている場合は、列見出しのフィルタ アイコンを使用して、これらの既知の値をフィルタリングできます。

注： 状態関連の特性の場合、これらの列に表示される値は、Azure がシステムの API 呼び出しに返す値に基づいています。Azure のドキュメントでは、これらの値をサービスでサポートされている既知の値として参照しています。時間の経過とともに、Azure は新しい既知の値を追加したり、既知の値に使用する特定の名前を更新したりすることがあります。次のリストに示す状態関連の値は、本書の執筆時点のものです。

リソース グループ

そのプロバイダ内のリソース グループを一覧表示し、Azure リージョンなどの各リソースに関する情報を表示します。[プロビジョニング状態] 列は、各リソース グループのデプロイ ステータスを示します。

- [リソース グループ名] - リソース グループの名前。
- [プロビジョニング状態] - この状態に関連する特性について、Azure は **成功**、**失敗**、**削除**、**更新** の値を報告します。
- [サブスクリプション ID] - 関連付けられた Azure サブスクリプションの ID。
- [リージョン] - リソースが存在する Azure リージョンの名前。

仮想マシン

そのプロバイダ内の仮想マシンを一覧表示し、NIC や IP アドレスなどの各仮想マシンに関する情報を表示します。

- [仮想マシン名] - 仮想マシン (VM) の名前。
- [サブスクリプション ID] - 関連付けられた Azure サブスクリプションの ID。
- [リソース グループ] - リソース グループの名前。
- [ネットワーク インターフェイス名] - 仮想マシンに接続されているネットワーク インターフェイス (NIC) の名前。
- [仮想ネットワーク名] - NIC に接続されている VNet の名前。
- [IP アドレス] - NIC に設定されている IP アドレス。
- [仮想マシンのサイズ] - 仮想マシンに使用される Azure 仮想マシン モデル。

ディスク

そのプロバイダ内のディスクを一覧表示し、ディスクの状態やディスク サイズなどの各ディスクに関する情報を表示します。

- [ディスク名] - ディスクの名前。
- [ディスクの状態] - この状態に関連する特性では、Azure は、**未接続**、**接続済み**、**アクティブな SAS**、**アクティブな SAS 凍結**、**凍結**、**アクティブ アップロード**、**アップロードの準備完了**、**予約済み** の値を報告します。

  これらの Azure のすべての既知の値の正確な定義については、Azure ドキュメントの ディスクの状態タイプ ページを参照してください。

次世代環境で通常表示されるディスクの状態は、**接続済み**、**予約済み**、**未接続** です。接続済みディスクは、実行中の仮想マシンに接続されます。予約済みディスクは、停止し割り当て解除された仮想マシンに接続されます。未接続のディスクはどの仮想マシンでも使用されていません。

- [サブスクリプション ID] - 関連付けられた Azure サブスクリプションの ID。
- [リソース グループ] - リソース グループの名前。
- [リージョン] - リソースが存在する Azure リージョンの名前。
- [ディスク サイズ (GB)] - ディスクのサイズ。

注： Azure ドキュメントで説明されているように、未接続のディスク状態は、そのサブスクリプション内でディスクが使用されていることを意味します。つまり、ディスクは以前にデスクトップに接続されていましたが、デスクトップが削除されても、ディスクは Azure 側に残っています。

ヒント: フローティング デスクトップ プールがある場合、この [ディスク] ビューにそのプールのリソース グループに対して複数の「**未接続**」ディスクが一覧表示される場合は、Microsoft Azure のコストを回避するために、これらの未接続のディスクを削除することがベスト プラクティスです。未接続の状態は通常、ディスクが使用されていないことを示し、削除されたフローティング デスクトップから実体なしになっている可能性があります。

ネットワーク インターフェイス

そのプロバイダ内のネットワーク インターフェイスを一覧表示し、それぞれのネットワーク インターフェイスに関する情報（存在するリソース グループなど）を表示します。

- [ネットワーク インターフェイス名] - ネットワーク インターフェイス (NIC) の名前。
- [サブスクリプション ID] - 関連付けられた Azure サブスクリプションの ID。
- [リソース グループ名] - リソース グループの名前。
- [リージョン] - リソースが存在する Azure リージョンの名前。

仮想ネットワーク

そのプロバイダ内の仮想ネットワーク (VNet) を一覧表示し、ピアリングステータスなどの各仮想ネットワークに関する情報を表示します。このビューには、VNet ごとに定義されたアドレス プリフィックスが一覧表示されます。

- [仮想ネットワーク名] - VNet の名前。
- [プロビジョニング状態] - この状態に関連する特性について、Azure は **成功**、**失敗**、**削除**、**更新** の値を報告します。
- [サブスクリプション ID] - 関連付けられた Azure サブスクリプションの ID。
- [リソース グループ名] - リソース グループの名前。
- [アドレス プリフィックス] - その VNet 内のアドレス プリフィックス。
- [ピアリングの状態] - この状態に関連する特性について、Azure は **接続済み**、**切断済み**、**開始済み** の値を報告します。

ストレージ アカウント

そのプロバイダ内のストレージ アカウントを一覧表示し、それぞれのストレージ アカウントに関する情報（存在するリソース グループなど）を表示します。

- [ストレージ アカウント名] - ストレージ アカウントの名前。
- [サブスクリプション ID] - 関連付けられた Azure サブスクリプションの ID。
- [リソース グループ名] - リソース グループの名前。
- [リージョン] - リソースが存在する Azure リージョンの名前。

可用性セット

そのプロバイダの可用性セットを一覧表示し、それぞれの可用性セットに関する情報（存在するリソース グループなど）を表示します。

- [可用性セット] - 可用性セットの名前。
- [サブスクリプション ID] - 関連付けられた Azure サブスクリプションの ID。
- [リソース グループ名] - リソース グループの名前。

パブリック IP アドレス

そのプロバイダのパブリック IP アドレスを一覧表示し、割り当て方法（静的、動的）など、各パブリック IP アドレスに関する情報を表示します。

- [パブリック IP アドレス名] - パブリック IP アドレスの名前。
- [プロビジョニング状態] - この状態に関連する特性について、Azure は 成功、失敗、削除、更新 の値を報告します。
- [パブリック IP アドレス] - このパブリック IP アドレスの IP アドレス。
- [パブリック IP バージョン] - IPv4 または IPv6。
- [IP 割り当て方法] - Azure は、動的 または 静的 の値を返します。
- [アイドル タイムアウト (分)] - パブリック IP アドレスのタイムアウト値。
- [サブスクリプション ID] - 関連付けられた Azure サブスクリプションの ID。
- [リージョン] - リソースが存在する Azure リージョンの名前。

UI アクション - フィルタ、列の管理、更新、およびエクスポート

各セクションでは、これらの標準アクションについて説明します。

フィルタ

各列見出しには、フィルタリング アイコンが表示されます。列にフィルタを設定してからデータをエクスポートすると、フィルタリングされたデータのみが CSV ファイルにエクスポートされます。

列の管理

この機能を使用して、列の表示と非表示を切り替えます。

更新

セクションを展開すると、システムはリソース プロバイダからデータを取得して、そのデータを表示します。セクションを展開したときに表示されるデータは、右上隅のリストで選択されたプロバイダにある、そのリソースに関する最新のデータです。

各セクション内で、しばらくの間データを表示していて、最新のデータを取得する場合は、そのセクションで [更新] をクリックして、そのセクションに最新のデータを入力します。

エクスポート

各セクション内には、データを CSV 形式でエクスポートし、コンソールの [ダウンロード] ページで CSV ファイルを使用できるようにするための [エクスポート] ボタンがあります。

列フィルタを設定している場合は、それらのフィルタがエクスポートされたデータに適用されます。

[エクスポート] をクリックすると、ダイアログ ボックスが表示され、ファイル名をカスタマイズするためのフィールドが表示されます。新しい名前を入力するか、表示されるデフォルト値を受け入れます。

準備ができたら、コンソールの [ダウンロード] ページ（[監視] - [ダウンロード]）からファイルをダウンロードできます。

注： デフォルトでは、[ダウンロード] ページのファイルの有効期限は 30 日間です。30 日後、ファイルはシステムから削除されます。

Horizon Accelerator - Horizon Pros - 専用サポート

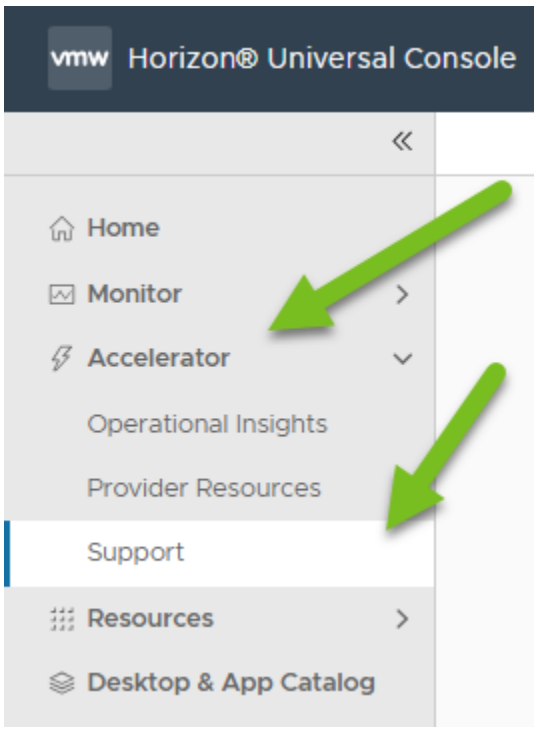
Horizon Accelerator サポート チームは、Horizon Cloud Service - next-gen 環境での Day 0 から Day 2 にわたる、専用の継続的なサポートを提供します。

注： Horizon Pros チームは、VMware Horizon Accelerator サポート チームとも呼ばれます。このチーム名は、E メールやその他の連絡方法において、`VHA Accelerator` サポート と省略された表記になっている場合があります。

この機能は、Horizon Accelerator アドオン ライセンスがある場合に Horizon Universal Console で使用できます。

仕組み

サポート チームにサポートを依頼するには、[Accelerator] - [サポート] をクリックします。

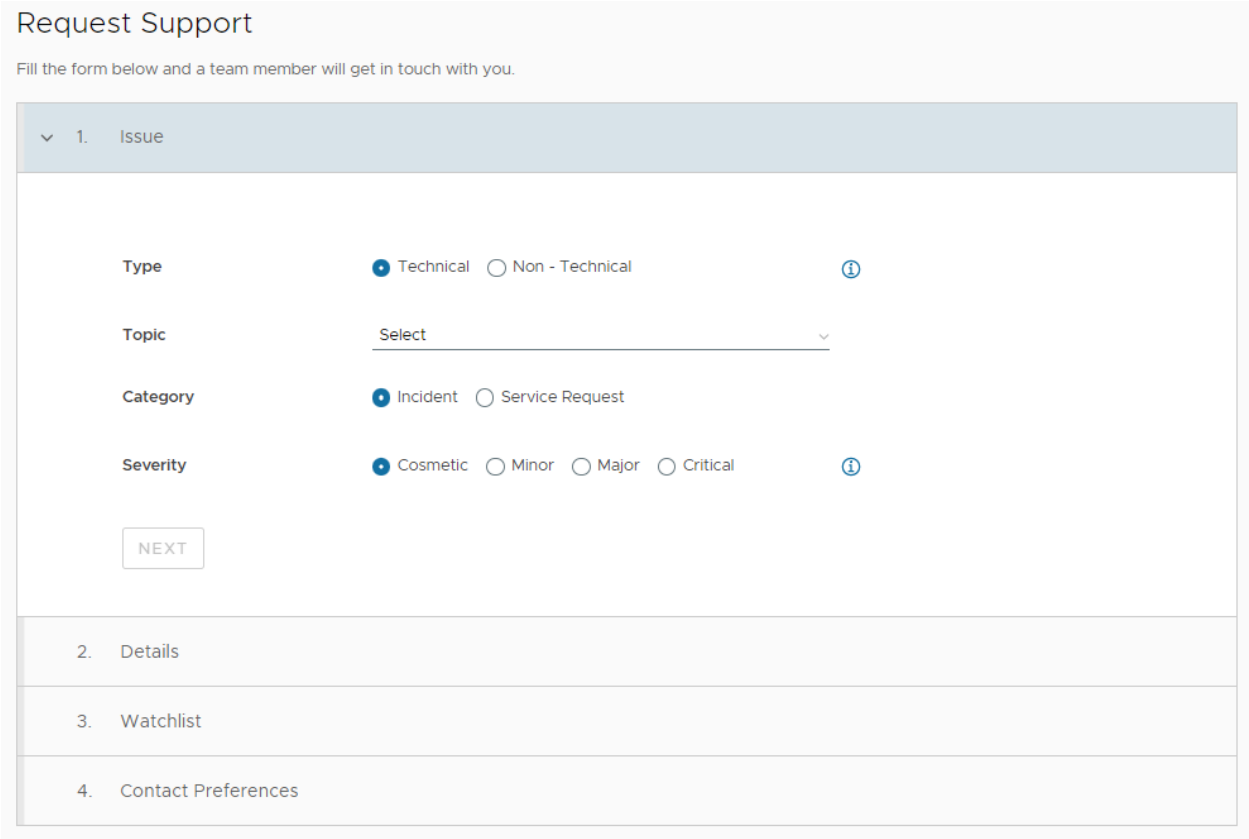


ウィザードが完了すると、サポート エージェントの 1 つがアラートを受け取り、リクエストについてユーザーに連絡します。

サポートに連絡

[Accelerator] - [サポート] をクリックすると、コンソールで [サポートに連絡] ウィザードが起動します。

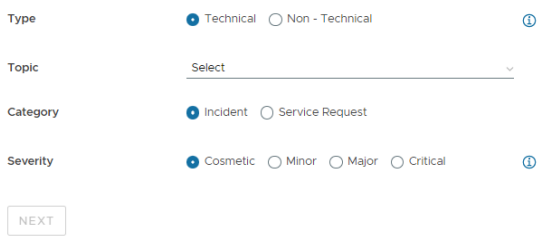
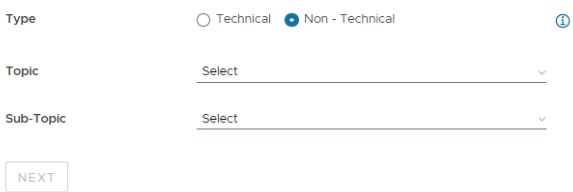
次のスクリーンショットは、ウィザードの最初の表示を示しています。



このウィザード内で、リクエストしているサポートのタイプに適した選択を行います。以降のセクションでは、各手順について説明します。

手順 1 - サポート タイプ

最初に、リクエストのタイプが技術的なものかどうかを決めます。技術的なリクエストには、問題カテゴリと重要度タグが関連付けられます。

技術的なタイプ	技術的でないタイプ
	

タイプを選択したら、ユーザー インターフェイスに従ってリクエストを最も当てはまるトピック領域にさらに関連付けます。（トピック領域については、正解も不正解もありません。）

システム定義リストからトピック領域を選択します。システム定義リストには、リクエストがリスト内の残りのどのトピックにも当てはまらない場合のために、**その他** というトピック領域が含まれています。

コンソールは動的であり、現時点でシステムで使用可能な選択肢が一覧表示されるため、このドキュメントにはトピックまたはサブトピック リストが列挙されません。このドキュメントで列挙しようとすると、ここのドキュメントはすぐに古くなってしまいます。列挙リストの代わりに、次にいくつかの例を示します。

- 技術的なリクエストの場合、トピック領域には、**接続**、`Edge` **デプロイ**、**メンテナンス**、および同様の技術的な機能に関連する概念など、技術的な機能に関連する領域が含まれます。
- 技術的でないリクエストの場合、トピック領域には、**エンタイトルメント** **アカウント**、**ユーザーと権限**、および同様のビジネス指向の概念など、ビジネス指向およびライセンス関連の領域が含まれます。技術的でないリクエストの場合は、選択したトピックのサブトピック領域を含めることができます。

[技術的] タイプには、次の問題カテゴリを選択します。

インシデント

実行中のサービスの破損、遅延やパフォーマンスの問題、およびそれらに類似した問題が発生しています。

インシデントには重要度タグが付けられます。重要度は高い順に [重大]、[メジャー]、[マイナー]、[コズメティック] になります。各重要度には、VMware Horizon Accelerator サポート ターゲットの初期応答時間が関連付けられています。

次の表に、重要度を選択する際の一般的なガイダンスを示します。

重要度	**説明**	**Horizon Accelerator ターゲットの初期応答時間**
[重要]	この問題により、手続き上の回避策なしで業務が停止しました。	30 分以内
[メジャー]	この問題は、業務の一部に大きな影響を与えています。	4 営業時間以内
[マイナー]	この問題は、部分的で重大度の低いサービス損失を引き起こしていますが、業務への影響は大きくありません。	8 営業時間以内
[コズメティック]	この問題は、アプリケーションの外観に関連しています。	12 営業時間以内

注： 本書の執筆時点では、表に記載されている時刻は、VMware Horizon Accelerator サポート チームが目標とする最新の時間です。実際に直面した時間について質問がある場合は、[サポートに連絡] ウィザードを使用できます。

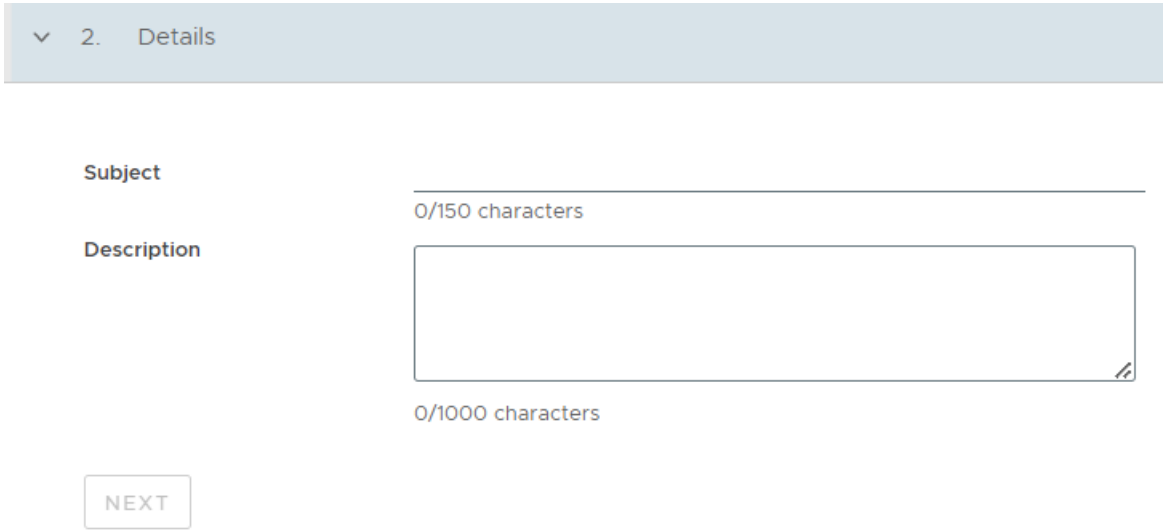
サービス リクエスト

情報をリクエストするか、専用サポート チームにタスクの実行をリクエストします。

ユーザー インターフェイスで [次へ] ボタンが使用可能になるまで、ユーザー インターフェイスの選択を続行します。[次へ] をクリックして選択内容を保存し、次の手順に進みます。

手順 2 - 詳細

この手順は次のように開始します。

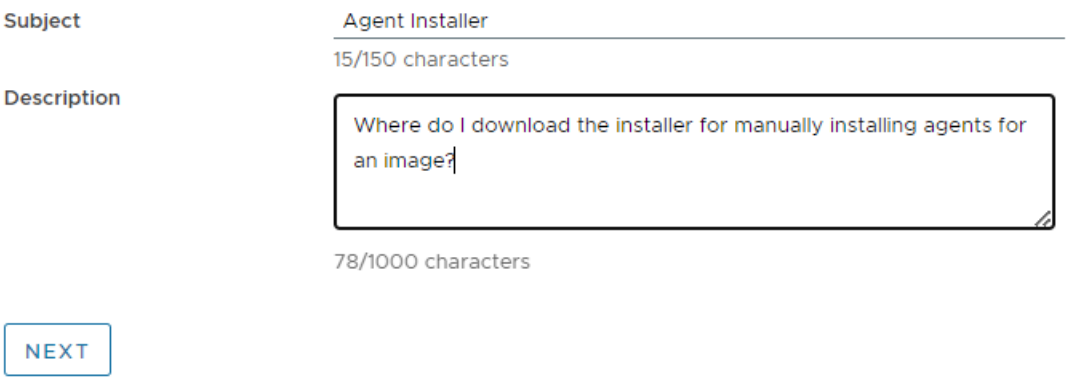


[件名] フィールドを使用して、問題の簡単な説明またはこのサポート リクエストの理由を入力します。

サポートが必要な理由の説明が長い場合は、大きいフィールドを使用します。

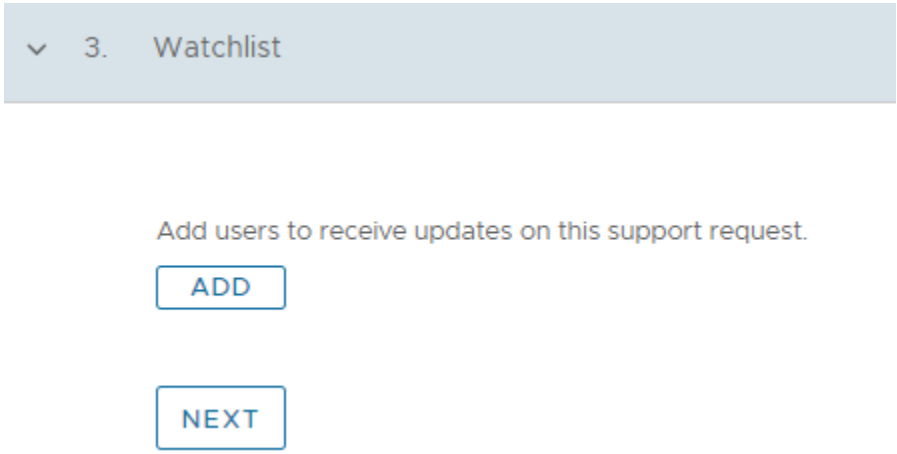
コンソールで [次へ] が使用可能になったら、[次へ] をクリックして次の手順に進みます。

スクリーンショットの例：



手順 3 - ウォッチリスト

この手順は次のように開始します。



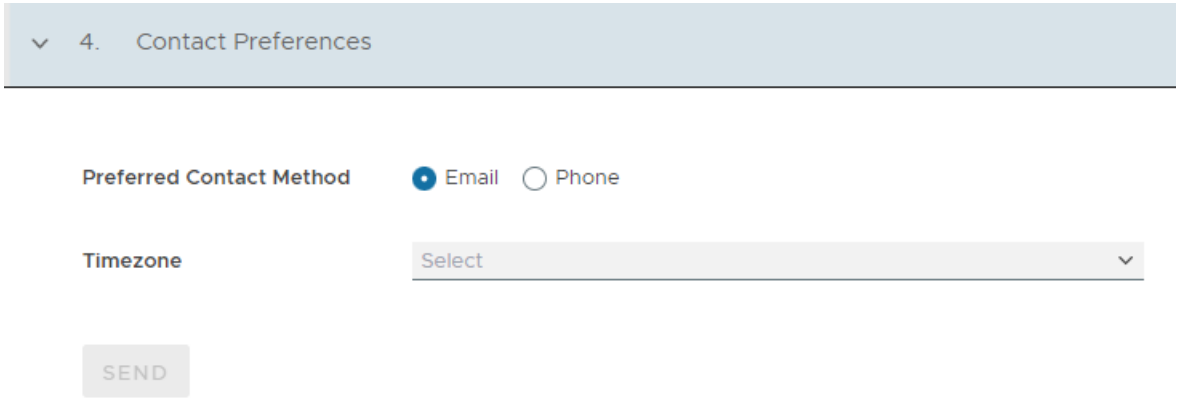
[追加] ボタンを使用して、このリクエストに関する更新情報を送信するユーザーのメール アドレスを指定します。名前を追加するには、もう一度 [追加] をクリックします。

注： デフォルトでは、リクエストの送信者のメール アドレス（お使いのメール アドレス）が自動的に含まれます。システムは、Horizon Universal Console へのログインに使用したログインに関連付けられた E メールを使用します。

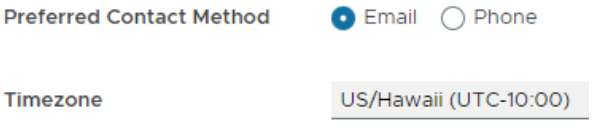
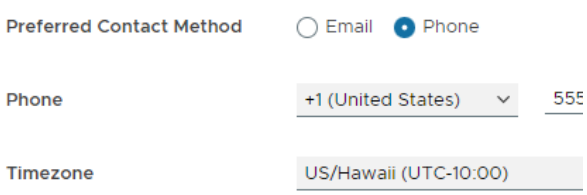
コンソールで [次へ] が利用可能になり、ウォッチリストにユーザーを追加したら、 [次へ] をクリックして次の手順に進みます。

手順 4 - 連絡先の設定

この手順は次のように開始します。



割り当てられたサポート エージェントがこのリクエストに関する連絡のために使用する方法を指定します。[電話] を選択する場合は連絡先の電話番号を入力します。

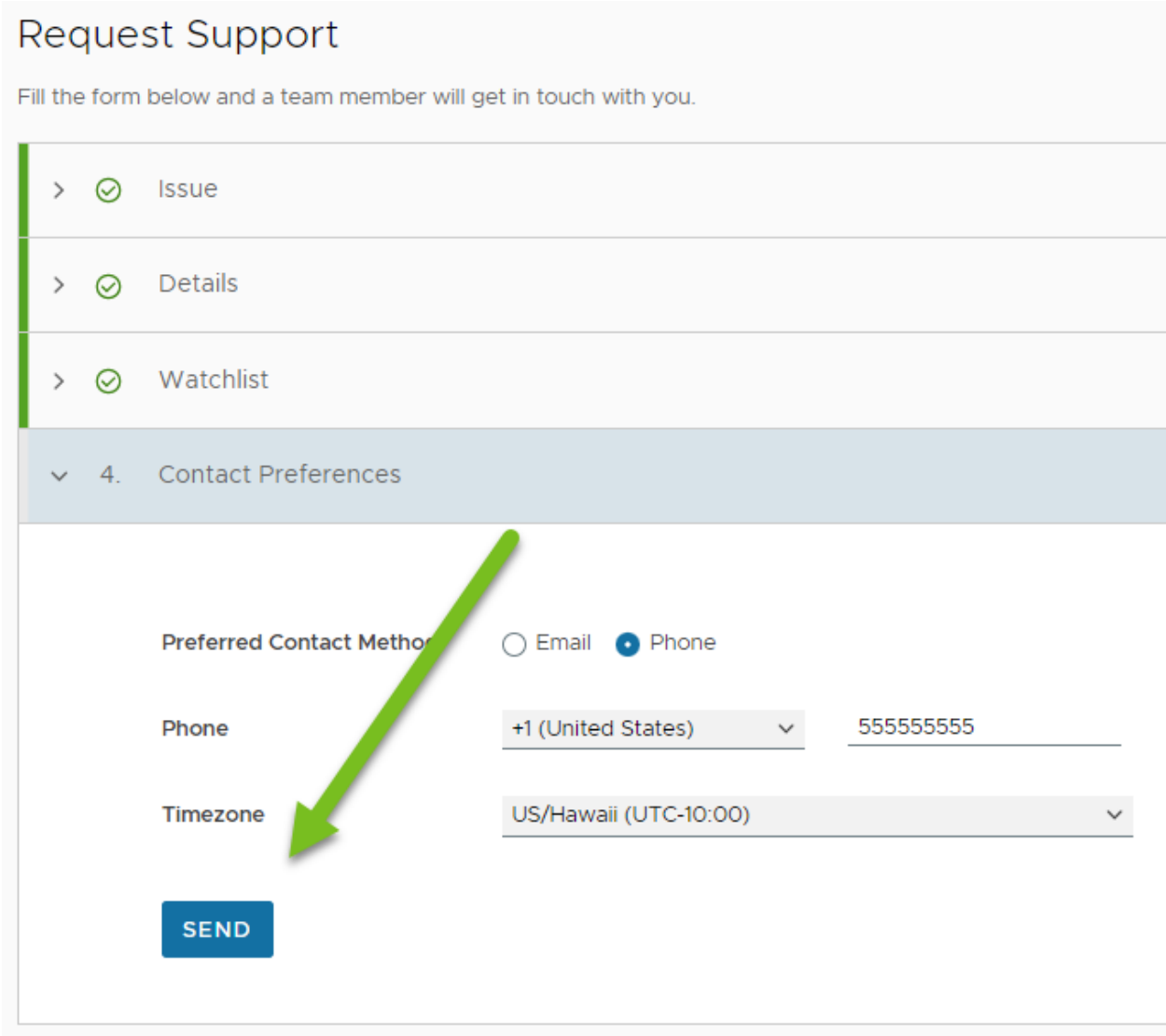
E メールによる連絡方法	電話による連絡方法
	

サポート チームの目標の 1 つは、営業時間内にサポートを提供することです。この目標を達成するために、サポート エージェントは選択したタイム ゾーンでの一般的な営業時間を推測します。このタイム ゾーンの選択は、サポート チームとお客様のチーム間のより効率的なコミュニケーションを促進するのに役立ちます。

コンソールで [送信] が使用可能になったら、[送信] をクリックしてサポート リクエストを発行できます。

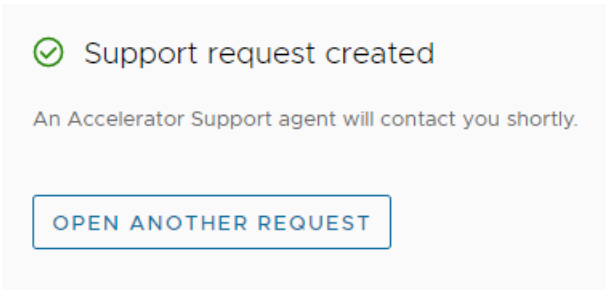
リクエストの送信

ユーザー インターフェイスで手順が完了し、リクエストを発行する準備ができたら、[送信] をクリックします。



[送信] をクリックすると、サポート リクエストがサポート チームに転送されます。

コンソールに確認メッセージが表示され、リクエストが作成されてサポート パイプラインに入っていることが通知されます。



次の処理

システムは、VMware Horizon Accelerator サポート チームにサポート リクエストを通知します。

同時に、システムはお使いのメール アドレスと、[ウォッチリスト] の手順で入力したアドレスを CC に指定して、VMware Horizon Accelerator サポート チームのアドレスに E メールを送信します。

発行されたサポート リクエストのシステム通知を受け取り次第、チームはすぐに連絡をしてリクエストへの対応を開始します。

最初に表示される通知は、[宛先] 行に VHA Accelerator サポート チームのアドレス、および [CC] 行にお使いのメール アドレスと [ウォッチリスト] の手順で入力した E メールが指定された確認メールです。

注： この確認 E メールが 15 分以内に届かない場合は、リクエストを再度発行できます。

E メールの送信者は、Horizon Cloud サポート チーム（送信者のアドレス：`do-not-reply-horizon@vmware.com`）になります。

E メールの件名の行には、作成されたサポート チケットの文字列が含まれ、本文にはウィザードで選択および入力した情報が含まれます。

Horizon 制御プレーンおよび Horizon Cloud Service - next-gen でのアセットおよびアップグレードの管理と監視

6

Horizon 制御プレーンと Horizon Cloud Service - next-gen 管理コンソールを使用して、イメージ、プール、デスクトップとアプリケーション、ロール、ライセンスを管理します。また、コンソールを使用して、リソースとメトリックの監視、ログの生成と表示、パッチおよび製品アップグレードのインストールを行います。

次のトピックを参照してください。

- Horizon Universal Console を使用した環境の管理
- Horizon Cloud Service - next-gen 環境の監視
- Horizon Agent ソフトウェアの管理
- Horizon Cloud Service - next-gen での Horizon Edge のメンテナンスと更新

Horizon Universal Console を使用した環境の管理

Horizon Universal Console を使用して、次世代 Horizon 制御プレーン 環境のユーザー イメージ、プールとプール グループ、デスクトップとアプリケーション、ロール、ライセンスを管理します。

最初のデプロイと構成が完了したら、Horizon Universal Console を使用して継続的に管理を行います。詳細については、以下のリンクされたページを参照してください。

- イメージ管理 - 次世代 Horizon 制御プレーン を使用した Horizon イメージの管理
- プールおよびプール グループの管理 - プール プロビジョニングの管理
- ユーザー資格 - エンド ユーザーへのデスクトップおよびアプリケーションの資格の付与
- ロールの管理 - Horizon Universal Console ユーザーへの管理ロールの割り当て
- ライセンス - Horizon Universal Console を使用した Horizon ライセンスの追跡

Horizon Cloud Service - next-gen の通知

Horizon Cloud Service - next-gen は、重要なイベントが発生したときに通知を使用して知らせます。

通知の表示

注：

- このトピックでは、Horizon Universal Console を使用して Horizon Cloud 通知を確認する方法について説明します。また、Cloud Services コンソール(Cloud Services エンゲージメント プラットフォームとも呼ばれる)を使用して通知を確認することもできます。ただし、通知に対して操作を実行する場合は、Horizon Universal Console を使用します。
- ページの右上隅にあるベル () アイコンから [すべての通知を表示] をクリックすると、Cloud Services コンソールの [自分の通知] にリダイレクトされます。

  [自分の通知] ページには、他のサービスから生成された通知を含むすべての通知が表示されます。

  Horizon Cloud 通知のみを表示するには、[Horizon Cloud 通知の表示] をクリックして、Horizon Universal Console の [通知] ページに移動します。

[通知] ページには、次のオプションがあります。

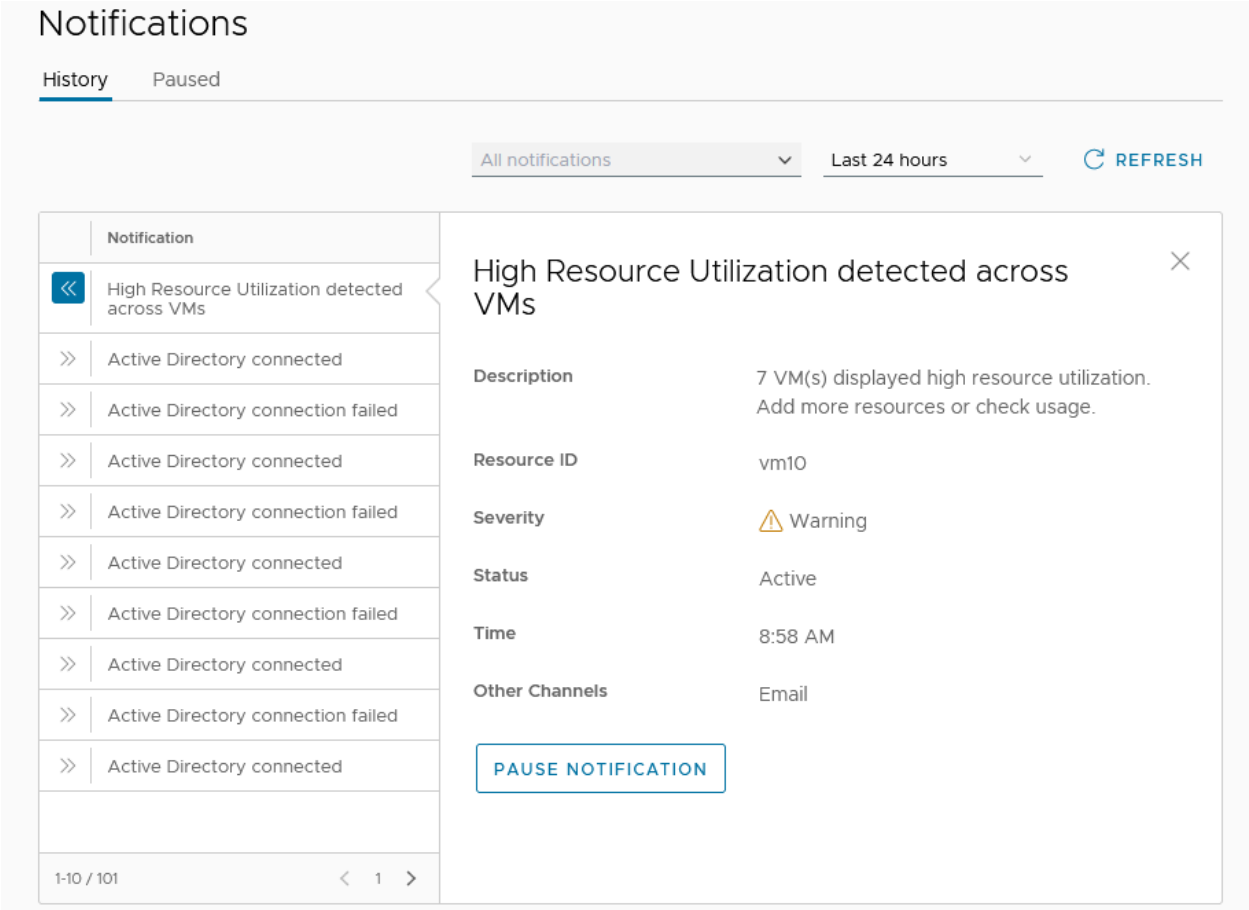
- [履歴] タブには、通知フィルタに基づく通知のリストが表示されます。フィルタ設定は、通知リストの上にあります。通知は、タイプと期間 (最大 90 日) でフィルタリングできます。

  通知の詳細を表示するには、その通知の左二重矢印アイコンをクリックします。通知の詳細ペインには、次の情報が適用されます。

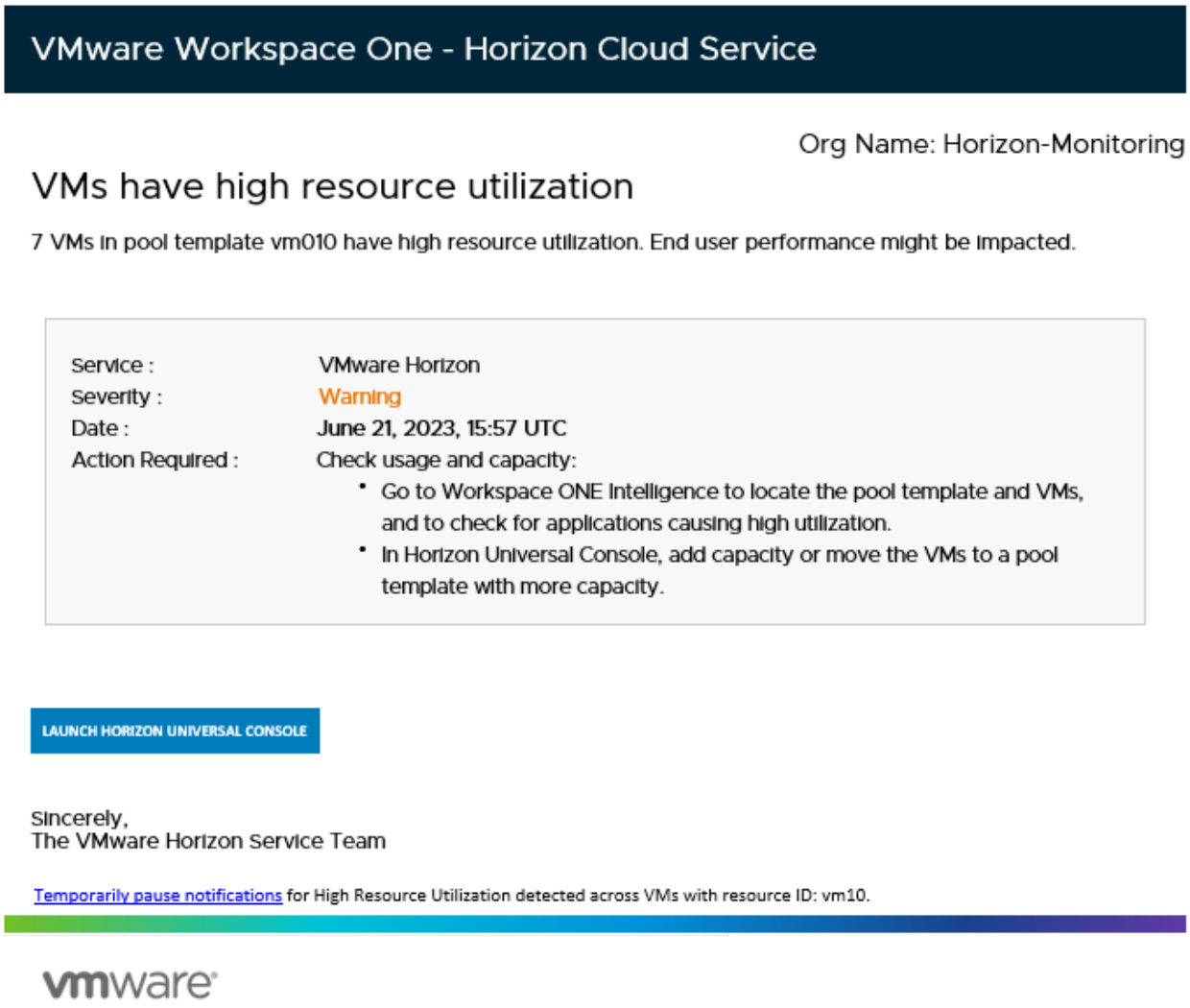
  - 詳細には、[説明]、[リソース ID]、[重要度]、[ステータス]、[時刻]、[その他のチャネル]（現在は E メール通知）が含まれます。
  - 次のステータスが適用されます。

通知タイプ	説明
有効	管理者がまだ対処していない通知
破棄されました	管理者が特に注意する必要がないと判断した通知

頻度の高い特定のタイプの通知（「仮想マシン全体で高いリソース使用率が検出されました」など）については、[通知を一時停止] オプションを使用できます。このオプションを使用すると、その通知タイプをすべてのチャネルで最大 72 時間一時停止できます。[通知を一時停止] オプションを使用することで、繰り返し警告を表示せずに、原因に対処できます。



これらの通知タイプでは、次の E メール メッセージのスクリーンショットに示すように、電子メール メッセージが送信されます。



これらのタイプの通知を一時停止する方法は 2 つあります。

- E メール メッセージから [通知を一時的に停止] をクリックして、Horizon Universal Console の [通知履歴] ページに直接進み、[通知を一時停止] をクリックします。
- Horizon Universal Console から直接 [通知履歴] ページに進み、[通知を一時停止] をクリックします。

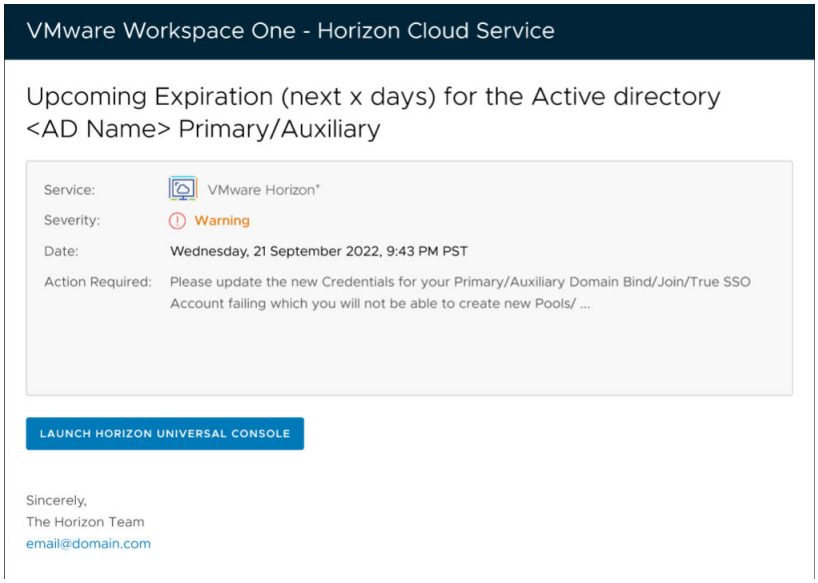
ドメイン アカウントの認証情報 Active Directory 期限切れ - 通知

コンソールのアプリ内通知に加えて、次に示すサービス アカウント認証情報のいずれかがまもなく期限切れになるか、すでに期限切れになっている場合、システムは E メール通知を送信します。

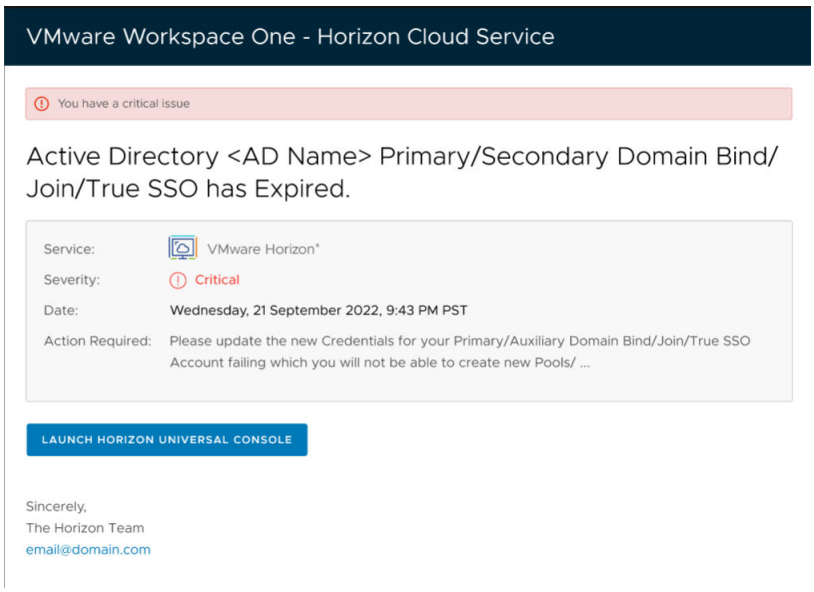
これらの E メールは、サービス アカウントに依存する Horizon Cloud 環境の操作が中断されないようにするために必要な手順を実行する必要があることを示します。

- ドメイン バインド
- ドメイン参加
- True SSO 登録サービス アカウント - プライマリと補助

次のスクリーンショットは、アカウントの認証情報の有効期限が切れそうになったときの E メール通知を示しています。



次のスクリーンショットは、アカウントの認証情報の有効期限が切れた場合の E メール通知を示しています。



次世代 Horizon 制御プレーン を使用した Horizon イメージの管理

イメージ管理は、次世代 Horizon 制御プレーン 環境の基本です。このドキュメント ページでは、Horizon イメージ管理サービス (IMS) を紹介します。このページでは、環境内での IMS 機能の使用に固有の要件についても説明します。

簡単な紹介

IMS を使用することで、Horizon Edge デプロイ全体でデスクトップおよびサーバ資格のイメージ バージョンを作成、カスタマイズ、および公開することができます。

サービスのプロセスは、システム イメージの迅速な管理に依存します。システム イメージによって仮想マシンがパワーオンされ、エンド ユーザーに資格がプロビジョニングされます。システム イメージを管理するには、すべてのイメージのカスタマイズで、管理者がイメージの新しいバージョンを追加して公開し、関連付けられた資格を個別に更新する必要があります。

IMS は、Horizon Edge デプロイ全体で次の機能とメリットを提供することにより、このプロセスを簡素化および合理化します。

- 一元化されたイメージ カタログ。Edge 全体のイメージとそのバージョンおよびコピーが一覧表示されます。
- イメージを公開するための使いやすいガイド付きの手順。
- 異なるクラウド接続された Edge とサイトの資格。イメージ サービスによって管理される同じイメージ バージョンを簡単かつ一貫性のある方法で使用できます。
- カスタマイズを制御および追跡するための簡素化されたイメージのバージョン管理。

重要な用語

イメージ管理を理解するには、`image`、`version`、`copy` などの用語を理解する必要があります。`image` は、オペレーティング システムと仮想マシン モデルを大まかに分類します。この `image` の下の各 `version` は、イメージ上のさまざまなソフトウェア セット用に設計された番号付きの `version` であり、`major.minor.patch` の形式になっています。各 `image version` のコピーは、各 Edge の具体的なインスタンスです。たとえば、`Game` という名前のイメージは、`major.minor.patch` 形式のバージョン `1.1.0` と、`Edge-1`、`Edge-2`、`Edge-3` など、さまざまな Edge でイメージ コピー `Game 1.1.0` を持つことができます。

作成されたイメージ バージョンとそのコピーは、変更不可として扱われます。さらに変更が必要な場合は、コンテンツがソース イメージと異なる場合はマイナー バージョンまたはメジャー バージョンで変更する必要があります。

Microsoft Azure のデプロイと IMS

このセクションでは、Microsoft Azure デプロイの Horizon Edge で IMS を使用する際に注意すべき要件と考慮事項について説明します。

まず、Microsoft Azure デプロイの Horizon Edge は、次のリンク ページの情報に従う必要があります。

Microsoft Azure - Horizon Edge 全体の要件

- Microsoft Azure Edge をデプロイするための要件チェックリスト
- Microsoft Azure Edge のデプロイ

前述のリンク ページの詳細に加えて、IMS 操作が正常に機能し、デプロイでサポートされるようにするには、それらのデプロイも次の要件を満たす必要があります。

デプロイがこれらの要件を継続して満たせない場合は、想定外の結果が発生し、イメージ管理の操作が失敗する可能性があります。公開を行う操作については、特にこれらの要件の影響を受けます。

Microsoft Azure の割り当て容量の要件

利用する Microsoft Azure サブスクリプションには、イメージ管理の操作のために選択する仮想マシン モデルに対する十分な割り当て容量が必要です。イメージ ベース仮想マシンのために使用する推奨モデル タイプにつ

いては、要件チェックリストの Image Management System Requirements セクションを参照してください。

サービス プリンシパルの要件

Microsoft Azure サブスクリプションのサービス プリンシパルの作成で説明されているように、サービスは API 呼び出しを使用して、Microsoft Azure サブスクリプションのリソースと連携します。操作を正常に実行するには、サービス プリンシパルが Microsoft Azure の Horizon Edge で使用するために登録されている限り、次の点に該当していることを確認します。

- そのページで説明されている要件を継続して満たしている。
- 有効期限が切れていない、および有効期限切れにならない。
- Azure ポータルに残っていて、削除されていない。

IMS 固有の既知の制限事項と既知の問題

IMS の既知の制限事項

サービスの既知の制限事項については、『Horizon Cloud Service - next-gen リリース ノート』の「既知の制限」セクションを参照してください。「イメージ」セクションを探します。

たとえば、それらの制限には、現在サポートされていないシナリオやユースケースが含まれる場合があります。

IMS の既知の問題

サービスの既知の問題については、『Horizon Cloud Service - next-gen リリース ノート』の「既知の問題」セクションを参照してください。

Horizon Cloud Service - next-gen でのイメージの追加

Horizon Image Management Service を使用して、Microsoft Azure Marketplace および Microsoft Azure Compute Gallery から提供されるイメージを追加および管理できます。

次の手順を実行する前に、Microsoft Azure のデプロイと IMS で重要な情報についても確認します。

前提条件

- イメージのために使用する仮想マシン モデルを決定します。仮想マシン モデルの要件については、Image Management System Requirements を参照してください。
- Unified Access Gateway と Horizon Edge Gateway は [準備完了] 状態です。
- サブスクリプションにより、ベース仮想マシンのために選択するモデルに適切な CPU コア割り当てが提供されていることを確認します。サポート対象のモデル タイプについては、Image Management System Requirements を参照してください。
- テナント（デスクトップ）サブネットが十分な数の IP アドレスを許可していることを確認します。
- ベース仮想マシンのカスタマイズのための Microsoft Remote Desktop Protocol (RDP) アクセスの場合は、必要な数のパブリック IP アドレスがプロビジョニングされていることを確認します。

- システム イメージ作成操作で使用されるエージェント関連のソフトウェアをダウンロードするために、`softwareupdate.vmware.com` が、TCP プロトコルを介した `443` ポートを使用して、管理サブネットとテナント（デスクトップ）サブネットから解決可能でアクセス可能であることを確認します。詳細については、Microsoft Azure での Horizon Cloud 環境のポートとプロトコルの要件を参照してください。
- プロバイダに少なくとも 1 つの仮想ネットワークとテナント（デスクトップ）サブネットが選択されていることを確認します。
- 追加するイメージのゲスト OS がサポートされているかどうかを確認します。

  ゲスト OS のサポートについては、「製品の相互運用性マトリックス」を参照してください。製品の相互運用性マトリックスの「VMware 製品の相互運用性マトリックス クエリ」の事前構成済み検索には、Horizon Cloud Service - next-gen でサポートされているオペレーティング システムがリストされます。

手順

1. [ホーム] ページで、[イメージ] タイルの [イメージ] をクリックして、[イメージ] ページに移動します。
2. [イメージ] ページで、[追加] をクリックして、[イメージの追加] ページに移動します。
3. [全般情報] セクションで、一意の [イメージ名] を追加し、[次へ] をクリックします。

   イメージ バージョンはダッシュ付きで名前に自動的に追加され、イメージ コピー名（Image-1-0、Image-1-100）が作成されます。
4. イメージの [説明] を追加できます。
5. [マーカー] フィールドに新しいマーカーを追加できます。マーカーに一意の名前を付けます。イメージの保存時に新しいマーカーが保存されます。

   マーカーはオプションですが、マーカーが関連付けられていない場合、プールの作成にイメージを使用することはできません。
6. [イメージ ソース] セクションで、ソース オプションを選択します。

Microsoft Azure Marketplace からのイメージの追加

Horizon Cloud Service next-gen を使用して、Microsoft Azure Marketplace から提供されるイメージを追加および管理できます。

次の手順を実行する前に、「Microsoft Azure のデプロイと IMS」で重要な情報についても確認してください。

手順

1. [ホーム] ページで、[イメージ] タイルの [イメージ] をクリックして、[イメージ] ページに移動します。
2. [イメージ] ページで、[追加] をクリックして、[イメージの追加] ページに移動します。
3. [全般情報] で、一意の [イメージ名] を追加し、[次へ] をクリックします。

   イメージ バージョンはダッシュ付きで名前に自動的に追加され、イメージ コピー名（Image-1-0、Image-1-100）が作成されます。
4. イメージの [説明] を追加できます。

5 [マーカー] フィールドに新しいマーカーを追加できます。マーカーに一意の名前を付けます。イメージの保存時に新しいマーカーが保存されます。

6 [イメージ ソース] セクションで [Microsoft Azure Marketplace] を選択し、[次へ] をクリックします。

7 [ターゲット] サブセクションで、[サイト]、[Horizon Edge]、および [プロバイダ] を選択します。

8 [仮想マシンの詳細] サブセクションで、[OS]、[世代タイプ]、[仮想マシン モデル タイプ]、および [仮想マシン モデル] を選択します。

9 [世代タイプ] には [V1] または [V2] のいずれかを選択します。

OS は、特定の [世代タイプ] のみをサポートします。

10 OS は、特定の [セキュリティ タイプ] のみをサポートします。[セキュリティ タイプ] オプションは、[標準] と [信頼できる起動] のいずれかが自動的に選択され、いずれかが無効になります。

[V1] を選択すると、[標準] [セキュリティ タイプ] のみが有効になります。[標準] は、仮想マシンに対する基本的なレベルのセキュリティを提供します。

[V2] を選択すると、デフォルトで [信頼できる起動] [セキュリティ タイプ] が有効になります。セキュア ブートはデフォルトで有効になっています。これにより、ブートキット、ルートキット、およびカーネルレベルのマルウェアに対する保護が提供されます。仮想 Trusted Platform Module (vTPM) もデフォルトで有効になっています。これは、キー、シークレットを安全に保存し、仮想マシンの起動の整合性を検証します。[信頼できる起動] はセキュリティを強化し、Gen 2 仮想マシンに対する高度な攻撃を防止します。

[V2] には [標準] [セキュリティ タイプ] を選択することもできます。

11 [仮想マシン モデル タイプ] には [GPU なし] または [GPU あり] のいずれかを選択します。

12 利用可能なオプションからサポートされている [仮想マシン モデル] を選択します。

[仮想マシン モデル] オプションは、仮想マシン モデル タイプと世代タイプに基づいて表示されます。

13 [ネットワーク] サブセクションで [パブリック IP アドレス] を有効にするには、トグルをスライドして Remote Desktop Protocol 接続を介してイメージにアクセスし、[ネットワークの選択] を行います。

イメージをカスタマイズおよび最適化するには、適切なネットワークで実行されているイメージから仮想マシンを作成してログインする必要があります。したがって、リソースに対して十分な割り当てを持つ適切な VNet、サブネット、およびパブリック IP アドレスを指定する必要があります。

14 [仮想マシンの管理者認証情報] サブセクションで、イメージのオペレーティング システムにアクセスし、イメージ カスタマイズ プロセスで使用するローカル管理者アカウントの [ユーザー名] と [パスワード] を追加します。

15 ソフトウェア アシュアランスを備えた Windows ライセンスの[チェック ボックス]を選択し、[追加] をクリックします。

[Microsoft Azure Marketplace] からイメージを追加すると、イメージは非公開の状態になり、カスタマイズの準備が整います。イメージは、公開後にのみプールで使用できます。

Microsoft Azure カスタム仮想マシンを使用したイメージの追加

Microsoft Azure Marketplace から提供された、すぐに使用できるカスタム仮想マシンから、イメージを追加および管理できます。

次の手順を実行する前に、Microsoft Azure のデプロイと IMS で重要な情報についても確認します。

前提条件

- Microsoft Azure で作成されたカスタム仮想マシンは、第 1 世代または第 2 世代の仮想マシン モデル タイプである必要があります。
- カスタム仮想マシンが作成されるリソース グループでは、最初にロールベースのアクセス制御 (RBAC) を設定する必要があります。
- ターゲット プロバイダのリージョンとカスタム仮想マシンが存在するリージョンは同じである必要があります。

注： 選択したカスタム仮想マシンは汎用化されたイメージに変換され、イメージ公開ワークフロー実行中に仮想マシンとして再利用することはできません。仮想マシンのバックアップをとっておくことをお勧めします。

手順

1 [ホーム] ページで、[イメージ] タイルの [イメージ] をクリックして、[イメージ] ページに移動します。

2 [イメージ] ページで、[追加] をクリックして、[イメージの追加] ページに移動します。

3 [全般情報] で、一意の [イメージ名] を追加し、[次へ] をクリックします。

イメージ バージョンはダッシュ付きで名前に自動的に追加され、イメージ コピー名（Image-1-0、Image-1-100）が作成されます。

4 イメージの [説明] を追加できます。

5 [マーカー] フィールドに新しいマーカーを追加できます。

マーカーに一意の名前を付けます。イメージの保存時に新しいマーカーが保存されます。

6 [イメージ ソース] セクションで [Microsoft Azure カスタム仮想マシン] を選択し、[次へ] をクリックします。

7 [ターゲット] サブセクションで、[サイト]、[Horizon Edge]、および [プロバイダ] を選択します。

8 [仮想マシンの詳細] で [仮想マシン] を選択します。

すべてのカスタム仮想マシンは、入力された [Azure リソース グループ]

`vmw-hcs-<ProviderInstance_Id>-base-vms` の一部である必要があります。リソース グループ名は、Microsoft Azure ポータルの [仮想マシンの詳細] ページで取得できます。

注： プールは、選択した仮想マシンの世代タイプでのみプロビジョニングできます。

9 このカスタム仮想マシンの [OS] タイプを選択します。

[カスタム仮想マシン] の [OS] タイプは検証できないため、正確に選択してください。

10 [仮想マシンの管理者認証情報] サブセクションで、イメージのオペレーティング システムにアクセスし、イメージ カスタマイズ プロセスで使用するローカル管理者アカウントの [ユーザー名] と [パスワード] を追加します。

ユーザー名の長さは最大 19 文字で、ピリオド（「.」）で終わることはできません。「guest」や「administrator」など、Microsoft Azure で禁止されているユーザー名は使用できません。

パスワードは 12 ～ 123 文字で、次の要件のうちの 3 つを満たしている必要があります：小文字（a ～ z）を使用、大文字（A ～ Z）を使用、数字を使用、特殊文字 (! @#$%/^&*)。

11 ソフトウェア アシュアランスを備えた Windows ライセンスの[チェック ボックス]を選択し、[追加] をクリックします。

Microsoft Azure Compute Gallery からのイメージの追加

Microsoft Azure Compute Gallery から提供されるイメージを追加および管理できます。

前提条件

- 「Horizon Cloud Service - next-gen でのイメージの追加」の説明に従って、一般的な前提条件の操作を実行します。
- Microsoft Azure Compute Gallery からイメージを追加する手順を実行する前に、使用する予定のオペレーティング システムがサポート対象であることを確認します。

  一般的な前提条件については、VMware 製品の相互運用性マトリックスを参照してください。Microsoft Azure Compute Gallery からイメージをインポートする場合は、指定されたクエリにリストされているイメージのみがサポートされます。

  具体的に言うと、その後のオペレーティング システムのリファレンス リストを使用して、イメージ定義が適切に設定されているかどうかを判断します。

Microsoft Azure Compute Gallery からイメージを追加する際のサポート対象オペレーティング システム

次の情報は、Horizon Cloud Service - next-gen がサポートする、Microsoft Windows オペレーティング システムごとのオファーと SKU の詳細を示しています。リストされているオファーと SKU の値は、Microsoft Azure Compute Gallery イメージ定義で設定する必要があります。たとえば、イメージに Microsoft - Windows Server 2022 オペレーティング システムを使用するには、オファー値が `windowsserver`、SKU 値が `2022-datacenter` であることを確認してください。

オペレーティング システム	Azure Marketplace 仮想マシン イメージ – Gen 1	Azure Marketplace 仮想マシン イメージ – Gen 2
Microsoft Windows Server 2022	発行元：microsoftwindowsserver オファー：windowsserver SKU：2022-datacenter	発行元：microsoftwindowsserver オファー：windowsserver SKU：2022-datacenter-g2
Microsoft - Windows Server 2019	発行元：microsoftwindowsserver オファー：windowsserver SKU：2019-datacenter	発行元：microsoftwindowsserver オファー：windowsserver SKU：2019-datacenter-gensecond
Microsoft - Windows Server 2016	発行元：microsoftwindowsserver オファー：windowsserver SKU：2016-datacenter	発行元：microsoftwindowsserver オファー：windowsserver SKU：2016-datacenter-gensecond
Microsoft - Windows 11 Enterprise multi-session 23H2	サポート対象外	発行元：microsoftwindowsdesktop オファー：windows-11 SKU：win11-23h2-avd
Microsoft - Windows 11 Enterprise 23H2	サポート対象外	発行元：microsoftwindowsdesktop オファー：windows-11 SKU：win11-23h2-ent

オペレーティング システム	Azure Marketplace 仮想マシン イメージ – Gen 1	Azure Marketplace 仮想マシン イメージ – Gen 2
Microsoft - Windows 11 Enterprise multi-session 22H2	サポート対象外	発行元：microsoftwindowsdesktop オファー：windows-11 SKU：win11-22h2-avd
Microsoft - Windows 11 Enterprise 22H2	サポート対象外	発行元：microsoftwindowsdesktop オファー：windows-11 SKU：win11-22h2-ent
Microsoft - Windows 11 Enterprise multi-session, 21H2	サポート対象外	発行元：microsoftwindowsdesktop オファー：windows-11 SKU：win11-21h2-avd
Microsoft - Windows 11 21H2 Enterprise	サポート対象外	発行元：microsoftwindowsdesktop オファー：windows-11 SKU：win11-21h2-ent
Microsoft - Windows 10 Enterprise multi-session, 22H2	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：win10-22h2-avd	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：win10-22h2-avd-g2
Microsoft - Windows 10 Enterprise 22H2	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：win10-22h2-ent	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：win10-22h2-ent-g2
Microsoft - Windows 10 Enterprise multi-session, 21H2	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：win10-21h2-avd	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：win10-21h2-avd-g2
Microsoft - Windows 10 Enterprise, 21H2	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：win10-21h2-ent	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：win10-21h2-ent-g2
Microsoft - Windows 10 Pro, 21H2	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：win10-21h2-pro	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：win10-21h2-pro-g2
Microsoft - Windows 10 Enterprise multi-session, 20H2	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：20h2-evd	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：20h2-evd-g2
Microsoft - Windows 10 Enterprise, 20H2	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：20h2-ent	発行元：microsoftwindowsdesktop オファー：windows-10 SKU：20h2-ent-g2

Microsoft Azure Compute Gallery からのイメージの追加の手順

Horizon Image Management Service を使用すると、Microsoft Azure Compute Gallery から、サポート対象のオペレーティング システムを含むカスタム イメージを追加できます。

次の手順を実行する前に、Microsoft Azure のデプロイと IMS で重要な情報についても確認します。

前提条件

必要に応じてクリックまたは上にスクロールして、「Microsoft Azure Compute Gallery からのイメージの追加」トピックの先頭に記載されている前提条件を確認してください。それらの前提条件を満たしていることを確認してください。

手順

1 [ホーム] ページで、[イメージ] タイルの [イメージ] をクリックして、[イメージ] ページに移動します。

2 [イメージ] ページで、[追加] をクリックして、[イメージの追加] ページに移動します。

3 [全般情報] で、一意の [イメージ名] を追加し、[次へ] をクリックします。

イメージ バージョンはダッシュ付きで名前に自動的に追加され、イメージ コピー名（Image-1-0、Image-1-100）が作成されます。

4 イメージの [説明] を追加できます。

5 [マーカー] フィールドに新しいマーカーを追加できます。マーカーに一意の名前を付けます。イメージの保存時に新しいマーカーが保存されます。

6 [イメージ ソース] セクションで [Microsoft Azure Compute Gallery] を選択し、[次へ] をクリックします。

7 [ターゲット] サブセクションで、[サイト] および [Horizon Edge] を選択します。

8 [ソース イメージ バージョンの詳細] サブセクションで、Microsoft Azure ポータルから [Microsoft Entra ID テナント ID] を追加します。イメージ定義のイメージ バージョンにある JSON View リンクをクリックして、Microsoft Azure ポータルから取得した [リソース ID] を追加します。イメージが Horizon Universal Console を使用して公開された場合、この ID はコンソールの [イメージ バージョンの詳細] ページにある [イメージ コピー] グリッドの [ロケーション パス] 列から取得できます。

選択したターゲット Horizon Edge のプロバイダに、ソース イメージ、またはイメージを含むリソース グループへの Microsoft Azure RBAC 読み取りアクセス権があることを確認します。また、ソース イメージがすでに Horizon Agent で公開されていることを確認します。

9 ソース イメージ バージョンの属性を使用するには、[イメージ属性] に対して [ソース イメージからコピー] を選択します。

`VMware Managed Services Provider` (MSP) でサポートされている場合は、MSP 組織のプロバイダから自分のプロバイダにイメージをコピーできます。このプロセスでは、自分の組織以外の外部組織 (MSP) に対応する Horizon カタログ内の公開済みソース イメージを利用します。MSP は、サーバに存在するアプリケーションの詳細を含む完全なイメージまたはマルチセッション イメージを提供します。

[ソース イメージからコピー] を選択した場合は、元のイメージを共有または公開した [組織 ID] を指定します。

[オーバーライド] によって、属性を構成できます。オーバーライド オプションは、Horizon カタログにないソース イメージをコピーする場合に適用できます。たとえば、Horizon プロバイダのサブスクリプションから読み取り可能な外部サブスクリプションのイメージなどです。

外部イメージをインポートする場合は、ソース イメージに最新の Horizon Agent がインストールされていることを確認します。インストールされていないと、このイメージのデスクトップ/サーバ プールの一部として作成された仮想マシンでエラーが発生する可能性があります。

ソース イメージは、必要なエージェントとソフトウェアで汎用化された、すでに公開されているイメージです。したがって、ユーザーの組織への同じイメージのコピーをプールで直接使用できます。他のサブスクリプションまたはリージョンに再公開することもできます。プロバイダには、ソース イメージへの適切な RBAC アクセス権が必要です。

[オーバーライド] を選択した場合は、ソース イメージの [OS] を指定します。OS が特定の世代タイプをサポートしていない場合、サポートされている世代タイプがデフォルトで選択されます。

10 選択可能な場合は、[世代タイプ] オプションを選択します。

注： Microsoft Azure 第 1 世代および第 2 世代の仮想マシンがサポートされています。[V1] を選択した場合、プールは V1 世代モデルを使用してのみプロビジョニングできます。

11 [仮想マシンの詳細] サブセクションで [仮想マシン モデル タイプ] および [仮想マシン モデル] を選択します。

注： [世代タイプ] および [仮想マシン モデル タイプ] の選択はフィルタとして機能し、[仮想マシン モデル] ドロップダウン メニューで使用可能な仮想マシン モデルを決定します。

12 [仮想マシンの管理者認証情報] サブセクションで、イメージのオペレーティング システムにアクセスし、イメージ変換プロセスで使用するローカル管理者アカウントの [ユーザー名] と [パスワード] を追加します。

13 ソフトウェア アシュアランスを備えた Windows ライセンスの[チェック ボックス]を選択し、[追加] をクリックします。

既存の Microsoft Azure Compute Gallery イメージへのバージョンの追加

バージョンのクローンを作成することなく、既存の Microsoft Azure Compute Gallery イメージに新しいバージョンを追加できます。既存のイメージのバージョンとして追加できるのは、類似のタイプのイメージのみです。

手順

1 Horizon Universal Console の [ホーム] ページの [イメージ] タイルをクリックします。

2 [イメージ] ページで、[Microsoft Azure Compute Gallery] から追加された [イメージ名] をクリックして、[イメージ] ページに移動します。

3 [追加] をクリックして、[イメージ バージョンの追加] ページに移動します。

4 [ソース] セクションで、[Microsoft Azure Compute Gallery] の下の [次へ] をクリックします。

5 [ソースの詳細] セクションの [ターゲット] サブセクションで、[サイト]、[Horizon Edge]、[プロバイダ] を選択します。

6 [ソース イメージ バージョンの詳細] サブセクションで、Microsoft Azure ポータルから [Microsoft Entra ID テナント ID] を追加します。イメージ定義のイメージ バージョンにある JSON View リンクをクリックして、Microsoft Azure ポータルの Active Directory プロパティから取得した [リソース ID] を追加します。イメージが Horizon Universal Console を使用して公開された場合、この ID はコンソールの [イメージ バージョンの詳細] ページにある [イメージ コピー] グリッドの [ロケーション パス] 列から取得できます。

選択したターゲット [Horizon Edge] のプライマリ プロバイダに、ソース イメージ、またはイメージを含むリソース グループへの Microsoft Azure RBAC 読み取りアクセス権があることを確認します。また、ソース イメージが Horizon Agent ですでに公開されていることを確認します。

7 イメージ属性については、[ソース イメージからコピー] および [オーバーライド] を選択します。

a [ソース イメージからコピー] を選択した場合は、Horizon Universal Console を使用してイメージを公開したアカウントの [組織 ID] を追加します。この ID は、そのアカウントのユーザー/組織設定で取得できます。[ソース イメージからコピー] オプションでは、ソース イメージ バージョンの属性が使用されます。

[OS 名]、[OS タイプ]、[セッション タイプ] がソース イメージから自動的にコピーされます。

`VMware Managed Services Provider` (MSP) でサポートされている場合は、MSP 組織のプロバイダから自分のプロバイダにイメージをコピーできます。このプロセスでは、自分の組織以外の外部組織 (MSP) に対応する Horizon カタログ内の公開済みソース イメージを利用します。MSP は、サーバに存在するアプリケーションの詳細を含む完全なイメージまたはマルチセッション イメージを提供します。

[ソース イメージからコピー] オプションは、MSP 組織のカタログで使用可能な既存の Horizon イメージ バージョンを使用してバージョンを追加する場合に適用されます。

b [オーバーライド] を選択した場合は、[OS]、[OS タイプ]、および [セッション タイプ] を選択する必要があります。

[オーバーライド] オプションは、Horizon カタログにないソース イメージをコピーする場合に適用されます。たとえば、Horizon プロバイダのサブスクリプションから読み取り可能な外部サブスクリプションのイメージなどです。

外部イメージを追加する場合は、ソース イメージに最新の Horizon Agent がインストールされていることを確認します。インストールされていないと、このイメージのデスクトップ/サーバ プールの一部として作成された仮想マシンでエラーが発生する可能性があります。

ソース イメージの作成に使用される Microsoft Azure Marketplace イメージの公開者、オファー、SKU が、ソース Azure Compute Gallery のイメージ定義で設定されていることを確認します。公開者、オファー、SKU の値は、新しい Azure Marketplace イメージをインポートするときにリストされるサポート対象イメージの既存のリストと一致する必要があります。

ソース イメージは、必要なエージェントとソフトウェアで汎用化された、すでに公開されているイメージです。したがって、ユーザーの組織への同じイメージのコピーをプールで直接使用できます。他のサブスクリプションまたはリージョンに再公開することもできます。プロバイダには、ソース イメージへの適切な RBAC アクセス権が必要です。

8 [仮想マシンの詳細] サブセクションで [仮想マシン モデル タイプ] および [仮想マシン モデル] を選択します。

注： [仮想マシン モデル] リストには、イメージと同じ世代タイプの仮想マシン モデルのみが一覧表示されます。

9 [仮想マシンの管理者認証情報] サブセクションで、イメージのオペレーティング システムにアクセスし、イメージ変換プロセスで使用するローカル管理者アカウントの [ユーザー名] と [パスワード] を追加します。

10 [ソフトウェア アシュアランスを備えた Windows ライセンス] の[チェック ボックス]を選択します。

11 [ターゲット バージョン] セクションで、[バージョンのタイプ] として [メジャー] または [マイナー] を選択します。

   a [メジャー] を選択すると、選択した内容と、イメージの既存のバージョンに基づいて、[想定されるバージョン番号] が自動的に入力されます。

   b [マイナー] を選択した場合は、[次のバージョン未満のバージョンを追加] にメジャー バージョン番号を追加します。その下に [マイナー] バージョンを追加すると、[想定されるバージョン番号] が自動的に入力されます。

12 [マーカー] フィールドに新しいマーカーを追加できます。マーカーに一意の名前を付けます。イメージの保存時に新しいマーカーが保存されます。

Microsoft Azure カスタム仮想マシンを使用した既存のイメージへのバージョンの追加

バージョンのクローンを作成することなく、既存の Microsoft Azure Compute Gallery イメージに新しいバージョンを追加できます。既存のイメージのバージョンとして追加できるのは、類似のタイプのイメージのみです。

手順

1 Horizon Universal Console の [ホーム] ページの [イメージ] タイルをクリックします。

2 [イメージ] ページで、[イメージ名] をクリックして、[イメージ] ページに移動します。

3 [追加] をクリックして、[イメージ バージョンの追加] ページに移動します。

4 [ソース] セクションで、[Microsoft Azure カスタム仮想マシン] の下の [次へ] をクリックします。

5 [ソースの詳細] セクションの [ターゲット] サブセクションで、[サイト]、[Horizon Edge]、[プロバイダ] を選択します。

6 [全般情報] で、一意の [イメージ名] を追加し、[次へ] をクリックします。

   イメージ バージョンはダッシュ付きで名前に自動的に追加され、イメージ コピー名（Image-1-0、Image-1-100）が作成されます。

7 イメージの [説明] を追加できます。

8 [マーカー] フィールドに新しいマーカーを追加できます。

   マーカーに一意の名前を付けます。イメージの保存時に新しいマーカーが保存されます。

9 [イメージ ソース] セクションで [Microsoft Azure カスタム仮想マシン] を選択し、[次へ] をクリックします。

10 [ターゲット] サブセクションで、[サイト]、[Horizon Edge]、および [プロバイダ] を選択します。

11 [仮想マシンの詳細] で [仮想マシン] を選択します。

   すべてのカスタム仮想マシンは、入力された [Azure リソース グループ]

   `vmw-hcs-<ProviderInstance_Id>-base-vms` の一部である必要があります。リソース グループ名は、Microsoft Azure ポータルの [仮想マシンの詳細] ページで取得できます。

   注： [仮想マシンの選択] リストには、イメージと同じ世代タイプのカスタム仮想マシンのみが一覧表示されます。

12 このカスタム仮想マシンの [OS] タイプを選択します。

[カスタム仮想マシン] の [OS] タイプは検証できないため、正確に選択してください。外部イメージをインポートする場合は、ソース イメージに最新の Horizon Agent がインストールされていることを確認します。インストールされていないと、このイメージのデスクトップ/サーバ プールの一部として作成された仮想マシンでエラーが発生する可能性があります。

13 [仮想マシンの管理者認証情報] サブセクションで、イメージのオペレーティング システムにアクセスし、イメージ カスタマイズ プロセスで使用するローカル管理者アカウントの [ユーザー名] と [パスワード] を追加します。

ユーザー名の長さは最大 19 文字で、ピリオド（「.」）で終わることはできません。「guest」や「administrator」など、Microsoft Azure で禁止されているユーザー名は使用できません。

パスワードは 12 ～ 123 文字で、次の要件のうちの 3 つを満たしている必要があります：小文字（a ～ z）を使用、大文字（A ～ Z）を使用、数字を使用、特殊文字 (! @#$%/^&*) を使用。「Password1」など、Microsoft Azure で禁止されているパスワードは使用できません。

14 [ソフトウェア アシュアランスを備えた Windows ライセンス] の[チェック ボックス]を選択します。

15 [ターゲット バージョン] セクションで、[バージョンのタイプ] として [メジャー] または [マイナー] を選択します。

a [メジャー] を選択すると、選択した内容と、イメージの既存のバージョンに基づいて、[想定されるバージョン番号] が自動的に入力されます。

b [マイナー] を選択した場合は、[次のバージョン未満のバージョンを追加] にメジャー バージョン番号を追加します。その下に [マイナー] バージョンを追加すると、[想定されるバージョン番号] が自動的に入力されます。

16 [マーカー] フィールドに新しいマーカーを追加できます。マーカーに一意の名前を付けます。イメージの保存時に新しいマーカーが保存されます。

イメージの削除

イメージ管理プロセスで、必要に応じてイメージを削除できます。

前提条件

- Unified Access Gateway と Edge Gateway が準備完了状態であること。
- イメージが使用可能、インポート済み、または失敗状態であること。

手順

1 Horizon Universal Console にログインします。

2 [リソース] - [イメージ] に移動してイメージのリストを表示します。

3 削除するイメージ名のリンクをクリックします。

4 削除するバージョンを選択します。

5 [削除] をクリックします。

6 [イメージのバージョンの削除] で、[削除] をクリックして削除プロセスを開始します。

このアクションにより、関連付けられているすべてのサイトからイメージのバージョンが削除されます。これがこのイメージの唯一のバージョンである場合は、関連付けられた親イメージも削除されます。

イメージのクローン作成

親イメージに重要な変更を加えた場合は、イメージ バージョンのクローンを作成して、既存の公開済みイメージ バージョンから新しいイメージを作成します。

次の手順を実行する前に、Microsoft Azure のデプロイと IMS で重要な情報についても確認します。

この手順では、使用可能、または部分的に使用可能なメジャーまたはマイナー バージョンから、バージョンの番号がインクリメントした新しいイメージ バージョンを作成します。

前提条件

- イメージがインポートおよび公開されていること。
- 選択したイメージが使用可能、または部分的に使用可能であること。
- プロバイダに少なくとも 1 つの仮想ネットワークとテナント（デスクトップ）サブネットが選択されている。

手順

1 Horizon Universal Console の [ホーム] ページで、[イメージ] をクリックします。

2 [イメージ] ページで、イメージ リンクをクリックしてイメージ バージョンをコピーします。

3 イメージを選択し、[コピー] - [イメージとしてコピー] をクリックします。

4 [全般情報] セクションで、[イメージ名] を追加し、[次へ] をクリックします。

5 [ネットワーク] で、コピーされたイメージの新しい仮想マシンに使用するネットワークを選択し、[保存] をクリックします。

イメージ バージョンのクローン作成

Horizon Cloud Service - next-gen でイメージ バージョンのクローンを作成すると、イメージのバージョン番号がインクリメントして、それを通常バージョンとして公開できます。クローンとして作成されたイメージを選択したターゲットに正常に公開したら、それらの公開されたクローンを使用してプール グループを作成できます。

次の手順を実行する前に、Microsoft Azure のデプロイと IMS で重要な情報についても確認します。

前提条件

- イメージがインポートおよび公開されていること。
- 選択したバージョンが使用可能、または部分的に使用可能であること。
- プロバイダに少なくとも 1 つの仮想ネットワークとテナント（デスクトップ）サブネットが選択されている。

手順

1 Horizon Universal Console の [ホーム] ページで、[イメージ] をクリックします。

2 [イメージ] ページで、イメージ リンクをクリックしてイメージ バージョンを一覧表示します。

3 イメージを選択し、[公開] - [イメージ バージョンとしてコピー] をクリックします。

4 [全般情報] セクションで、次のいずれかのオプションを選択し、[次へ] をクリックします。

- 別のソフトウェアを使用するなど、イメージをアップグレードするには、[メジャー] を選択します。これにより、バージョン番号のメジャー部分が増分されます。
- パッチ適用や既存のソフトウェア アップグレードなど、イメージを段階的にアップグレードするには、[マイナー] を選択します。これにより、バージョン番号のマイナー部分が増分されます。

  最大 99 のバージョンのメジャーまたはマイナー アップグレード イメージを使用できます。合計 99 のメジャー バージョンを作成できます。任意のメジャー バージョンの下に合計 99 のマイナー バージョンを作成できます。

5 [ネットワーク] パネルで、コピーされたイメージ バージョンの新しい仮想マシンに使用するネットワークを選択し、[保存] をクリックします。

イメージ バージョンの編集

部分的に使用可能または使用可能な状態にあるイメージ バージョンのマーカーを編集できます。

前提条件

- イメージがインポートおよび公開されていること。
- 選択したバージョンは部分的に使用可能または使用可能な状態にあること。

手順

1 Horizon Universal Console にログインします。

2 ホーム ページで、[イメージ] タイルの [イメージ] をクリックします。

3 [イメージ] ページで、[使用可能] 状態のイメージ リンクをクリックして、イメージ バージョンを一覧表示します。

4 イメージ バージョン ページでイメージ バージョンを選択し、[編集] をクリックします。

5 [バージョンの編集] ページで、[説明] を追加または編集し、既存の [マーカー] を追加または削除するか、新しい [マーカー] を追加します。

  バージョンの既存のマーカーを現在編集されているバージョンに追加すると、マーカーに関連付けられたすべてのプールが現在のバージョンに更新されます。プールに関連付けられたマーカーは削除できません。古いエージェントに関連付けられているマーカーが選択されている場合は、警告メッセージが表示されます。ベスト プラクティスとして、最新のエージェント バージョンを含むマーカーを選択します。

6 [保存] をクリックします。

イメージの公開

イメージを追加して詳細を確認したら、Horizon Cloud Service - next-gen からイメージを公開できます。

次の手順を実行する前に、Microsoft Azure のデプロイと IMS で重要な情報についても確認します。

前提条件

続行する前に、次のタスクが完了していることを確認します。

- ドメイン登録が完了していること。
- Microsoft Entra ID が VMware Cloud に接続されていること。
- サイトが正常に作成されました。
- Unified Access Gateway と Edge Gateway の準備が完了していること。
- イメージ情報が検証され、イメージは未公開の状態であること。
- システム イメージ作成操作で使用されるエージェント関連のソフトウェアをダウンロードするために、`softwareupdate.vmware.com` は、TCP プロトコルを介した `443` ポートを使用して、管理サブネットとテナント（デスクトップ）サブネットから解決可能でアクセス可能です。Edge プロキシが設定されている場合は、直接または Edge プロキシ経由でアクセスできる必要があります。プロキシ自体は、テナント（デスクトップ）サブネット内のイメージ仮想マシンからアクセスできる必要があります。イメージ サービスは、Edge レベルで設定されたプロキシを使用します。詳細については、Microsoft Azure での Horizon Cloud 環境のポートとプロトコルの要件を参照してください。
- GPU タイプの仮想マシン モデルが選択されている場合は、NVIDIA GPU ドライバが仮想マシンにインストールされていることを確認します。詳細については、Windows を実行している N シリーズ仮想マシンに NVIDIA GPU ドライバをインストールするを参照してください。
- プロバイダに少なくとも 1 つの仮想ネットワークとテナント（デスクトップ）サブネットが選択されている。
- 必要に応じて、イメージに Horizon Agent を手動でインストールします。

  Horizon Cloud Service - next-gen は、公開ワークフロー実行中に Horizon Agent を自動的にインストールします。ただし、特定のユースケースで公開ワークフローの前にエージェントをインストールする必要がある場合は、KB 91998 を参照してください。Horizon Agent を手動でインストールする場合は、次の手順を実行するときに、[Horizon Agent のインストール] トグルの選択を解除します。
- Microsoft Azure カスタム スクリプト拡張機能 (CSE)、Azure RunCommand、および Sysprep が、Microsoft Azure のイメージ仮想マシン上のポリシー、ファイアウォール、または外部ソリューションによってブロックまたは中断されていないことを確認します。Azure イメージのイメージ公開プロセスでは、Azure カスタム スクリプト拡張機能と Azure RunCommand が使用され、Azure コンピューティング ギャラリーでキャプチャする前に Sysprep を使用してイメージが汎用化されます。

  イメージ仮想マシンでプロキシを設定する場合は、URL `https://softwareupdate.vmware.com/` をホワイトリストに登録して、URL がプロキシによってバイパスされるようにする必要があります。

Horizon Cloud Service - next-gen では、CSE は Horizon Agent をインストールするのに必要です。したがって、Azure ポリシーを使用して、イメージの準備に使用される仮想マシンであるイメージ仮想マシンへの拡張機能のインストールを制限する場合は、公開プロセスの失敗を防ぐために、構成のポリシーの割り当てフェーズで次のいずれかを実行してください。

- CSE に関連する Microsoft Azure セキュリティ ポリシーで、イメージ仮想マシンへの CSE のインストールと実行が許可されていることを確認します。

  注： ポリシーを割り当てるときに、除外するものを選択できます。これは、ポリシーの割り当てから除外することになるリソースです。この方法を使用する場合は、ポリシーから除外するイメージ関連リソースを選択します。

- **`vmw-hcs-image-CustomScriptExtension`** という名前の CSE の実行を許可します。公開プロセス中に、Horizon Cloud Service - next-gen は、イメージ仮想マシンに接続されている CSE の **`vmw-hcs-image-CustomScriptExtension`** 名を使用します。

手順

1 Horizon Universal Console の [ホーム] ページで、[イメージ] タイルをクリックして、[イメージ] ページに移動します。[公開の準備完了] になっているイメージをクリックします。

2 イメージの詳細ページで、イメージの [バージョン] を選択し、ドロップダウンを [非公開] - [公開] の順にクリックします。

3 [送信先] セクションで、イメージ バージョンがインポートされた [送信元 Horizon Edge] が事前に選択されているため、選択解除できません。

  注： イメージは常に送信元 Horizon Edge に公開されます。

  [イメージ] をさらに多くの Horizon Edge に公開するには、表内のチェックボックスを選択します。[次へ] をクリックします。

4 [プロパティ] セクションで、トグルをスライドして [自動 Windows アップデートをオフにする] を選択できます。

  これにより物理デスクトップ機能が無効になり、仮想マシンのパフォーマンスとキャパシティの使用が効率化され、Microsoft Windows Sysprep の問題を回避できるようになります。

5 [Windows ストア アプリを削除]（AppX パッケージとも呼ばれる）トグルをスライドして、アプリケーションおよび Windows ストアの自動更新とダウンロードを無効にできます。これによりパフォーマンスが向上し、Microsoft Windows Sysprep の問題を回避できるようになります。

  次の Windows Store アプリは保持され、公開プロセス中は削除されません。

```
Microsoft.DesktopAppInstaller
Microsoft.Messaging
Microsoft.MSPaint
Microsoft.Windows.Photos
Microsoft.MicrosoftStickyNotes
Microsoft.WindowsCalculator
Microsoft.WindowsCommunicationsApps
Microsoft.WindowsSoundRecorder
```

```
Microsoft.WindowsStore
Microsoft.WindowsNotepad
Microsoft.ScreenSketch
Microsoft.Xbox.TCUI
Microsoft.XboxApp
Microsoft.XboxGameCallableUI
Microsoft.XboxGameOverlay
Microsoft.XboxGamingOverlay
Microsoft.XboxIdentityProvider
Microsoft.XboxSpeechToTextOverlay
MSTeams
Windows.CBSPreview
windows.immersivecontrolpanel
Windows.PrintDialog
```

6 トグルを [公開エラー リカバリを有効にする] にスライドすると、公開プロセスでリカバリ不能なエラーが発生した場合に備えたイメージ リカバリ用のバックアップ仮想マシンを作成できます。[次へ] をクリックします。

7 イメージに優先エージェントがすでにインストールされている場合は、[Horizon Agent のインストール] トグルを選択解除します。

重要： [Horizon Agent のインストール] トグルはデフォルトでオンになっています。これは通常、イメージにエージェントがインストールされておらず、公開を行う操作によってエージェントがインストールされるためです。ただし、イメージに優先エージェントがすでにインストールされている場合は、このトグルを確実にオフにします。このトグルをオンにして [公開] をクリックすると、イメージを公開する手順の一環として、イメージに対するエージェントのインストール プロセスが実行されます。イメージにエージェントがすでにインストールされてる場合にこのトグルをオンにして [公開] をクリックすると、エージェントがすでにインストールされているイメージでエージェントのインストール プロセスが実行されるため、操作の競合が発生することがあります。

8 [Horizon Agent の機能] の選択を実行し、[次へ] をクリックします。

9 [公開イメージ操作] セクションで、トグルを [リモート アプリケーションのスキャン] にスライドできます。これは、マルチセッション（Azure 仮想デスクトップまたは RDSH）イメージにのみ適用されます。また、トグルを [公開イメージの検証] にスライドして、イメージを使用してプールをプロビジョニングするときに公開イメージでエラーが発生しないように検証することができます。この場合、システム生成のプールを使用してイメージを検証します。

トグルを [公開イメージの検証] にスライドすると、公開プロセスの時間が長くなる可能性があります。

10 [リモート アプリケーションのスキャン] または [公開イメージの検証] を有効にする場合は、イメージから作成されたシステム生成のプールに添付される、宛先の [仮想ネットワーク] を選択します。今後プールを作成するために使用するものと同じテナント仮想ネットワークを選択してください。

11 公開イメージ操作のための [ネットワークの選択] を行います。[公開] をクリックします。

公開前のイメージの詳細の確認

イメージを公開する前に、イメージ情報が正確であることを確認します。

前提条件

異なるサブスクリプションでイメージが表示されるようにするには、まずロールベースのアクセス制御 (RBAC) を設定する必要があります。詳細については、Horizon Cloud アプリケーション登録にカスタム ロールを使用するを参照してください。

手順

1 Horizon Cloud Service にログインします。

2 [リソース] - [イメージ] に移動してイメージのリストを表示します。

3 イメージ名のリンクをクリックすると、イメージのバージョンとステータスを示す [バージョン] の表が表示されます。

4 イメージの詳細を確認します。

   a 確認するイメージ バージョンのリンクをクリックします。

   b [プロパティ]、[イメージ コピー]、[プール]、[アプリケーション スキャン プール]、[リモート アプリケーション] の情報を確認します。

リカバリ不能なエラーが発生して失敗したイメージの公開

Sysprep やイメージ検証エラーなどのリカバリ不能なエラーでイメージが失敗した場合は、最初から公開し直すことができます。

手順

1 VMware Horizon® Cloud Service™ - next-gen にログインします。

2 Horizon Universal Console の [ホーム] ページで、[イメージ] をクリックします。

3 [イメージ] ページで、[失敗] のイメージ リンクをクリックしてイメージ バージョン ページに移動します。

4 イメージ バージョン ページでイメージを選択し、[エラー] - [公開] の順にクリックして、イメージを最初から再度公開します。

   最初から公開することが可能になるのは、[公開エラー リカバリを有効にする]および[公開イメージの検証]が、イメージの公開 のときに有効になっている場合のみです。

公開イメージの検証

公開イメージは、イメージ管理プロセスで検証できます。

前提条件

- Edge Gateway の準備が完了していること。
- イメージが正常に公開されていること。
- プロバイダに少なくとも 1 つの仮想ネットワークとテナント（デスクトップ）サブネットが選択されている。

手順

1 Horizon Universal Console の [ホーム] ページで、[イメージ] をクリックします。

2 [イメージ] ページで、イメージ リンクをクリックしてイメージ バージョン ページに移動します。

3 検証するイメージ バージョンを選択し、[公開] - [検証] をクリックします。

4 イメージの検証に使用するネットワークを選択します。

5 [保存] をクリックして検証を開始します。

検証中に失敗したイメージの再検証

イメージ管理プロセスで検証中に失敗したイメージを再検証できます。

前提条件

- Edge Gateway の準備が完了していること。
- イメージが正常に公開されていること。
- プロバイダに少なくとも 1 つの仮想ネットワークとテナント（デスクトップ）サブネットが選択されている。

手順

1 Horizon Universal Console の [ホーム] ページで、[イメージ] をクリックします。

2 [イメージ] ページで、[失敗] のイメージ リンクをクリックしてイメージ バージョン ページに移動します。

3 検証するイメージ バージョンの名前を選択し、[公開] - [検証] をクリックします。

4 イメージの検証に使用する[ネットワークの選択]を行います。[保存] をクリックします。

イメージ バージョンの再公開

失敗したイメージ バージョンの公開を再試行するか、イメージ バージョンの場所を追加のプロバイダ インスタンスに拡張できます。

次のユースケースでは、Horizon Cloud Service の [再公開] 機能を使用します。

- イメージ バージョンを公開しようとすると失敗する場合。

  イメージ バージョンを再公開するために、古いイメージを削除し、最初から開始する必要はありません。

- プロバイダ インスタンスの最初の公開にイメージ バージョンが含まれていない場合。

  イメージ バージョンを再公開して、プロバイダ インスタンスに追加できます。

次の手順を実行する前に、Microsoft Azure のデプロイと IMS で重要な情報についても確認します。

追加のプロバイダ インスタンスへのイメージ バージョンの再公開

複数のプロバイダ インスタンスがある場合、以前の公開フェーズで選択したもの以外の追加のプロバイダ インスタンス (Edge) にイメージ バージョンの場所を拡張する必要がある場合があります。

イメージ バージョンの場所を新しいプロバイダ インスタンスに拡張します。

前提条件

イメージ バージョンは、一部公開済み、失敗、または利用可能の状態である必要があります。

手順

1 Horizon Universal Console の [ホーム] ページで、[イメージ] をクリックします。

2 [イメージ] ページで、公開済みのイメージ リンクをクリックします。

3 公開済みのイメージを選択し、[公開] をクリックします。

4 [イメージを再公開] ページで、イメージ バージョンの公開に失敗した Horizon Edge は自動的に選択され、選択解除することはできません。イメージを含まない Edge を選択し、[再公開] をクリックします。

失敗したイメージの再公開

イメージを公開しようとして失敗した場合は、[再公開] ワークフローを使用して公開を再試行できます。[再公開] オプションを使用すると、失敗した時点から公開操作を再トリガできます。

前提条件

イメージは、一部公開済み、失敗、または利用可能の状態である必要があります。

手順

1 Horizon Universal Console の [ホーム] ページで、[イメージ] をクリックします。

2 [イメージ] ページで、失敗したイメージのリンクをクリックします。

3 失敗したイメージを選択し、[公開] をクリックします。

4 [イメージを再公開] ページで、イメージの公開に失敗した Horizon Edge は自動的に選択され、選択解除することはできません。[再公開] をクリックします。

リモート デスクトップへのアプリケーションのスキャン

イメージ管理プロセスでアプリケーションをスキャンできます。

前提条件

- Edge Gateway の準備が完了していること。
- イメージが正常に公開されていること。
- プロバイダに少なくとも 1 つの仮想ネットワークとテナント（デスクトップ）サブネットが選択されている。

手順

1 Horizon Universal Console の [ホーム] ページで、[イメージ] をクリックします。

2 [イメージ] ページで、イメージ リンクをクリックしてイメージ バージョン ページに移動します。

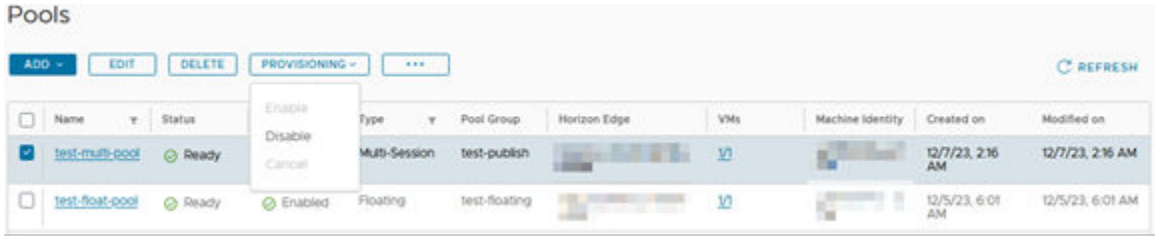
3 スキャンするイメージ バージョンの名前を選択し、 [公開済み] - [アプリケーションのスキャン] をクリックします。

4 スキャンをトリガするネットワークを選択します。

5 [保存] をクリックしてスキャンを開始します。

プール プロビジョニングの管理

[プールを追加] ワークフローを完了して Microsoft Azure Edge のプールを作成すると、システムはそのプールの仮想マシンのプロビジョニングを開始します。Horizon Universal Console 内のプールに対する仮想マシンのプロビジョニングを管理する方法は多数あります。たとえば、プールの構成方法に誤りがあったことに気づいた場合は、プロビジョニングが完了するのを待たずに、プールをキャンセルできます。その他のオプションも使用できます。



プール プロビジョニングの再試行

このタスクは、[プール] ページでプールのステータスが「エラー」と表示されている場合に実行できます。

このタスクを実行する理由

Horizon Universal Console がプールのプロビジョニング エラーの解決を支援できるようにし、プールのプロビジョニングを再度試行できるようにします。

このタスクを実行する方法

プール プロビジョニングの再試行を参照してください。

プール プロビジョニングのキャンセル

このタスクを実行する理由

非常に長い時間がかかる場合があるプールのプロビジョニング プロセスを停止することで時間を節約します。プールのプロビジョニング方法に誤りがあることに気付く場合があります。プールのプロビジョニングをキャンセルし、構成の問題の修正を試みて、プールを再プロビジョニングすることができます。

このタスクを実行する方法

[プール] ページで、プールに「拡張中」のステータスが表示されているときに、[プロビジョニング] - [キャンセル] を選択します。

結果

仮想マシンのプロビジョニングがすぐに停止し、プールのステータスが「部分的にプロビジョニング済み」、「準備完了」、「エラー」などに変わります。プロビジョニングまたはカスタマイズが進行中の仮想マシンが削除されます。

プール プロビジョニングの無効化

このタスクを実行する理由

新しい仮想マシンが特定のプールでプロビジョニングされないようにします。このオプションを使用すると、[有効にする] オプションを使用してプロビジョニングが再度有効になるまで、そのプール上の仮想マシンのプロビジョニングを明示的に防止できます。

このタスクを実行する方法

[プール] ページで、プール プロビジョニングが [有効] として表示されているときに、[プロビジョニング] - [無効にする] を選択します。

結果

新しい仮想マシンのプロビジョニングが停止し、プールのステータスが「部分的にプロビジョニング済み」、「準備完了」、「エラー」などに変わります。このオプションを実装すると、プロビジョニングまたはカスタマイズが進行中の仮想マシンは処理を続行します。

プール プロビジョニングの有効化

このタスクを実行する理由

プールを拡張または縮小できるようにします。このオプションを使用すると、必要に応じて拡張および縮小するために、プールでの仮想マシンのプロビジョニングを明示的に許可できます。

このタスクを実行する方法

[プール] ページで、プール プロビジョニングが [無効] として表示されている場合は、プールのプロビジョニングを有効にしてプールの拡張または縮小を開始できるようにすることができます。[プロビジョニング] - [有効にする] を選択します。

結果

プールは、必要に応じて拡張または縮小を開始します。

プールの作成

Horizon Universal Console に少なくとも 1 つのイメージが表示されたら、そのイメージに基づいてプールを作成できます。

前提条件

プールを作成する前に、システムでは、next-gen 環境で次の項目が構成されている必要があります。これらの項目が適切に構成されていることを確認します。

- エンドユーザー ID プロバイダ - エンドユーザー ID に使用する ID プロバイダが構成されていることを確認します。背景については、「Horizon Cloud Service - next-gen 環境での ID とアクセス管理」を参照してください。
  - Microsoft Entra ID をエンドユーザー ID の ID プロバイダとして使用する場合は、Microsoft Entra ID Connect の構成が完了していることを確認してください。

- マシン ID プロバイダ - マシン ID プロバイダの構成が適切であることを確認します。このプロバイダは、リモート デスクトップとアプリケーションを提供する仮想マシンのマシン ID を確立します。
  - エンドユーザー ID に Microsoft Entra ID を使用している場合、それをマシン ID に使用することも、代わりに Active Directory ドメインをマシン ID に使用することもできます。

    注： マシン ID に Microsoft Entra ID を使用している場合、Microsoft Entra ID に参加しているプールまたは仮想マシンを削除するには、プールまたは仮想マシンを削除するときに Microsoft Entra ID からデバイス エントリを削除するため、プールの指定されたプロバイダに特定の権限が必要であることに注意してください。

    必要な権限は次のとおりです。

    ```
    Scope: Microsoft Graph https://graph.microsoft.com/
    Permission : Device.ReadWrite.All Read and write devices
    Admin Consent Required: Yes
    ```

    Azure ポータルを使用してアプリケーションの権限をプロバイダのサービス プリンシパルに追加するには、[アプリケーション登録] に移動し、サービス プリンシパルのアプリケーション登録を選択し、Azure ポータルの [API 権限] ユーザー インターフェイスを使用して [Microsoft Graph] アプリケーションの権限 `Device.ReadWrite.All` を追加します。
  - マシン ID に Active Directory ドメインを使用する場合は、Active Directory ドメインが構成されていることを確認してください。背景については、「Active Directory ドメインの設定」を参照してください。

    注： エンドユーザー ID に Workspace ONE Access を使用する場合は、マシン ID に使用する Active Directory ドメインを構成する必要があります。
- Horizon Edge が正常に作成され、Horizon Edge Gateway と UAG のデプロイが Horizon Universal Console の [リソース] - [キャパシティ] - [Horizon Edge] に健全な（緑色）状態で表示されていることを確認します。
- このプールで使用する VDI またはマルチセッション イメージが正常に公開されていることを確認します。イメージの状態は、Horizon Universal Console の [リソース] - [イメージ] で確認できます。

手順

1. Horizon Universal Console で、[リソース] - [プール] をクリックして [プール] ページに移動します。
2. [追加] - [Microsoft Azure] をクリックして、プール作成ウィザードを開始します。
3. [プールの追加] ウィザードの [プール名] フィールドにプールの一意の名前を入力し、必要に応じて [説明] を追加します。
4. プール タイプを選択します。
   - [専用単一セッション]：各デスクトップが単一のユーザーにマッピングされるパーシステントな VDI デスクトップ エクスペリエンスの場合。

- [フローティング単一セッション]：複数のユーザーが異なる時間にデスクトップを使用でき、ユーザー セッションごとにデスクトップがリセットされる非パーシステントな VDI デスクトップ エクスペリエンスの場合。
- [マルチセッション]：セッションベースで公開されたデスクトップおよびアプリケーションの場合。

プール タイプを選択すると、後続のウィザード セクションに、選択したプール タイプに適した選択肢が自動的に表示されます。

5 [デスクトップ] セクションの [宛先] サブセクションで、[サイト]、[Horizon Edge]、[プロバイダ] オプションの値を選択します。

6 また、[宛先] サブセクションで Azure アベイラビリティ ゾーンを使用する場合は、[Azure アベイラビリティ ゾーンの使用] オプションを有効にします。

Azure アベイラビリティ ゾーンは、Microsoft Azure で使用可能な高可用性機能です。[Azure アベイラビリティ ゾーンの使用] を選択するとプールの仮想マシンがすべてのアベイラビリティ ゾーンに分散され、特定の Azure アベイラビリティ ゾーンで障害が発生した場合にプール内のすべての仮想マシンのダウンタイムを回避できます。

注： Azure アベイラビリティ ゾーンのサポートの制限については、次の Microsoft のドキュメントを参照してください。

7 [イメージ] サブセクションで、このプールの [生成タイプ] オプションと [イメージ] オプションを選択します。

注：

- Microsoft Azure 第 1 世代および第 2 世代の仮想マシンを使用したイメージがサポートされています。
- [V1] を選択すると、Microsoft Azure 第 1 世代の仮想マシンと第 1 世代をサポートするモデルを使用したイメージのみを選択できます。
- [世代タイプ] の選択はフィルタとして機能し、[イメージ] ドロップダウン メニューに表示されるイメージと、[モデル] ドロップダウン メニューに表示されるモデルを決定します。

8 選択したイメージの [マーカー] を選択します。

イメージ バージョンのプールを後で編集するには、1 つ以上のマーカーを追加する必要があります。以前にイメージ バージョンに追加されていない場合は、マーカーを追加します。詳細については、既存の Microsoft Azure Compute Gallery イメージへのバージョンの追加を参照してください。

注： 古いエージェント バージョンに関連付けられているマーカーが選択されている場合は、警告メッセージが表示されます。ベスト プラクティスとして、最新のエージェント バージョンを含むマーカーを選択します。

9 [この Windows OS に対する有効なライセンスを持っていますか] の横にあるトグルをスライドして、この Azure Hybrid Benefit を適用するためのソフトウェア アシュアランスを備えた適格な Windows ライセンスまたは Windows Server サブスクリプションがあることを確認し、[チェックボックス]を選択します。

10 [仮想マシンの詳細] サブセクションで、プールの [モデルのフィルタリング]、[モデル]、[ディスク タイプ]、[ディスク サイズ]、[ディスクの暗号化] オプションの値を選択します。

注： [モデル] 設定については、ナレッジベースの記事「Horizon Cloud Service - next-gen の Microsoft Azure 仮想マシンのタイプとサイズ (89090)」を参照し、Microsoft Azure 仮想マシンのさまざまなタイプとサイズと next-gen 環境との互換性を確認してください。

- [モデルのフィルタリング] 設定を使用すると、[モデル] 設定を構成するときに表示される Microsoft Azure 仮想マシン モデルのオプションの数を減らすことができます。削減されたリストには、特定の要件に基づくモデルのサブセットが含まれます。

  Microsoft Azure 仮想マシン モデルのリストは、[タグ]、[シリーズ]、[GPU タイプ]、[ディスク タイプ] でフィルタリングできます。他のフィルタを追加するには、[+] をクリックします。各フィルタを使用してリストをさらに絞り込むことができます。

[タグ]	等しい	■ [VMware 推奨] は、プールに特に適している Microsoft Azure 仮想マシン モデルを示します。 ■ [高パフォーマンス] は、優れたディスク サポートを提供する Microsoft Azure 仮想マシン モデルです。
[シリーズ]	等しい	ドロップダウン メニューを使用して、さまざまな Microsoft Azure 仮想マシン シリーズのリストを表示します。 ニーズに最適なシリーズを選択します。
[GPU タイプ]	等しい	[GPU タイプ] フィルタを使用して、GPU 対応の Microsoft Azure 仮想マシン モデルを選択できます。 ■ [なし] は、GPU 対応モデルをリストからフィルタリングします。 ■ [AMD] は、AMD GPU 対応モデルのみをリストに含めます。 ■ [NVIDIA] は、Nvidia GPU 対応モデルのみをリストに含めます。
[ディスク タイプ]	等しい	[ディスク タイプ] フィルタを使用して、優れたディスク サポートを提供する [プレミアム] を選択できます。

- プールに使用する Microsoft Azure 仮想マシンの [モデル] タイプを選択するか、デフォルトを受け入れます。

  1 デフォルト モデルを受け入れるには、リストされているデフォルトを選択するか、ドロップダウン メニューを使用して別のデフォルト モデルを選択します。

  2 別のモデルを選択するには、[X] をクリックし、ドロップダウン メニューをクリックしてモデルを選択します。

  [モデルのフィルタリング] 設定を使用していない場合、モデルのリストは非常に長くなります。[モデルのフィルタリング] 設定を使用した場合、リストはより管理しやすくなります。

- 選択した仮想マシン モデル、および Microsoft Azure サブスクリプションとリージョンに基づいて、[ディスク タイプ] の値を選択できます。
- [ディスク サイズ] の値は 127 ～ 4095 GB の間で変更できます。デフォルトの [ディスク サイズ] の値は 127 です。
- このプール内のすべての仮想マシンのディスクを暗号化する場合は、トグルを [ディスクの暗号化] にスライドします。

11 [マシン ID (ドメイン)] サブセクションで、このプールに使用する [マシン ID] プロバイダを選択します。

選択肢は次のとおりです。

- マシン ID を提供する目的で next-gen 環境に構成された Active Directory ドメイン。この選択により、デフォルトの `CN=Computers` 組織単位 (OU) を、その Active Directory ドメイン内にプールのマシンが作成される特定の [コンピュータの OU] に置き換えることができます。デフォルトでは、プールのマシンは `CN=Computers` に作成されます。
- [Azure Active Directory] の選択。[Azure Active Directory] を選択すると、システムはコンピュータの OU を使用しないため、[コンピュータの OU] フィールドが無効になります。

  プールのマシン ID に [Azure Active Directory] を使用する場合は、[Azure Active Directory] に RBAC を構成して、[仮想マシン管理者ログイン] または [仮想マシン ユーザー ログイン] ロールを持つユーザーまたはユーザー グループのみが資格にログインできるようにする必要があります。

  リソース グループ レベルで RBAC を構成すると、Azure Active Directory に参加したプールに関連付けられているリソース グループを特定しやすくなるために、プールのリソース グループに対して次のタグが使用されます。

  - [pool-name]：プールの作成時に入力したプール名を示します。
  - [add-joined]：[true] に設定されている場合、プールの仮想マシンが Microsoft Entra ID に参加しているマシンであることを示します。

注： Windows 11 および Windows 10 デバイスはすべてサポートされます。ただし、Windows Server 2019 Home エディションと、Azure で実行されている新しい仮想マシンを除きます（サーバ コアはサポートされていません）。

12 [プロビジョニング] サブセクションで、必要に応じて設定を構成します。

a [仮想マシンのプロビジョニング] サブセクションで、[オンデマンド] と [一度にすべて] の間で仮想マシンをプロビジョニングする方法を選択します。

b このプール用にプロビジョニングできる [仮想マシンの最大数] を入力します。

c [オンデマンド] オプションが選択されている場合は、[スペア仮想マシンの最小数] と [スペア仮想マシンの最大数] の数を選択します。

13 [プロパティ] サブセクションで次の項目を指定します。

- [仮想マシン名のプリフィックス]：プールの仮想マシンに使用するプリフィックスを入力します。
- [仮想マシン名の再利用]：このオプションは、仮想マシンの削除後に仮想マシン名を再利用するように指定します。
- [デスクトップ管理者のユーザー名] と [デスクトップ管理者のパスワード]：イメージのオペレーティング システムへのアクセス、およびイメージ変換プロセスで使用されるローカル管理者アカウントの認証情報を入力します。
- [送信プロキシを使用]：プロキシ サーバを介してインターネットへの送信要求をルーティング場合は、このトグルをスライドできます。

14 [次へ] をクリックして、次のセクションに進みます。

15 [ネットワーク] サブセクションで、仮想ネットワークとテナント（デスクトップ）サブネットを選択します。

デフォルトでは、仮想デスクトップは IPv4 アドレスを使用します。仮想マシンで IPv4 アドレスと IPv6 アドレスを使用する場合は、[デュアル スタック サポートを有効にする] オプションを有効にしてデュアル スタックとして構成されているサブネットを選択します。

注： デュアル スタック オプションを有効にすると、デュアル スタックとして構成されているサブネットのみが一覧表示されます。

16 [VMware Dynamic Environment Manager] サブセクションでは、必要に応じて、このプールの VMware Dynamic Environment Manager 構成を選択できます。

17 [保存] をクリックして、新しく作成したプールを環境に保存します。

[保存] をクリックすると、この新しいプールを新しいプール グループに追加するか、既存のプール グループに追加するか、そのタスクの実行を延期するフローを開始するオプションが表示されます。

- [プール グループに追加]：このボタンをクリックすると、新しいプールを既存のプール グループに追加するフローが開始され、このプールが追加される新しいプール グループを作成するオプションも選択できます。
- [終了]：プール グループにプールを追加するタスクを延期するには、このボタンをクリックします。[終了] をクリックすると、新しく作成されたプールがリストされた [プール] ページに戻ります。[プール] ページで、プールを選択し、[...] - [プール グループに追加] をクリックすることで、プールをプール グループに追加できます。

18 プール作成ウィザードの最後で [プール グループに追加] をクリックすると、システムはプールをプール グループに追加するためのウィザードを開始します。

システムは、追加するプールのタイプに基づいて選択されたプール グループのタイプでフローを自動的に開始します。

この [プール グループに追加] フローの詳細については、「単一セッション プール グループの作成」または「マルチセッション プール グループの作成」を参照してください。

プール グループにプールが関連付けられていない場合は、プールを選択し、[プール グループに追加] をクリックしてプール グループに追加することもできます。

結果

[プール] ページにプールが表示されたら、ページのユーザー インターフェイス要素を使用して、プールの定義の編集やプールの削除などのアクションをプールに対して実行できます。

プール グループが関連付けられていないプールの場合は、プールを選択して [...] - [プール グループに追加] をクリックすることで、プール グループにプールを追加できます。

次のステップ

- プールのプロビジョニングを監視し、必要に応じてアクションを実行します。プール プロビジョニングの管理を参照してください。
- プール グループを作成します。プール グループの作成を参照してください。

プール グループの作成

プール グループを使用すると、デスクトップおよびアプリケーションの使用資格をいつでも任意のユーザーまたはグループに付与できます。単一セッション プールまたはマルチセッション プールを作成できます。

単一セッション プール グループの作成

プール グループを使用すると、デスクトップおよびアプリケーションの使用資格をいつでも任意のユーザーまたはグループに付与できます。Horizon Cloud Service - next-gen を使用して、任意のプロバイダのプールとポリシーを含む単一セッションを作成できます。

手順

1 [ホーム] ページで、[プール グループ] タイルをクリックして、[プール グループ] ページに移動します。

2 [追加] をクリックして [単一セッション プール グループの追加] を選択します。

3 [単一セッション プール グループの追加] ページで、一意のプールの [名前] を入力します。

4 [表示名] および [説明] を追加します。

[表示名] は、Horizon Client でエンド ユーザーに表示する名前です。64 文字以下にする必要があります。空白のままにすると、プール グループ名がデフォルトで使用されます。

5 [プール グループ タイプ] を選択します。単一ユーザーにマッピングされたパーシステント VDI デスクトップ環境の場合は [専用]、各セッションの後にリセットされ、複数のユーザーが異なる時間に使用できる非パーシステント VDI デスクトップ環境の場合は [フローティング] を選択します。

6 [プール] からプールを選択し、[次へ] をクリックします。

7 [App Volumes アプリケーション] セクションで、フローティング デスクトップで使用できるようにする App Volumes アプリケーションを選択します。[次へ] をクリックします。

プール グループ レベルで選択した App Volumes アプリケーションは、フローティング仮想マシンに配信されます。この割り当ては、資格（ユーザー/ユーザー グループ）レベルでの App Volumes アプリケーションの割り当てに加えて行われます。

注：

- App Volumes アプリケーションを選択して、[フローティング デスクトップ] のデスクトップのみで使用できるようにすることができます。これは、[専用デスクトップ] には使用できません。
- App Volumes アプリケーションを配信するには、App Volumes Agent をプール イメージにインストールし、アプリケーション パッケージを Horizon Edge で使用できるようにする必要があります。
- アプリケーション パッケージを同じリージョン内の仮想マシンに配信するには、そのリージョンでアプリケーション パッケージを利用できる必要があります。
- キャプチャされたパッケージのないアプリケーションは選択できません。このチェックボックスは無効になり、選択できません。

8 [アプリケーションの詳細] セクションで、各アプリケーションのパッケージを選択します。

9 プール グループとユーザー/ユーザー グループ資格により、ユーザーに同じアプリケーションのさまざまなパッケージを使用する資格が付与されている場合は、[競合の優先順位] に対して [プール グループ] と [ユーザー/ユーザー グループ資格] のどちらかを選択して、配信するパッケージを選択します。[次へ] をクリックします。

10 デフォルトの [クライアント] 設定の [ポリシー] セクションで、エンド ユーザー セッションの [デフォルトのプロトコル] を選択します。

ユーザーがデスクトップにログインするときにプロトコルを選択できるようにするには、[ユーザーによるプロトコル選択を許可] トグルをスライドします。

11 [優先クライアントのタイプ] を選択して、[Horizon Client] または [ブラウザ] で資格を起動します。

12 [専用] プール グループの場合は、[割り当て済みのマシン名を表示] を選択します。

[割り当て済みのマシン名を表示] を選択すると、Horizon Client にログインする際に、プール グループの表示名ではなく、割り当てられたマシンのホスト名が表示されます。

ユーザーにプール グループ内の複数のマシンが割り当てられている場合、割り当てられたマシン名は常に表示されます。この機能は、[フローティング] プール グループでは使用できません。

13 [仲介] サブセクションで、使用可能なデスクトップを検索する [範囲]（[任意のサイト] または [1 つのサイトに制限]）を選択します。

14 [サイト接続のアフィニティ] フィールドで、エンド ユーザーが接続するデフォルト サイトを [最も近いサイト] および [ホーム サイト] から選択します。

[ホーム サイト制限] トグルをスライドして、エンド ユーザーまたはユーザー グループの資格へのアクセスを制限できます。すなわち、資格のホーム サイトの上書きを介してのみ、または上書きが指定されていない場合はユーザーのホーム サイトを介してのみアクセスできるようにします。選択しない場合は、最も近いサイトが使用されます。

15 [SSO] サブセクションで、トグルをスライドしてプールの SSO を有効にできます。

Horizon Cloud が Horizon Edge Gateway でサポートされる SSO タイプのいずれかを構成するための前提条件が揃っていて、その SSO タイプのすべての要件を満たしている必要があります。構成された SSO タイプに必要な前提条件を満たしていない場合、エンド ユーザーは認証情報の入力を求められます。

16 [電源管理] セクションの [専用] [プール グループ タイプ] で、[未使用の仮想マシン] のしきい値を指定します。これは、任意の時点でのプール グループ内の仮想マシンの仮想マシン合計数に対するパワーオンにしておく仮想マシンの最小数です。

未使用の仮想マシンとは、プロビジョニングされ、パワーオンされているが、ユーザーがログインしていない仮想マシンのことです。この設定は、電源管理スケジュールを指定しない限り、資格内の各プール グループに適用されます。

17 [パワーオフ保護時間] フィールドに、ヘッドルーム エラーが原因でパワーオン後に仮想マシンがパワーオフしないように保護される時間（分単位、1 ～ 60）を追加します。デフォルトは 30 です。

18 [フローティング] [プール グループ タイプ] の [電源管理] セクションで、[電源管理タイプ] を [占有率ベース] と [占有率ベース以外] から選択します。

19 [占有率ベース] の場合、この資格の仮想マシン使用率のしきい値を、[電源管理モード] フィールドの [パフォーマンスの最適化]、[バランシング済み]、および [コストの最適化] から選択します。しきい値に達すると、新しい仮想マシンがスピン アップしてドレイン状態になります。

[パフォーマンスの最適化] を選択すると、新しい仮想マシンはすぐにスピン アップして、キャパシティを容易に利用できるようになり、可能な範囲で向上したユーザー エクスペリエンスを得られます。

[コストの最適化] を選択すると、新しい仮想マシンが起動するまでに仮想マシンはより高い使用率に達するため、コストを最小化できます。

20 任意の時点でのプール グループ内の仮想マシンの合計に対する、パワーオン状態を維持する仮想マシンの最小割合を示す [仮想マシンの最小数] を追加します。

この設定は、電源管理スケジュールを指定しない限り、資格内の各プール グループに適用されます。

21 [パワーオフ保護時間] フィールドに時間（分単位、1 ～ 60）を追加します。

仮想マシンは、パワーオンした後、ヘッドルーム エラーによるパワーオフから保護されます。デフォルトは 30 です。

22 [占有率ベース以外] で、[未使用の仮想マシン] のしきい値を指定します。これは、任意の時点でのプール グループ内の仮想マシンの合計数です。

未使用の仮想マシンとは、プロビジョニングされ、パワーオンされているが、ユーザーがログインしていない仮想マシンのことです。この設定は、電源管理スケジュールを指定しない限り、資格内の各プール グループに適用されます。

23 [パワーオフ保護時間] フィールドに時間（分単位、1 ～ 60）を追加します。

仮想マシンは、パワーオンした後、ヘッドルーム エラーによるパワーオフから保護されます。デフォルトは 30 です。

24 [スケジュールの追加] をクリックして情報を追加し、[電源管理スケジュール] を追加することもできます。

25 [タイムアウト処理] セクションで、[切断されたセッションからログアウト] フィールドで、切断されたセッションがいつログアウトされるかを決定します。[なし]、[ただちに] または [次の時間後にログアウト] から選択します。

[切断されたセッションからログアウト] のデフォルトは [なし] です。[次の時間後にログアウト] を選択した場合は、切断されたセッションがログアウトされるまでのタイムアウトを指定します。

[次の時間後にログアウト] のデフォルト値は 120 分です。[空のセッションがタイムアウトになるまでの時間 (分)] で [なし] と [タイムアウトまでの時間] を選択し、空のセッションがタイムアウトになるまでの時間を分単位で追加します。

空のアプリケーション セッションでタイムアウトが発生した場合の操作として、[ログオフ] または [切断] を選択します。切断されたセッションがログオフされると、セッションは失われます。

[セッションの最大有効期間] フィールドにセッションの最大時間（分）を入力します。[セッションの最大有効期間] のデフォルト値は 10080 分です。

[アイドル セッションのタイムアウト] フィールドで、システムが強制的に切断するまでにユーザーがアイドル セッションを維持できる時間を入力します。[アイドル セッションのタイムアウト] のデフォルト値は 10080 分です。

26 [保存] をクリックします。

27 [プール グループの資格を付与] をクリックして、このプール グループの使用資格をユーザーまたはユーザー グループに今すぐ付与するか、[終了] をクリックして後で資格を付与します。

マルチセッション プール グループの作成

プールを使用すると、デスクトップおよびアプリケーションの使用資格をいつでも任意のユーザーまたはグループに付与できます。任意のプロバイダのプールとポリシーを含むマルチセッション プールを作成できます。

手順

1 [ホーム] ページで、[プール グループ] タイルをクリックして、[プール グループ] ページに移動します。

2 [追加] をクリックして、[マルチセッション] プール グループを選択します。

3 [マルチセッション プール グループの追加] ページで、一意のプール グループの [名前] を入力します。

4 [表示名] および [説明] を追加します。

[表示名] は、Horizon Client でエンド ユーザーに表示する名前です。64 文字以下にする必要があります。空白のままにすると、プール名がデフォルトで使用されます。

5 [公開デスクトップ]、[公開アプリケーション]、および [公開デスクトップとアプリケーション] から [プール グループ タイプ] を選択します。

6 [公開デスクトップ] の場合は、[プール] からプールを選択して [次へ] をクリックします。[ポリシー] の場合は、手順 11 に進みます。

7 [手動アプリケーション] セクションで [追加] をクリックして、新しい手動アプリケーションを作成します。

8 [手動アプリケーションの追加] モーダル ウィンドウで、アプリケーションの [名前] を追加し、オプションで [参照] をクリックして [アイコン ファイル] を参照し、アイコンを追加します。アプリケーションの [パス]、[バージョン]、および [公開者] を追加します。必要に応じて、[すべてのプール] と [カスタム] の間のパラメータを選択し、アプリケーション パラメータを追加し、オプションで [開始フォルダ] を追加します。

9 プール グループで公開アプリケーションとして使用できるようにする手動アプリケーションを選択します。[次へ] をクリックします。リスト内のアプリケーション名の横にある 3 つのドットをクリックして、アプリケーションを [編集] および [削除] することもできます。

10 [アプリケーションの属性] セクションでは、必要に応じて、選択したアプリケーションのアプリケーション属性を指定できます。デフォルトでは、マルチセッション モードは無効になっています。アプリケーションのマルチセッション モードを編集できます。

11 デフォルトの [クライアント] 設定の [ポリシー] セクションで、エンド ユーザー セッションの [デフォルトのプロトコル] を選択します。

ユーザーがデスクトップにログインするときにプロトコルを選択できるようにするには、[ユーザーによるプロトコル選択を許可] トグルをスライドします。

12 [優先クライアントのタイプ] を選択して、[Horizon Client] または [ブラウザ] で資格を起動します。

13 [仲介] サブセクションで、使用可能なデスクトップを検索する [範囲]（[任意のサイト] または [1 つのサイトに制限]）を選択します。

14 [サイト接続のアフィニティ] フィールドで、エンド ユーザーが接続するデフォルト サイトを [最も近いサイト] および [ホーム サイト] から選択します。

[ホーム サイト制限] トグルをスライドして、エンド ユーザーまたはユーザー グループの資格へのアクセスを制限できます。すなわち、資格のホーム サイトの上書きを介してのみ、または上書きが指定されていない場合はユーザーのホーム サイトを介してのみアクセスできるようにします。選択しない場合は、最も近いサイトが使用されます。

15 [SSO] サブセクションで、トグルをスライドしてプールの SSO を有効にできます。

Horizon Cloud が Horizon Edge Gateway でサポートされる SSO タイプのいずれかを構成するための前提条件が揃っていて、その SSO タイプのすべての要件を満たしている必要があります。構成された SSO タイプに必要な前提条件を満たしていない場合、エンド ユーザーは認証情報の入力を求められます。

16 [電源管理] セクションで、[電源管理タイプ]に、[占有率ベース以外] と [占有率ベース以外] を選択します。[占有率ベース] は、プール占有率の負荷に基づいて消費電力を最適化します。[占有率ベース以外] は、プロビジョニングされた仮想マシンの合計数に対するパワーオンされた未使用の仮想マシンの数に基づいて消費電力を最適化します。

17 [占有率ベース] で、この資格の仮想マシン使用率のしきい値を、[電源管理モード] フィールドの [パフォーマンスの最適化]、[バランシング済み]、および [コストの最適化] から選択します。しきい値に達すると、新しい仮想マシンがスピン アップしてドレイン状態になります。モード。

[パフォーマンスの最適化] を選択すると、新しい仮想マシンはすぐにスピン アップして、キャパシティを容易に利用できるようになり、可能な範囲で向上したユーザー エクスペリエンスを得られます。[コストの最適化] を選択すると、新しい仮想マシンが起動するまでに仮想マシンはより高い使用率に達するため、コストを最小化できます。

18 任意の時点でのプール グループ内の仮想マシンの合計に対する、パワーオン状態を維持する仮想マシンの最小割合を示す [仮想マシンの最小数] を追加します。

この設定は、電源管理スケジュールを指定しない限り、資格内の各プール グループに適用されます。

19 [パワーオフ保護時間] に時間（分単位、1 ～ 60）を追加します。

仮想マシンは、パワーオンした後、ヘッドルーム エラーによるパワーオフから保護されます。デフォルトは 30 です。

20 [占有率ベース以外] で、[未使用の仮想マシン] のしきい値を指定します。これは、任意の時点でのプール グループ内の仮想マシンの合計数です。

未使用の仮想マシンとは、プロビジョニングされ、パワーオンされているが、ユーザーがログインしていない仮想マシンのことです。この設定は、電源管理スケジュールを指定しない限り、資格内の各プール グループに適用されます。

21 [パワーオフ保護時間] に時間（分単位、1 ～ 60）を追加します。

仮想マシンは、パワーオンした後、ヘッドルーム エラーによるパワーオフから保護されます。デフォルトは 30 です。

22 [スケジュールの追加] をクリックして情報を追加し、[電源管理スケジュール] を追加することもできます。

23 次のオプションの説明に基づいて、[ロード バランシング] セクションの入力を完了します。

注： 次の設定は、環境内で必要な電力消費とパフォーマンスのバランスを達成するのに役立ちます。

オプション	説明
[連続するセッション割り当て間の時間]	この設定により、新しいユーザー セッションが分散され、構成した期間内に仮想マシンに割り当てられるセッションの数が制限されます。たとえば、この設定が 20 秒で、ユーザーが直近 20 秒以内に VM1 に割り当てられている場合、次のユーザーは VM2 に割り当てられます。
[CPU 使用率]	CPU 使用率のしきい値 (%)。0 ～ 100 の値を設定できます。推奨値は 90 で、これはデフォルト値でもあります。
[メモリ使用率]	メモリ使用率のしきい値 (%)。0 ～ 100 の値を設定できます。推奨値は 90 で、これはデフォルト値でもあります。
[ディスク キュー長]	サンプリング時間中、選択されたディスクの再度キューに入った読み取り要求と書き込み要求の両方の平均数のしきい値。任意の正の整数を設定できます。デフォルトでは、この設定はロード バランシングで考慮されません。デフォルト値は 0 です。
[ディスクの読み取り遅延]	ディスクからのデータ読み取りの平均時間のしきい値（ミリ秒）。任意の正の整数を設定できます。デフォルトでは、この設定はロード バランシングで考慮されません。デフォルト値は 0 です。
[ディスクの書き込み遅延]	ディスクへのデータ書き込みの平均時間のしきい値（ミリ秒）。任意の正の整数を設定できます。デフォルトでは、この設定はロード バランシングで考慮されません。デフォルト値は 0 です。
[ホストのロード インデックス]	仮想マシンがいっぱいとみなされ、新しいセッションが割り当てられなくなるときの合計しきい値。値は 0 ～ 100 の範囲で入力できます。デフォルト値は 90 です。値は、CPU、メモリ、ディスクの使用率をそれぞれのしきい値と比較して計算されます。使用率がしきい値と比較して最も高いリソースには、最も大きい値が重み付けされます。

24 [ローリング メンテナンス] セクションで [ローリング メンテナンスを有効にする] と、可用性を維持するために複数セッション仮想マシンの自動更新が提供されます。これにより、キャッシュされたリソースまたはメモリ リークがクリアされ、エンドユーザー セッションの問題を回避できます。

25 [メンテナンス タイプ] を [スケジュール設定済み] にするか、[セッション] にするかを選択します。

ローリング メンテナンスで仮想マシンの更新がトリガされます。スケジュール設定済みの場合は、入力するパラメータに応じて、更新は日単位か週単位でトリガされます。セッションの場合は、ログインしているセッションの数が入力した値に達したときに、更新がトリガされます。いずれの場合でも、エンド ユーザーがログオフするまで更新は発生しません。

26 仮想マシンの更新がスケジュール設定される頻度については、[繰り返し] のドロップダウンから [日単位] または [週単位] を選択します。

27 スケジュール設定された時間の設定に適した [タイム ゾーン] を選択します。

28 仮想マシンの更新がスケジュール設定される時間については、[スケジュール済み時間] を追加します。

29 メンテナンスのために同時に停止状態になることが可能な仮想マシンの数については、[プールあたりの同時静止仮想マシン数] の数を追加します。

このプロセスの進行中、仮想マシンはサービスを提供しますが、新しいセッションのためには使用できません。

30 メンテナンスが必要な仮想マシンについては、[仮想マシンのアクション] として [再起動] または [再構築] を選択します。

[再起動] を選択した場合、影響を受ける仮想マシンが再起動します。[再構築] を選択した場合、影響を受ける仮想マシンが削除され、最新のイメージを使用して再プロビジョニングされます。

31 [タイムアウト処理] セクションで、[切断されたセッションからログアウト] フィールドで、切断されたセッションがいつログアウトされるかを決定します。[なし]、[ただちに] または [次の時間後にログアウト] から選択します。[切断されたセッションからログアウト] のデフォルトは [なし] です。[次の時間後にログアウト] を選択した場合は、切断されたセッションがログアウトされるまでのタイムアウトを指定します。[次の時間後にログアウト] のデフォルト値は 120 分です。切断されたセッションがログオフされると、セッションは失われます。[セッションの最大有効期間] フィールドにセッションの最大時間（分）を入力します。[セッションの最大有効期間] のデフォルト値は 10080 分です。[アイドル セッションのタイムアウト] で、システムが強制的に切断するまでにユーザーがアイドル セッションを維持できる時間を入力します。[アイドル セッションのタイムアウト] のデフォルト値は 10080 分です。

[空のアプリケーション セッションのタイムアウト] で [なし] および [次の時間後にタイムアウト] から選択します。[空のアプリケーション セッションのタイムアウト] のデフォルトは [なし] です。ユーザーがアプリケーション セッションを実行していて、そのセッションで実行されているアプリケーションがない場合、そのセッションは空と見なされます。[次の時間後にタイムアウト] を選択した場合は、空のセッションがタイムアウトになるまでの時間を分単位で追加します。[次の時間後にタイムアウト] のデフォルト値は 1 分です。[タイムアウトの発生時] フィールドで、[ログアウト] と [切断] を選択します。[タイムアウトの発生時] のデフォルトは [ログアウト] で、切断せずにセッションがログアウトされます。[空のアプリケーション セッションのタイムアウト] 設定は、[公開アプリケーション] または [公開デスクトップとアプリケーション] セッションを選択した場合に適用され、[公開デスクトップ] には適用されません。

32 [保存] をクリックします。

33 [プール グループの資格を付与] をクリックして、このプール グループの使用資格をユーザーまたはユーザー グループに今すぐ付与するか、[終了] をクリックして後で資格を付与します。

プール グループ クライアントを直接接続のみとして構成する

Horizon Cloud Service - next-gen では、プール グループ クライアントを直接接続として構成できるため、内部 Horizon Client ユーザーは、Unified Access Gateway の外部 FQDN を使用することなく、デスクトップやエージェントなどの内部リソースに直接接続できます。

プール グループ内のクライアントがデスクトップやエージェントなどの内部リソースに直接接続し、Unified Access Gateway をバイパスすることを許可できます。プール グループの作成または編集中に [Direct Connect] オプションを指定できます。[Direct Connect] オプションは、任意のタイプのプール グループ（専用、フローティング、またはマルチセッション）で使用できます。

このオプションを構成するには、まず次の前提条件を満たす必要があります。

- 管理者として、プール グループの [Direct Connect] オプションを指定します。

  Horizon Universal Console で [リソース] - [プール グループ] をクリックし、[ポリシー] ステッパー ページの [クライアント] セクションで [直接接続のみ] オプションを有効にします。

- 管理者として、Direct Connect で使用できる内部ネットワーク範囲を指定します。

  Horizon Universal Console で、[設定] - [クライアントの設定] - [ネットワーク範囲] をクリックし、Direct Connect に使用できる内部ネットワーク範囲を指定します。

既存のプール グループを編集して Direct Connect を許可する例を次に示します。

1 Horizon Universal Console を開きます。

2 [リソース] - [プール グループ] をクリックします。

3 既存のプール グループを選択して、[編集] をクリックします。

4 [2.ポリシー] ページで、ページの [クライアント] セクションにある [直接接続のみ] トグル ボタンを有効にします。

[直接接続のみ] ボタンを有効にすると、[内部アクセスのみ] ボタンが自動的に有効になります。この設定は現在、[直接接続のみ] オプションとは別にアクセスすることはできません。詳細については、両方のボタンの説明ヘルプ テキストを参照してください。

5 [保存] をクリックします。

確認のために、プール グループのポリシーのサマリ ページで、[仲介] セクションの [直接接続のみ] オプションのステータスを表示できます。

このオプションは、エンド ユーザーに対して次のように表示されます。

- ユーザーが内部ユーザーではなく、構成された IP アドレス範囲の外部から接続している場合、[直接接続のみ] として構成されているプール グループの資格は表示されません。
- ユーザーが内部ユーザーの場合、[直接接続のみ] として構成されているプール グループの資格は、Unified Access Gateway の関与なしに起動されます。その他の資格は、Unified Access Gateway を使用して起動されます。

プール グループの作成に関する関連情報については、「単一セッション プール グループの作成」および「マルチセッション プール グループの作成」を参照してください。

プール プロビジョニングの再試行

単一セッションまたはマルチセッション プールのプロビジョニングが失敗した場合は、プロビジョニング プロセス中にプールで 1 つ以上のエラーが発生した可能性があります。エラーを解決して、プールのプロビジョニングを再試行できます。

プールのプロビジョニング エラーの具体的な例については、「Horizon Cloud Service - next-gen のプールの詳細」を参照してください。

手順

1 Horizon Universal Console にログインします。

2 [プール] タイルで [プール] をクリックします。

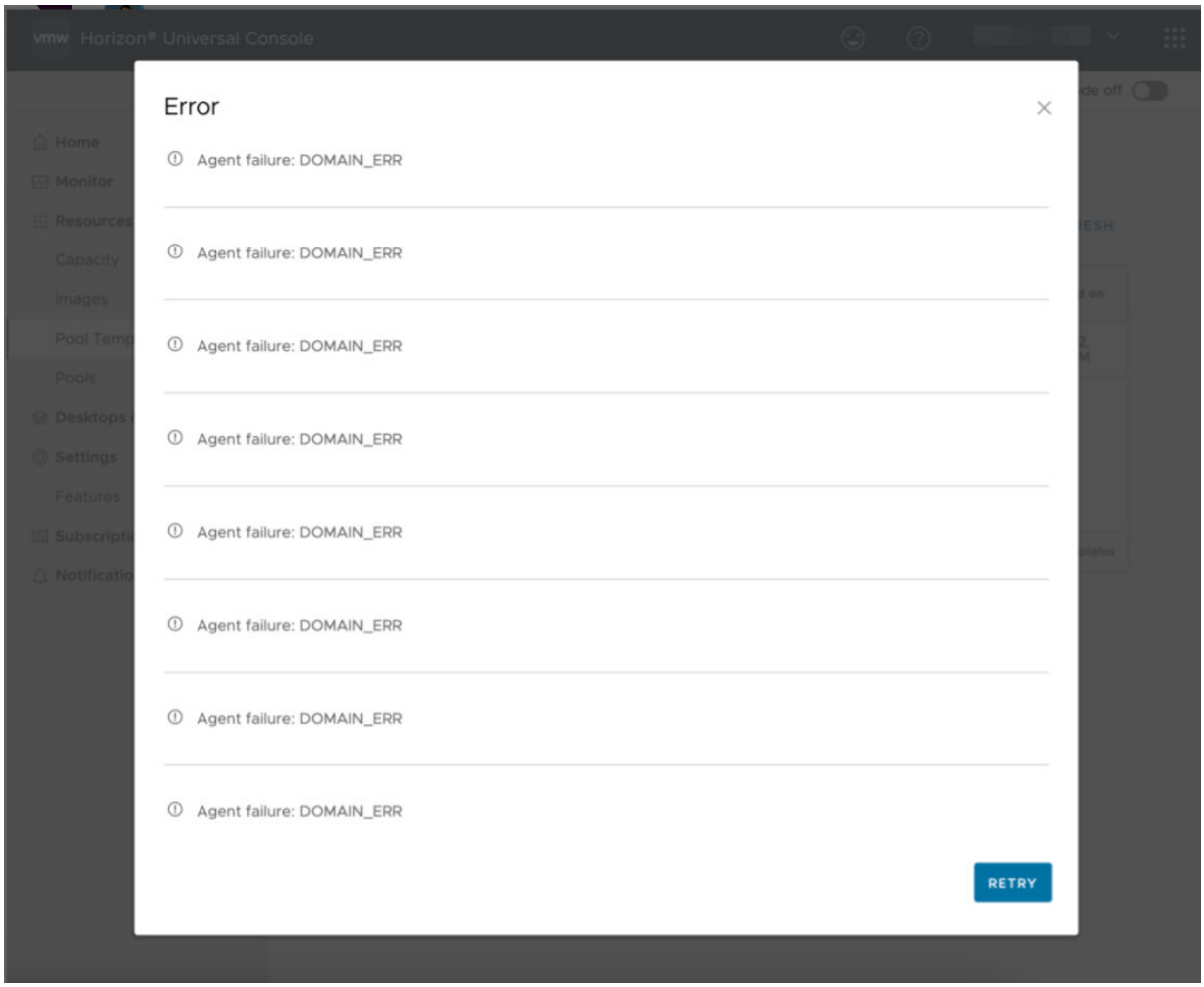
3 [プール] ページで、失敗したプールの [エラー] ステータスのツールチップをクリックします。

4 [すべてを表示] をクリックして、エラーの完全なリストを表示します。

3 つ以上のエラーがある場合は、[すべてを表示] ボタンが表示されます。

5 エラーを解決し、[再試行] をクリックします。

6 [ログの表示] をクリックして、[アクティビティ ログ] ページに移動します。



プールの編集

Horizon Universal Console を使用して環境のプールを編集します。

注： システムは、プールの構成内の特定のプロパティを変更するためにを提供します。更新できるプロパティについては、次の手順で説明します。プールの名前とそのタイプなど、プールの作成後にプールを編集するときに、構成された値の一部を変更することはできません。プールの作成中に指定できる項目の詳細については、「プールの作成」を参照してください。

手順

1 Horizon Universal Console で、[リソース] - [プール] をクリックして [プール] ページに移動します。

2 [プール] ページで編集するプールを選択し、[編集] をクリックします。

3 [プールの編集] セクションで、説明を更新できます。

このセクションでは、プールのタイプ(次のいずれかのタイプ)も示します。

- [専用単一セッション]: 各デスクトップが単一のユーザーにマッピングされるパーシステントな VDI デスクトップ エクスペリエンスの場合。

- [フローティング単一セッション]：複数のユーザーが異なる時間にデスクトップを使用でき、ユーザー セッションごとにデスクトップがリセットされる非パーシステントな VDI デスクトップ エクスペリエンスの場合。
- [マルチセッション]：セッションベースで公開されたデスクトップおよびアプリケーションの場合。

4 [デスクトップ] セクションの [送信先] サブセクションには、プールに構成されている [サイト]、[Horizon Edge]、[プロバイダ] が表示されます。これらの値は、既存のプールでは編集できません。

5 また、[宛先] サブセクションで Azure アベイラビリティ ゾーンを使用する場合は、[Azure アベイラビリティ ゾーンの使用] オプションを有効にします。

Azure アベイラビリティ ゾーンは、Microsoft Azure で使用可能な高可用性機能です。[Azure アベイラビリティ ゾーンの使用] を選択するとプールの仮想マシンがすべてのアベイラビリティ ゾーンに分散され、特定の Azure アベイラビリティ ゾーンで障害が発生した場合にプール内のすべての仮想マシンのダウンタイムを回避できます。

注：

- Azure アベイラビリティ ゾーンのサポートの制限については、次の Microsoft のドキュメントを参照してください。
- プールの編集時に Azure アベイラビリティ ゾーンを有効にすると、有効化後に作成された仮想マシンのみが Azure アベイラビリティ ゾーン全体に分散されます。既存の仮想マシンは移動されません。

6 [イメージ] サブセクションで、プールのイメージを別のイメージに変更するには、このプールの [世代タイプ] オプションと [イメージ] オプションを選択します。

注：

- Microsoft Azure 第 1 世代および第 2 世代の仮想マシンを使用したイメージがサポートされています。
- [V1] を選択すると、Microsoft Azure 第 1 世代の仮想マシンと第 1 世代をサポートするモデルを使用したイメージのみを選択できます。
- [世代タイプ] の選択はフィルタとして機能し、[イメージ] ドロップダウン メニューに表示されるイメージと、[モデル] ドロップダウン メニューに表示されるモデルを決定します。

7 選択したイメージの [マーカー] を選択します。

イメージ バージョンのプールを後で編集するには、1 つ以上のマーカーを追加する必要があります。以前にイメージ バージョンに追加されていない場合は、マーカーを追加します。詳細については、既存の Microsoft Azure Compute Gallery イメージへのバージョンの追加を参照してください。

注： 古いエージェント バージョンに関連付けられているマーカーが選択されている場合は、警告メッセージが表示されます。ベスト プラクティスとして、最新のエージェント バージョンを含むマーカーを選択します。

8 [この Windows OS に対する有効なライセンスを持っていますか] の横にあるトグルが有効であることを確認して、この Azure Hybrid Benefit を適用するためのソフトウェア アシュアランスを備えた適格な Windows ライセンスまたは Windows Server サブスクリプションがあることを確認し、確認のチェック ボックスを選択します。

9 [仮想マシンの詳細] サブセクションで、プールの [モデルのフィルタリング]、[モデル]、[ディスク タイプ]、[ディスク サイズ]、[ディスクの暗号化] オプションの値を選択します。

注： [モデル] 設定については、Horizon Cloud Service - next-gen の Microsoft Azure 仮想マシンのタイプとサイズ (89090)を参照し、Microsoft Azure 仮想マシンのさまざまなタイプとサイズと VMware Horizon Cloud Service - next-gen との互換性を確認してください。

- [モデルのフィルタリング] 設定を使用すると、[モデル] 設定を構成するときに表示される Microsoft Azure 仮想マシン モデルのオプションの数を減らすことができます。削減されたリストには、特定の要件に基づくモデルのサブセットが含まれます。

  Microsoft Azure 仮想マシン モデルのリストは、[タグ]、[シリーズ]、[GPU タイプ]、[ディスク タイプ] でフィルタリングできます。他のフィルタを追加するには、[+] をクリックします。各フィルタを使用してリストをさらに絞り込むことができます。

[タグ]	等しい	■ [VMware 推奨] は、プールに特に適している Microsoft Azure 仮想マシン モデルを示します。 ■ [高パフォーマンス] は、優れたディスク サポートを提供する Microsoft Azure 仮想マシン モデルです。
[シリーズ]	等しい	ドロップダウン メニューを使用して、さまざまな Microsoft Azure 仮想マシン シリーズのリストを表示します。 ニーズに最適なシリーズを選択します。
[GPU タイプ]	等しい	[GPU タイプ] フィルタを使用して、GPU 対応の Microsoft Azure 仮想マシン モデルを選択できます。 ■ [なし] は、GPU 対応モデルをリストからフィルタリングします。 ■ [AMD] は、AMD GPU 対応モデルのみをリストに含めます。 ■ [NVIDIA] は、Nvidia GPU 対応モデルのみをリストに含めます。
[ディスク タイプ]	等しい	[ディスク タイプ] フィルタを使用して、優れたディスク サポートを提供する [プレミアム] を選択できます。

- プールに使用する Microsoft Azure 仮想マシンの [モデル] タイプを選択するか、デフォルトを受け入れます。

  1 デフォルト モデルを受け入れるには、リストされているデフォルトを選択するか、ドロップダウン メニューを使用して別のデフォルト モデルを選択します。

  2 別のモデルを選択するには、[X] をクリックし、ドロップダウン メニューをクリックしてモデルを選択します。

  [モデルのフィルタリング] 設定を使用していない場合、モデルのリストは非常に長くなります。[モデルのフィルタリング] 設定を使用した場合、リストはより管理しやすくなります。

- 選択した仮想マシン モデル、および Microsoft Azure サブスクリプションとリージョンに基づいて、[ディスク タイプ] の値を選択できます。
- [ディスク サイズ] の値は 127 ～ 4095 GB の間で変更できます。デフォルトの [ディスク サイズ] の値は 127 です。
- このプール内のすべての仮想マシンのディスクを暗号化する場合は、トグルを [ディスクの暗号化] にスライドします。

10 [マシン ID (ドメイン)] サブセクションに、プールに構成されているマシン ID が表示されます。

この既存のプールがローカル Active Directory ドメインを使用するように構成されている場合は、必要に応じて、プールがマシン ID に使用する OU を変更できます。

注： 名前の競合を防ぐため、プールが仮想マシン名を再利用している場合、[コンピュータの組織単位 (OU)] フィールドの値は変更できません。[プロパティ] サブセクションの [仮想マシン名の再利用] オプションの表示状態は、プールが仮想マシン名を再利用しているかどうかを示します。

11 [プロビジョニング] サブセクションで、必要に応じて設定を更新します。

a プールのプロビジョニングが無効になっている場合は、[有効にする] をクリックして、プールのプロビジョニングを再度有効にすることができます。

このオプションは、このプールのプロビジョニングが以前に無効になっていた場合にのみ使用できます。これは、[プロビジョニング] - [無効にする] または [プロビジョニング] - [キャンセル] の選択で実行できます。

b [仮想マシンのプロビジョニング] サブセクションで、[オンデマンド] と [一度にすべて] の間で仮想マシンをプロビジョニングする方法の選択を変更できます。

c このプール用にプロビジョニングできる [仮想マシンの最大数] を変更できます。

d [オンデマンド] オプションが選択されている場合は、[スペア仮想マシンの最小数] と [スペア仮想マシンの最大数] の数を変更できます。

12 [プロパティ] サブセクションで、既存のプールを編集するときに次の項目を更新できます。

- [送信プロキシを使用] - プロキシ サーバを介して送信要求をインターネットにルーティングする場合は、このトグルを有効にして、プロキシ ホスト、プロキシ ポート、およびオプションのバイパス プロキシ IP アドレス（送信プロキシが適用されない IP アドレス）の値を指定します。

13 [次へ] をクリックして、次のセクションに進みます。

14 [ネットワーク] サブセクションで、仮想ネットワークとテナント（デスクトップ）サブネットを選択します。

注： デュアル スタック オプションは、プールを編集するときに変更できません。

15 [VMware Dynamic Environment Manager] サブセクションでは、必要に応じて、このプールの VMware Dynamic Environment Manager 構成を選択できます。

仮想デスクトップのサイズ変更

専用デスクトップ割り当てにある、すでに作成済みでデプロイされているデスクトップで Azure 仮想マシンのタイプとサイズを変更することで、個々の仮想デスクトップのサイズを変更できます。

手順

1 VMware Horizon® Cloud Service™ - next-gen にログインします。

2 [ホーム] ページで、[プール] をクリックします。

3 [プール] ページで、[専用プール] の [プール] の [仮想マシン] をクリックします。

4 [パワーオフ] [ステータス] でプロビジョニング済みの [仮想マシン] を 1 つ以上選択します。[編集] をクリックします。

5 ドロップダウン メニューから仮想マシン [モデル] を選択します。

6 [仮想マシンを編集] 画面で、ドロップダウンから [ディスク タイプ] を選択します。

[ディスク タイプ] のオプションは、選択した仮想マシン モデル、および Microsoft Azure サブスクリプションとリージョンに基づいています。

7 [ディスク サイズ] を変更します。使用できるディスク サイズは 127 GB から 4095 GB までです。デフォルトの ディスク サイズ は 127 です。[保存] をクリックします。

プール内のマルチセッション仮想マシンの電源管理とロード バランシング

Horizon Cloud Service - next-gen は、ロード バランシング設定に基づいてエージェント ロード インデックスを使用して、プール内のマルチセッション仮想マシンの電源管理とロード バランシングを行います。

Horizon Cloud Service - next-gen エージェントは、次のしきい値設定を使用してエージェント ロード インデックスを計算します。インデックス値は 0 ～ 100 の範囲で、各仮想マシンの負荷を測定するために使用されます。これらの設定は、プール グループ ポリシーを使用して構成します。

- CPU 使用率のしきい値
- メモリ使用率のしきい値
- ディスク キュー長のしきい値
- ディスクの読み取り遅延のしきい値
- ディスクの書き込み遅延のしきい値

電源管理とロード バランシングでエージェント ロード インデックスが重要な役割を果たすため、消費電力とパフォーマンスの最適なバランスを実現するには、適切な値を選択してください。

プール内の仮想マシン使用量に対するシステムの決定

システムは、次の 2 つの割合値のうちの高い方を選択することによって、特定のプールの仮想マシンの使用量を決定します。

- セッション占有率

  プール内のパワーオン状態の仮想マシンで可能なセッションの合計数で割ったプール内のアクティブなセッションの数。可能なセッション数は、プール内のパワーオン状態の仮想マシンの数に、プールに指定した仮想マシン 1 台あたりのセッション数の値を掛けて計算されます。

- 平均ロード インデックス

  上記で説明した、プール内のパワーオン状態の仮想マシンの平均エージェント ロード インデックス。

プール拡張の場合、システムは選択した平均ロード インデックス値を、電源管理設定に指定された高しきい値と比較します。

拡張を行うには、仮想マシンの最大数設定を 1 より大きくする必要があります。

次のいずれの例でも、[電源管理] 設定は [最適化されたパフォーマンス] です。最適化されたパフォーマンス設定の高しきい値は 50% です。つまり、使用率が 50% に到達すると、システムは未使用の仮想マシンの 1 つをパワーオンします。

例：セッション占有量が高しきい値を超えたためにプールを拡張

この例では、次の設定が使用されます。

- 仮想マシン 1 台あたりのセッション数 = 20
- 電源管理の高しきい値 = 50%

拡張前	拡張後
パワーオン状態の仮想マシン 仮想マシン 1 ■ 実行中のセッション数 = 10 ■ エージェント ロード インデックス = 25% **使用量値** ■ セッション占有率 = 実行中のセッション数 10 / （仮想マシン 1 台あたり 20 セッション x 1 台の仮想マシン） = 50% ■ 平均ロード インデックス = エージェント ロード インデックス 25% / 1 台の仮想マシン = 25% 2 つの値の高い方は 50% で、これは、電源管理の最適なパフォーマンス設定の高しきい値に一致します。その結果、システムは 2 台目の仮想マシンをパワーオンします。	**パワーオン状態の仮想マシン** 仮想マシン 1 ■ 実行中のセッション数 = 10 ■ エージェント ロード インデックス = 25% 仮想マシン 2 ■ 実行中のセッション数 = 0 ■ エージェント ロード インデックス = 0% **使用量値** ■ セッション占有率 =（実行中のセッション数 10 + 0）/（仮想マシン 1 台あたり 20 セッション x 2 台の仮想マシン）= 25% ■ 平均ロード インデックス =（エージェント ロード インデックス 25% + 0%）/ 2 台の仮想マシン = 12.5% 2 つの値の高い方は 25% で、これは、電源管理の最適なパフォーマンス設定の高しきい値を下回っています。このため、システムは何もアクションを実行しません。

例：平均ロード インデックスが高しきい値を超えたためにプールを拡張

この例では、次の設定が使用されます。

- 仮想マシン 1 台あたりのセッション数 = 20
- 電源管理の高しきい値 = 50%

拡張前	拡張後
パワーオン状態の仮想マシン 仮想マシン 1 ■ 実行中のセッション数 = 5 ■ エージェント ロード インデックス = 50% **使用量値** ■ セッション占有率 = 実行中のセッション数 5 /（仮想マシン 1 台あたり 20 セッション x 1 台の仮想マシン） = 25% ■ 平均ロード インデックス = エージェント ロード インデックス 50% / 1 台の仮想マシン = 50% 2 つの値の高い方は 50% で、これは、電源管理の最適なパフォーマンス設定の高しきい値に一致します。その結果、システムは 2 台目の仮想マシンをパワーオンします。	**パワーオン状態の仮想マシン** 仮想マシン 1 ■ 実行中のセッション数 = 5 ■ エージェント ロード インデックス = 50% 仮想マシン 2 ■ 実行中のセッション数 = 0 ■ エージェント ロード インデックス = 0% **使用量値** ■ セッション占有率 =（実行中のセッション数 5 + 0）/（仮想マシン 1 台あたり 20 セッション x 2 台の仮想マシン） = 12.5% ■ 平均ロード インデックス =（エージェント ロード インデックス 50% + 0%）/ 2 台の仮想マシン = 25% 2 つの値の高い方は 25% で、これは、電源管理の最適なパフォーマンス設定の高しきい値を下回っています。このため、システムは何もアクションを実行しません。

Horizon Cloud Service - next-gen のプールの詳細

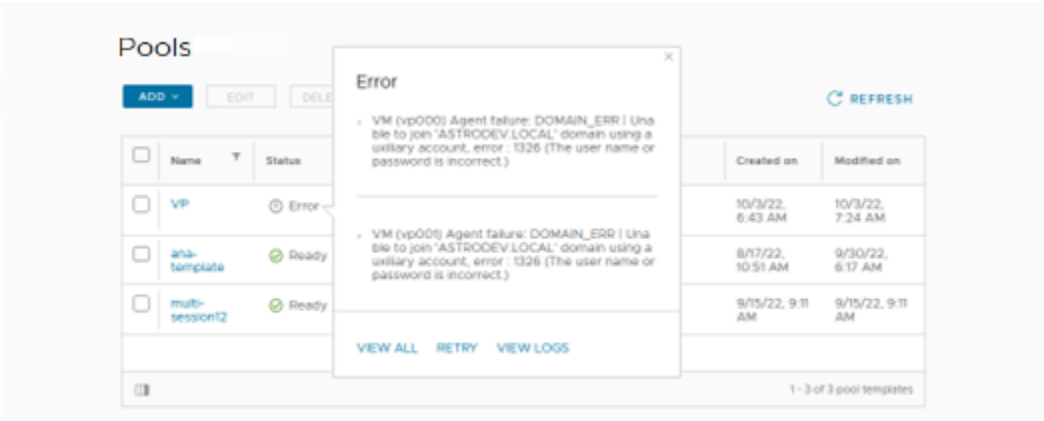
Horizon Cloud Service - next-gen のプールのサマリ ページで、1 つ以上のプールの詳細を表示および確認できます。

手順

1 Horizon Universal Console にログインします。

2 ホーム ページで、[プール] タイルの [プール] をクリックします。

a プールにエラーが表示される場合は、[エラー] をクリックしてエラーを表示し、対処します。



b 「`Anomaly detected for template`」で始まるエラーが表示された場合は、不要なリソースを削除し、KB90261 を参照して、[再試行] をクリックします。

再試行が成功すると、仮想マシンは [拡張]、[圧縮]、または [準備完了] 状態に変わります。

プール プロビジョニングの詳細については、「プール プロビジョニングの再試行」を参照してください。

3 [プール] の [名前] リンクをクリックして、[プール] の詳細ページに移動します。

4 [概要] をクリックして、[キャパシティ]、[セッション]、[全般設定]、[プロビジョニング] を表示します。[概要] ページで、[セッション キャパシティ] が [最大]、[プロビジョニング済み]、または [使用中] に設定されています。また、[使用中のセッション数] が [接続済み] または [切断済み] に設定されています。

[プール] の詳細ページから、[プール] の [編集] または [削除] をクリックすることもできます。

5 [仮想マシン]、[セッション]、および [管理アクティビティ] タブで、[列の管理] をクリックして、[アベイラビリティ ゾーン ID] 列や [IPv6 アドレス] 列など、デフォルトでテーブルに表示されない列を選択します。

たとえば、[仮想マシン] タブで、[列の管理] オプションを使用し、[アベイラビリティ ゾーン ID] を選択して、その列を仮想マシン リストに追加します。[アベイラビリティ ゾーン ID] 列には、リスト内の各仮想マシンの Azure アベイラビリティ ゾーンが一覧表示されます。その後、プール内の仮想マシンが Azure アベイラビリティ ゾーン全体でどのように分散されているかを確認できます。

Azure アベイラビリティ ゾーンのサポートの制限については、次の Microsoft のドキュメントを参照してください。

6 [仮想マシン] をクリックして、[仮想マシン] のリストを表示します。

Microsoft Azure ポータルまたはゲスト OS のシャットダウンを使用して、Horizon Universal Console の外部で仮想マシンを [パワーオフ] または [パワーオン] しないでください。これを行うと、内部ステータスが更新され、Microsoft Azure ポータルに表示される仮想マシンの最新のステータスが反映されます。この更新には 10 ～ 15 分かかります。また、仮想マシンが外部でシャットダウンされていても、割り当て解除されていない場合、システムは仮想マシンの割り当てを解除してコストを削減します。同期アクションは、[アクティビティ ログ] に [システム アクティビティ] として表示されます。

7 [ドロップダウン]をクリックしてプールを選択します。ドロップダウンには、メイン プールと、メイン プールのすべての拡張プールが一覧表示されます。

8 [セッション] をクリックして、[セッション] のリストを表示します。

9 [セッション] タブで、3 つの連続するドットをクリックしてセッションを [ログオフ] します。

10 [管理アクティビティ] をクリックして、選択したプールで管理者によって開始されたアクティビティの詳細を表示します。

11 [管理アクティビティ] タブで [エクスポート] をクリックして、選択したプールで管理者によって開始されたアクティビティのログをエクスポートします。

ログには、指定した期間（1 ～ 90 日）の管理アクティビティが含まれます。ログには、誰がいつイベントを開始したかなど、各管理アクティビティ イベントに関する詳細が表示されます。

Horizon Cloud Service - next-gen のプール グループの詳細

プールのサマリ ページで、1 つ以上のプールの詳細を表示および確認できます。

手順

1 Horizon Universal Console にログインします。

2 [ホーム] ページの [プール グループ] タイルをクリックします。

3 [プール グループ] ページで [プール グループ] の [名前] リンクをクリックして、プールの詳細ページに移動します。

4 [概要] をクリックして、[セッション キャパシティ]、[使用中のセッション数]、[ポリシー]、[電源管理]、および [タイムアウト処理] を表示します。

5 [プール] をクリックして、[プール] のリストを表示します。

6 [アプリケーション] をクリックして、[アプリケーション] のリストを表示します。

フローティング プール グループの場合は、[App Volumes アプリケーション] をクリックして、フローティング プール グループに追加された App Volumes アプリケーションのリストを表示します。既存のフローティング プール グループとの間で App Volumes アプリケーションを [追加] および [削除] できます。[アプリケーション] タブは、公開アプリケーション、公開デスクトップ、およびアプリケーション プール グループ タイプにのみ適用されます。

7 [資格] をクリックして、[資格] のリストを表示します。

8 [セッション] をクリックして、[セッション] のリストを表示します。

Horizon Cloud Service - next-gen は、Windows 10 のマルチセッション（ユーザー セッションごとに一意のアプリケーション配信）をサポートします。

9 3 つの連続するドットをクリックして、セッションから [ログオフ] します。

管理者ユーザーの管理と Horizon Cloud Service - next-gen 環境のライセンスの管理

このドキュメント ページには、管理者ユーザーの追加、ロールの割り当て、およびライセンスの管理に関するハウツー ページへのリンクが記載されています。

Horizon Universal Console ユーザーへの管理ロールの割り当て

Horizon Cloud 管理ユーザーを作成し、ロールを割り当てることができます。ロールは、特定の情報の表示や特定のアクションの実行など、Horizon Universal Console に対して指定された権限を管理ユーザーに提供します。

Horizon Universal Console の管理ロール

各ロールは、指定した領域に対する作成、読み取り、更新、および削除の権限を付与し、その他のすべてに対しては読み取り権限のみを付与します。

ロール	権限の領域
管理者	ユーザー インターフェイスと API 全体へのアクセス。
読み取り専用管理者	ユーザー インターフェイスと API への読み取り専用アクセス
プール管理者	プールと仮想マシン
展開管理者	Horizon Edge、Unified Access Gateway、プロバイダ
プール グループ管理者	プール グループ

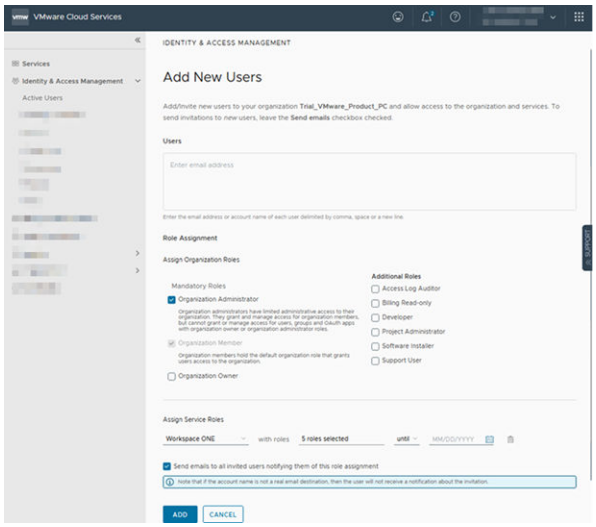
ロール	権限の領域
資格管理者	資格
イメージ管理者	イメージ

Horizon Universal Console ユーザーの追加とロールの割り当て

管理者ユーザーに Horizon Universal Console へのアクセス権を付与するには、VMware Cloud Services コンソール を使用して、最初にそれらのユーザーに組織ロールを割り当てます。その後、これらのユーザーに Horizon Cloud サービス ロールを割り当てることができます。

このタスクでは、Cloud Services コンソール にアクセスする必要があります。新しいユーザーを追加するには、組織の所有者であるか組織の管理者である必要があります。

注： VMware Cloud™ Services の詳細については、VMware Cloud Services 製品ドキュメントを参照してください。VMware 製品およびドキュメントでは、「VMware Cloud Services Platform」(CSP) や「VMware Cloud Services Engagement Platform」など、VMware Cloud services に他の名前が使用されることがあります。



手順

1 Cloud Services コンソール にログインします。

2 左側のメニューで、[ID とアクセス管理] - [アクティブ ユーザー] を選択します。

注： [ID とアクセス管理] ノードは、組織の所有者および組織の管理者のみが使用できます。

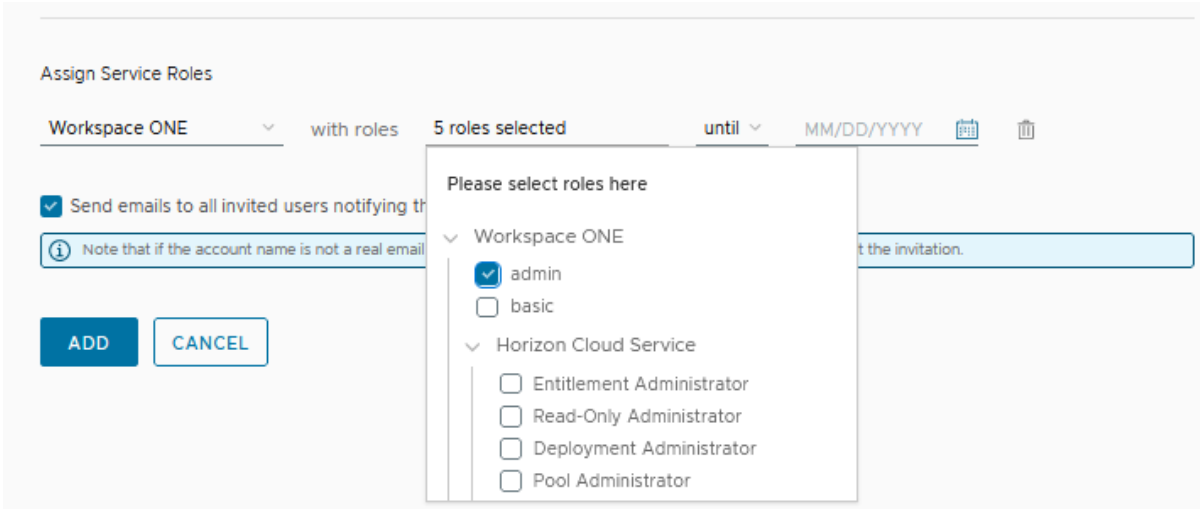
3 [アクティブ ユーザー] - [ユーザーの追加] を選択します。

4 [ユーザー] テキスト ボックスに、管理ロールを割り当てるユーザーのメール アドレスを追加します。

5 追加したユーザーの組織ロールを選択します。

組織の所有者および組織の管理者は、Cloud Services コンソール を使用してユーザーを追加および編集できます。

6 [サービスの追加] をクリックし、必要に応じて [Workspace ONE] を選択します。



7 [次のロールを持つ] テキスト ボックスをクリックして使用可能なロールのリストを表示し、必要に応じて追加のロールを選択します。

8 次のドロップダウン メニューで、権限の有効期限がある時点で切れるようにするかどうかに応じて、[次の日付] または [次の日付まで] を選択します。

9 必要に応じて、次のフィールドに有効期限を入力します。

10 [追加] をクリックします。

結果

追加したユーザーは、権限が付与された Horizon Universal Console にアクセスできます。

[アクティブ ユーザー] ページで実行できるその他のアクション

Cloud Services コンソール を使用してユーザーを追加したら、[アクティブ ユーザー] ページで他のいくつかのアクションを実行できます。

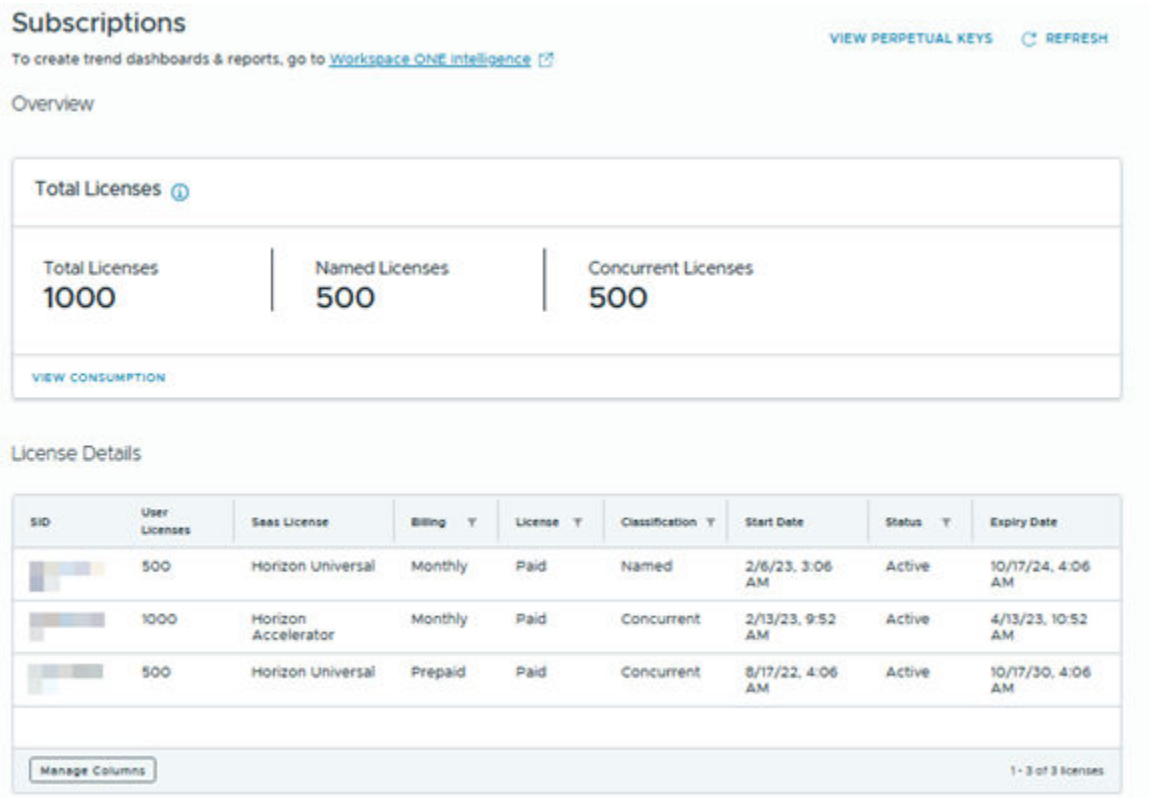
次のアクションを実行できます。その多くは、最初の Horizon Availability Monitoring テストを構成する手順と同じか類似しています。

アクション	説明
アクティブ ユーザーのリストを検索する。	[検索] テキスト ボックスにテキスト文字列を入力して、アクティブ ユーザーのリストを検索します。
選択したアクティブ ユーザーのロール関連情報を表示する。	アクティブ ユーザーの名前の横にある二重矢印をクリックして、次の情報を表示します。 ■ そのユーザーの組織ロール（組織の管理者、組織の所有者、組織のメンバーなど）。 ■ そのユーザーのサービス（Horizon Cloud Service など）と、ユーザーに割り当てられたそのサービスのロール（イメージ管理者やインベントリ管理者など）。
ユーザーのロールを編集する。	ユーザーを選択し、[ロールを編集] をクリックします。 ロールの編集は、前に説明したロールの追加手順と非常によく似ています。
ユーザーを削除する。	1 人以上のユーザーを選択し、[ユーザーを削除] をクリックします。

Horizon Universal Console を使用した Horizon ライセンスの追跡

[サブスクリプション] ページの目的は、管理者が Horizon サブスクリプション ライセンスのステータスを迅速に判断できるようにすることです。

Horizon サブスクリプション ライセンスを表示するには、左側のメニューで [サブスクリプション] をクリックします。



[サブスクリプション] ページには、次の詳細が適用されます。

- デプロイに含まれるライセンスの数は、[ライセンスの合計] セクションで確認できます。セクションにはライセンスの合計数、および分類別のライセンスの数が一覧表示されます。ライセンスの分類については、次の情報を参照してください。
- ページで使用可能な並べ替え矢印またはフィルタを使用して、ライセンスの詳細をページに表示する方法を変更できます。たとえば、表見出しでは、[分類]（[同時実行] または [名前付き]）や [ステータス] などの列のフィルタを使用できます。また、[開始日] および [有効期限] などの列の並べ替え矢印も使用できます。
- SID

  サービス インスタンス ID

  サブスクリプションごとに生成された一意の識別子
- 課金 - ライセンスの課金タイプは次のとおりです。

  支払い済み

ライセンスの開始時に課金が 1 回発生します

毎月

ライセンス期間中の各月に課金が 1 回発生します

試用版

ライセンスは試用版ライセンスであるため、課金はありません

- 分類 - ライセンス使用モデルの分類は次のとおりです。

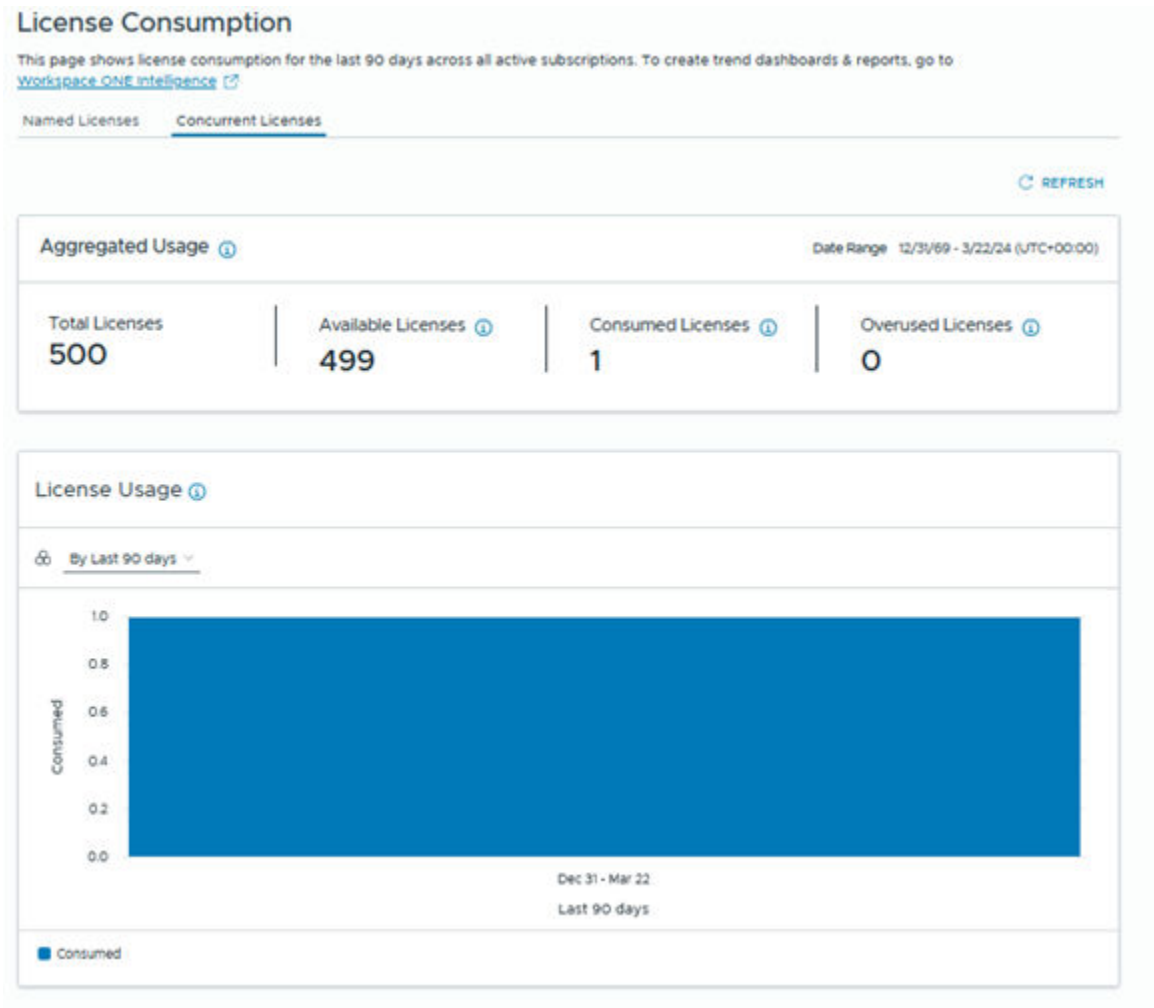
重要： 現在、ライセンス使用量メトリックは、ネイティブの Microsoft Azure デプロイでのみ使用できます。使用量メトリックは現在、Horizon 8 デプロイでは使用できません。

ライセンス使用量の詳細を表示するには、[使用量の表示] をクリックします。[ライセンス使用量] ページでは、サブスクライブしているライセンスのタイプに関するタブを使用できます。したがって、[同時使用ライセンス] タブ、[名前付きライセンス] タブ、またはその両方が表示されることがあります。

同時使用ライセンス

エンドポイント デバイスからデスクトップまたはアプリケーションへのアクティブ接続またはアイドル接続を維持するために、任意の時点でソフトウェアにアクセスまたはソフトウェアを使用しているエンド ユーザーの合計数を追跡するライセンスです。次の例を参照してください。

- 3 つの異なるエンドポイント デバイスを介して同時に 3 台のデスクトップを実行している同時接続ユーザーは、同時接続された 3 つのデスクトップ セッションごとに 1 回、合計 3 回カウントされます。
- 同じエンドポイント デバイスと同じクライアントを介して 3 台のデスクトップを同時に実行している同時接続ユーザーは、1 回のみカウントされます。



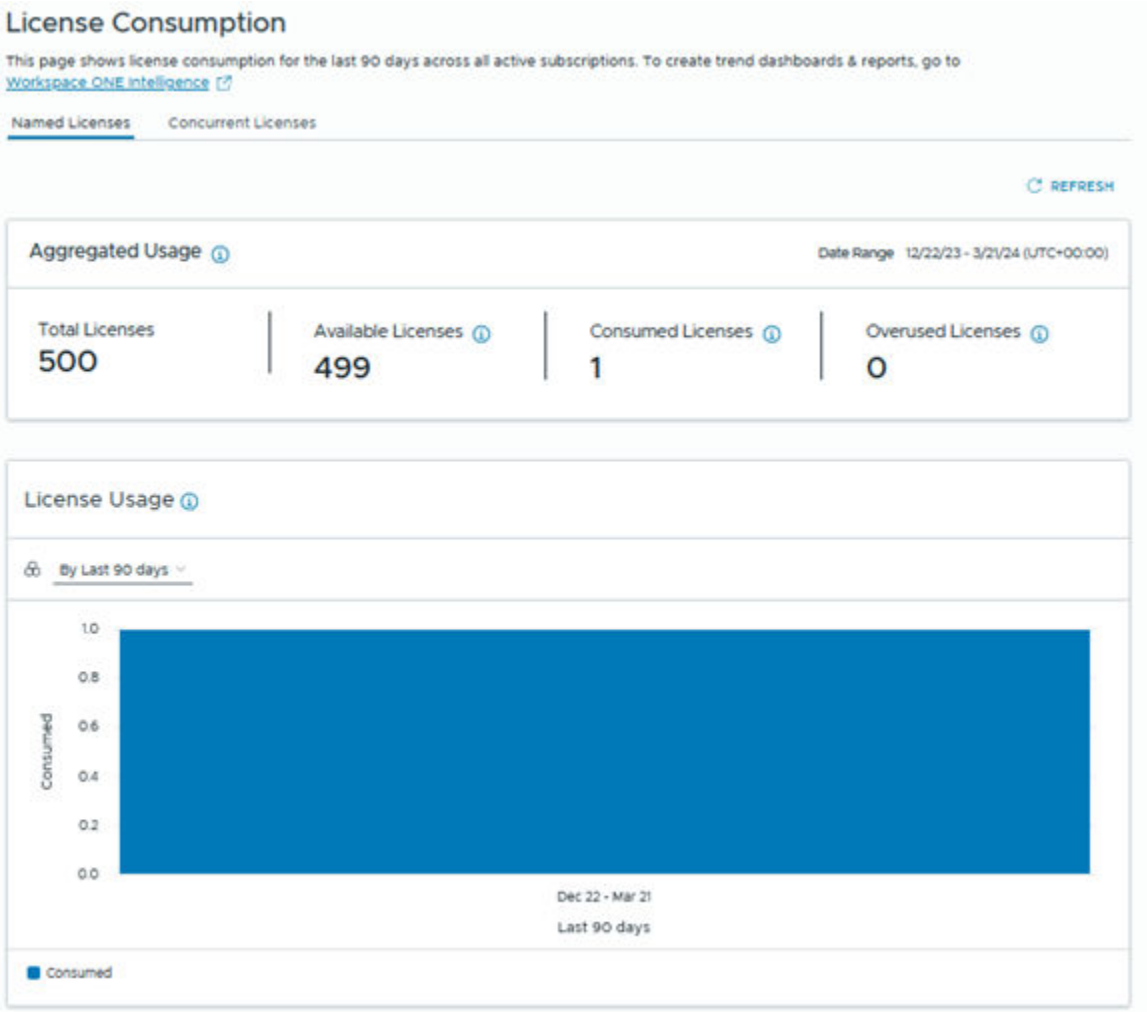
注： [更新] をクリックして、ピーク時の使用率統計情報を更新します。

[同時使用ライセンス] ページには、使用可能な同時使用ライセンスの合計数やピーク時の使用率統計情報など、同時使用ライセンスに関する情報が表示されます。ピーク時の使用率統計情報には、特定の期間に使用されている同時使用ライセンスの最大数が表示されます。

デフォルトでは、ライセンス使用量の詳細として [直近 90 日間ごと] が表示され、その他に [月ごと] および [直近 7 日間ごと] の使用量の詳細オプションを使用できます。

名前付きライセンス

ソフトウェアにアクセスまたはソフトウェアを使用してデスクトップまたはアプリケーションに接続した一意のエンド ユーザーを追跡するライセンスです。VMware Horizon Cloud Service - next-gen は、昨日から過去 90 日間にセッションを開始した一意のエンド ユーザーの数をカウントします。複数のデスクトップおよびアプリケーションにアクセスしている場合も、1 回のみカウントされます。



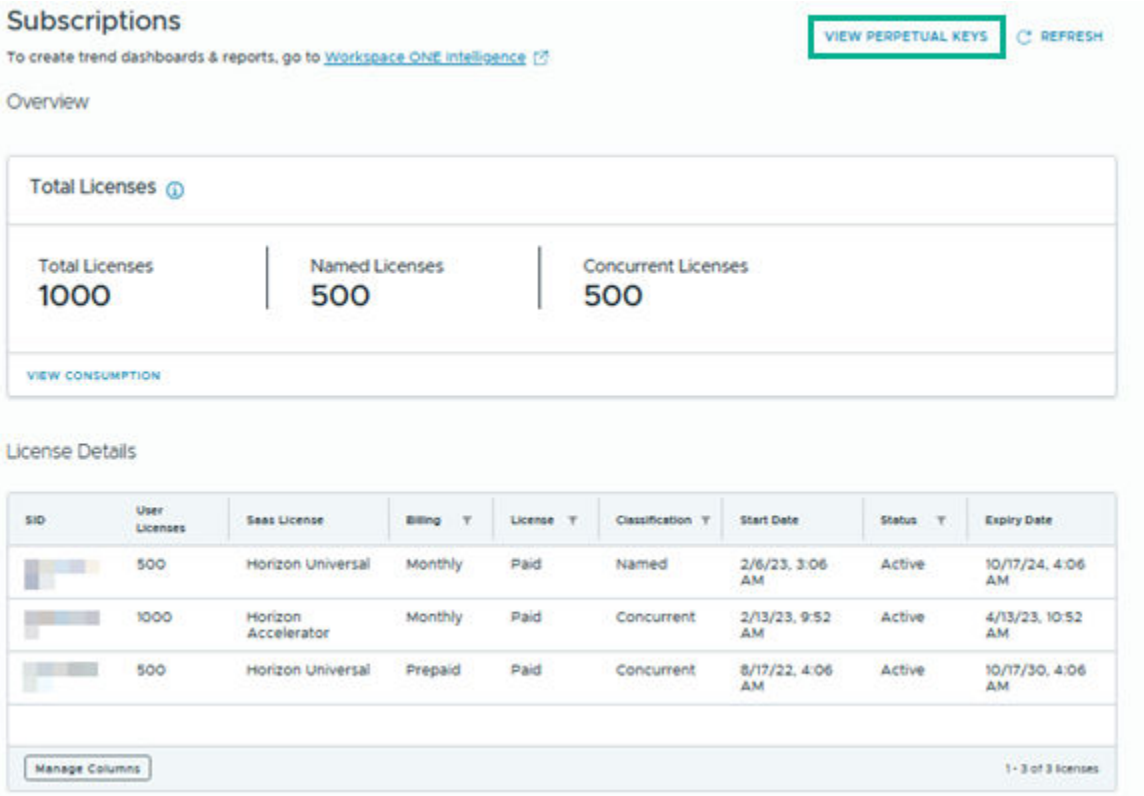
デフォルトでは、ライセンス使用量の詳細として [直近 90 日間ごと] が表示され、その他に [月ごと] および [直近 7 日間ごと] の使用量の詳細オプションを使用できます。

Horizon Universal Console を使用したエンタープライズ インフラストラクチャ キーの取得

このドキュメント ページでは、Horizon Universal Console を使用して、VMware エンタープライズ インフラストラクチャ製品のライセンス キーを取得する方法について説明します。

Horizon Cloud サブスクリプションに、vSphere、vSAN、vCenter Server、ThinApp Client、ThinApp 仮想パッケージャ、App Volumes Enterprise、Workstation などの VMware の基本製品が含まれている場合、管理者ロールを使用して Horizon Universal Console にログインすると、コンソールの [サブスクリプション] ページにエンタープライズ インフラストラクチャ ライセンス キーを表示するためのリンクが表示されます。

前述の要件を満たしていない場合、コンソールには [無期限キーの表示] リンクは表示されません。



キーの生成

[無期限キーの表示] をクリックすると、[エンタープライズ インフラストラクチャのライセンス キー] 画面が開き、エンタープライズ インフラストラクチャ ライセンス キーを生成および表示できます。ライセンス キーを生成するには、次の要件を満たす必要があります。

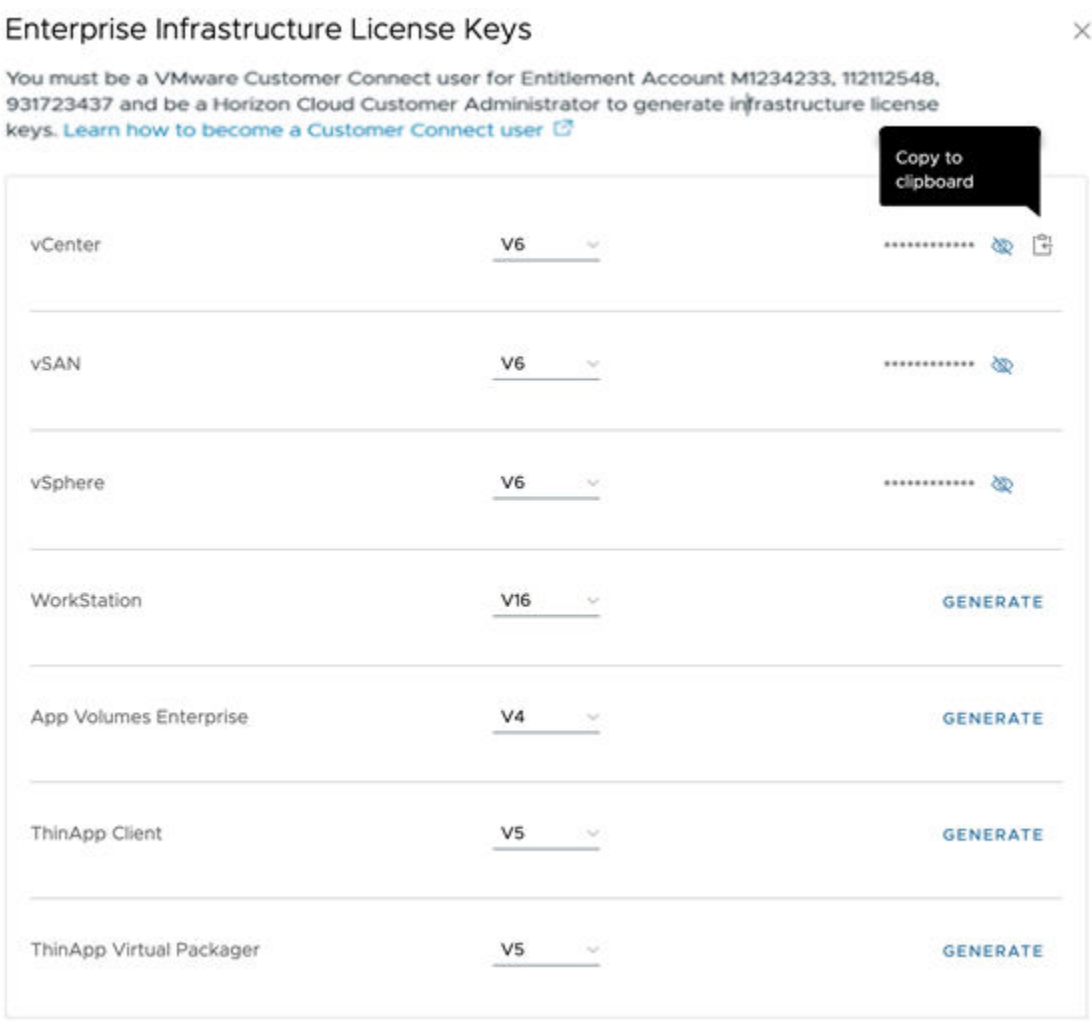
- 管理者ロールがあること
- VMware Customer Connect ユーザーであること

特定の製品のライセンス キーを生成するには、[エンタープライズ インフラストラクチャのライセンス キー] 画面で、その製品のドロップダウン メニューからバージョンを選択し、[生成] をクリックします。その製品のキーが表示されます。

キーの表示またはコピー

[無期限キーの表示] をクリックすると、[エンタープライズ インフラストラクチャのライセンス キー] 画面が開き、以前に生成されたエンタープライズ インフラストラクチャ ライセンス キーを表示できます。ライセンス キーを表示するには、管理者ロールまたは読み取り専用管理者ロールが必要です。

生成されたキーを表示するには、ライセンス キーの横にある目のアイコンをクリックします。生成されたキーをコピーするには、ライセンス キーの横にある [コピー] アイコンをクリックします。



Horizon Cloud Service - next-gen Universal Console を使用した Horizon 8 Edge Gateway の新しいバージョンへのアップグレード

デプロイされた Horizon 8 Edge Gateway で新しいバージョンが使用可能な場合は、Horizon Cloud Service - next-gen Universal Console に示されている一連の手順に従って、新しいバージョンに手動でアップグレードできます。

デプロイされた Horizon 8 Edge Gateway で新しいバージョンが利用可能かどうかを確認し、Horizon Universal Console の [キャパシティ] セクションで説明されている一連の手順を使用して新しいバージョンにアップグレードします。

このワークフローは、フェデレーションされていない Horizon View Edge で使用できます。

注： アップグレードする Edge が接続済みの Edge である場合は、Edge がデプロイされている古い仮想マシンをオフにして、以下の説明に従ってアップグレードを続行します。アップグレードに成功した場合は、古いバージョンの仮想マシンを破棄できます。アップグレードに失敗した場合は、プロンプトに従ってアップグレードを再試行します。再試行しない場合は、仮想マシンをパワーオンし直して、Edge が再び稼動するようにします。データが失われることはありません。

手順

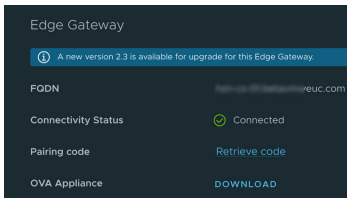
この手順を使用して、新しいバージョンの Horizon 8 Edge Gateway にアップグレードします。

1 Horizon Cloud Service - next-gen にログインし、[Horizon Universal Console] ページの左側のペインのナビゲーションから [キャパシティ] をクリックします。

2 表示される [キャパシティ] ページで [サマリ] タブをクリックし、選択した Edge の情報を確認します。特に、ページの [Edge Gateway] 領域の情報に注意してください。

アップグレード可能なすべての Edge が、[使用可能なアップグレード] セクションの [メンテナンス] タブに一覧表示されます。アップグレード情報は、個々の Edge の詳細ページでも確認できます。

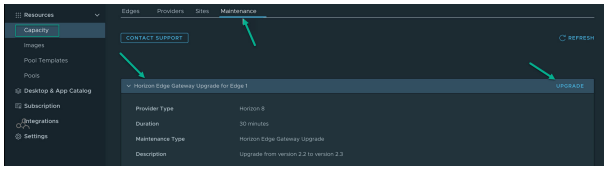
Edge Gateway の新しいバージョンが使用可能な場合は、ページの [Edge Gateway] 領域に「`A new version n.n is available for upgrade for this Edge Gateway.`」というメッセージが表示されます。



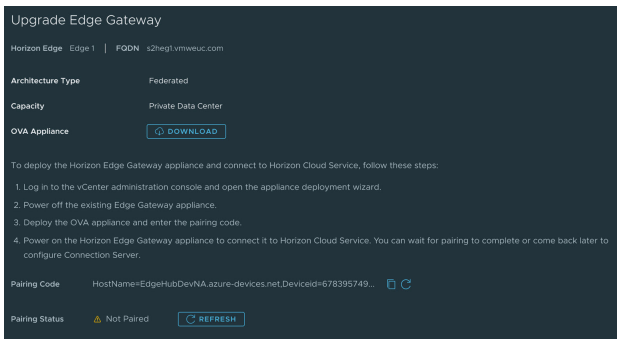
3 [ペアリング コード] オプションで、[コードを取得] をクリックします。コピー アンド ペーストして、取得したコードを将来使用するために安全な場所に保存します。このペアリング コードは、以降の手順で必要になります。

4 [OVA アプライアンス] オプションで、[ダウンロード] をクリックします。将来使用するために、OVA のダウンロード名と場所をメモしておきます。この OVA アプライアンスは、以降の手順で必要になります。

5 指定した Edge Gateway のアップグレードを続行するには、[キャパシティ] ページの [メンテナンス] タブをクリックし、指定した Edge Gateway の [アップグレード] をクリックします。



6 次のサンプル画面に示すように、画面の指示に従って OVA アプライアンスにアクセスし、Edge Gateway アプライアンスをデプロイして、Horizon Cloud Service - next-gen に接続します。



7 アップグレードが完了すると、Edge は [メンテナンス] タブにアップグレード可能として表示されなくなり、アップグレード バナー メッセージは表示されなくなります。

前述のように、アップグレードに成功した場合は、古いバージョンの仮想マシンを破棄できます。アップグレードに失敗した場合は、プロンプトに従ってアップグレードを再試行します。アップグレードに失敗した後に再試行しない場合は、仮想マシンをパワーオンし直して、Edge が再び稼動するようにします。データが失われることはありません。

Horizon Cloud Service - next-gen 環境の監視

Horizon Cloud Service - next-gen の Horizon Universal Console を使用して、ユーザーの検索、デスクトップおよびアプリケーション データの表示、仮想マシン ログのダウンロード、収集されたイベント情報（通知、監査イベント、システムおよびユーザー アクティビティなど）の確認を行うことができます。

Horizon Cloud Service - next-gen 環境内のヘルプ デスク機能

Horizon Universal Console では、エンド ユーザーによる仮想デスクトップとアプリケーションの使用状況を監視し、問題のトラブルシューティングを行えます。Horizon Universal Console の管理者は、コンソールの検索機能を使用してユーザーを検索できます。管理者は、特定のユーザーのセッションを検索して問題のトラブルシューティングを行い、特定のデスクトップ メンテナンス操作を実行できます。

ヘルプ デスク機能の目的

組織では、管理者が Horizon Universal Console にアクセスして、環境で提供される仮想デスクトップやリモート アプリケーションの使用など、エンド ユーザーのさまざまなアクティビティをサポートすることができます。これらの管理者は、エンド ユーザーのセッションを監視したり、デスクトップ インスタンスを監視して、セッションに影響を与える可能性のある問題を特定することもできます。

Horizon Universal Console では、次の項目が、これらのヘルプ デスク関連のタスクの実行をサポートします。

- Horizon Universal Console の検索機能。ヘルプ デスク ワーカーは、この機能を使用して特定のエンド ユーザーを検索できます。
- ユーザー カードの機能。特定のユーザーのユーザー カードを使用することにより、ヘルプ デスク ワーカーはそのユーザーのセッションを調べて問題のトラブルシューティングを行ったり、特定のデスクトップ メンテナンス操作を実行したりすることができます。

プロバイダ タイプに基づいてヘルプ デスク機能の環境を準備する

Horizon Universal Console のヘルプ デスク機能は、Microsoft Azure と Horizon 8 の両方のデプロイをサポートします。

注： ハイブリッド環境の場合、Microsoft Azure および Horizon 8 環境のヘルプ デスク情報を並べて表示できます。

Horizon Cloud Service – next-gen on Microsoft Azure

前提条件は必須の手順で、オンボーディング プロセスで実行する必要があります。したがって、オンボーディング後、ヘルプ デスク機能はデフォルトで機能します。

Horizon Cloud Service – next-gen on Horizon 8

ヘルプ デスク機能を実際の環境で動作させるための前提条件が満たされていることを確認します。Horizon 8 環境のヘルプ デスク機能の前提条件を実行するを参照してください。

Horizon 8 環境のヘルプ デスク機能の前提条件を実行する

Horizon 8 環境でヘルプ デスク機能を動作させるには、次の要件を満たしている必要があります。

手順

- デプロイ用の Horizon ユニバーサル ライセンスがあることを確認します。
- Horizon 8 Edge を Horizon Cloud Service – next-gen にオンボーディングします。
- ID プロバイダが Horizon Cloud Service – next-gen 制御プレーンと同期されていることを確認します。

  SID 同期は必須です。
- エージェントの監視を有効にします。
- Horizon Connection Server のペアリングに使用されるアカウントに、Horizon Connection Server に追加されたセカンダリ認証情報があることを確認します。

  セカンダリ認証情報を追加すると、一方向の信頼されたドメインからユーザーまたはグループを検索できます。
- Horizon Connection Server への接続に使用するアカウントに、再起動操作の管理 (`MACHINE_REBOOT`) 権限と セッションの管理 (`MANAGE_VDI_SESSION`) 権限があることを確認します。

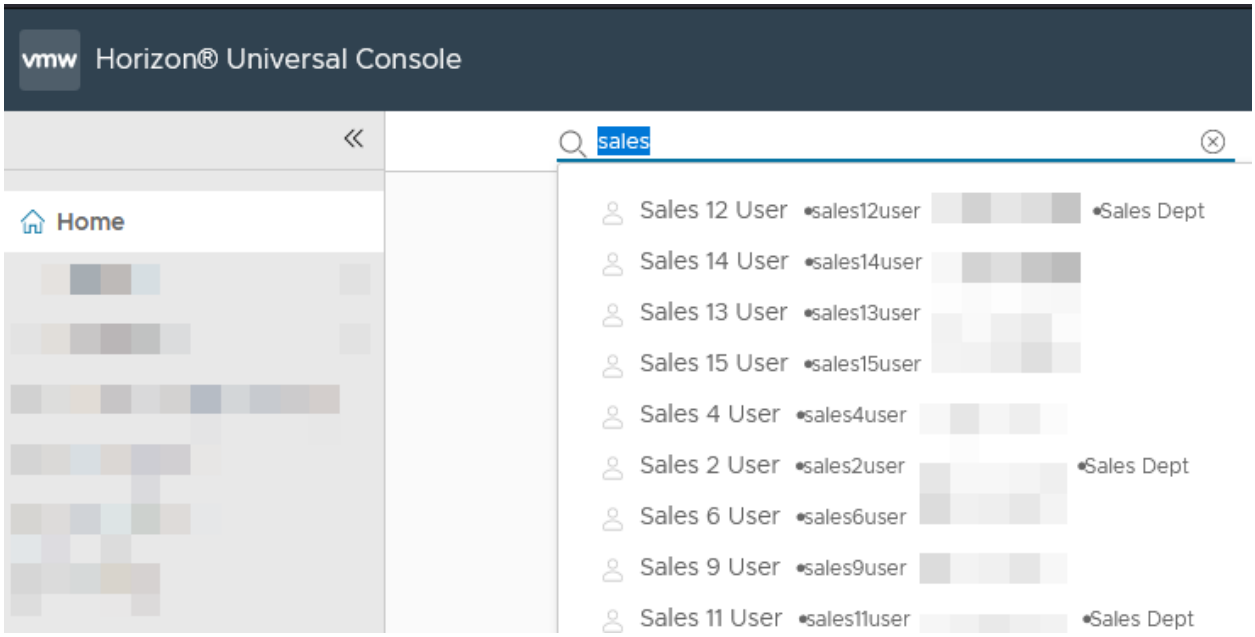
次のステップ

以下に続くトピックの説明に従って、Horizon Universal Console の検索機能とヘルプ デスク機能を使用します。

コンソールの検索機能の使用

Horizon Universal Console の検索機能を使用して、環境内の特定のエンド ユーザーを名前で特定します。ユーザーは、名、姓、または表示名で検索できます。

Horizon Universal Console の任意のページで、検索テキスト ボックスに検索語を入力します。[検索] テキスト ボックスに少なくとも 3 文字を入力すると、それらの文字で始まる名前が表示されます。結果を絞り込むには、さらに文字を入力します。



検索しているユーザーの名前が表示されたら、クリックしてそのユーザーの詳細を取得できます。詳細については、Horizon Cloud ユーザー カードおよびヘルプ デスク機能の使用を参照してください。

Horizon Cloud ユーザー カードおよびヘルプ デスク機能の使用

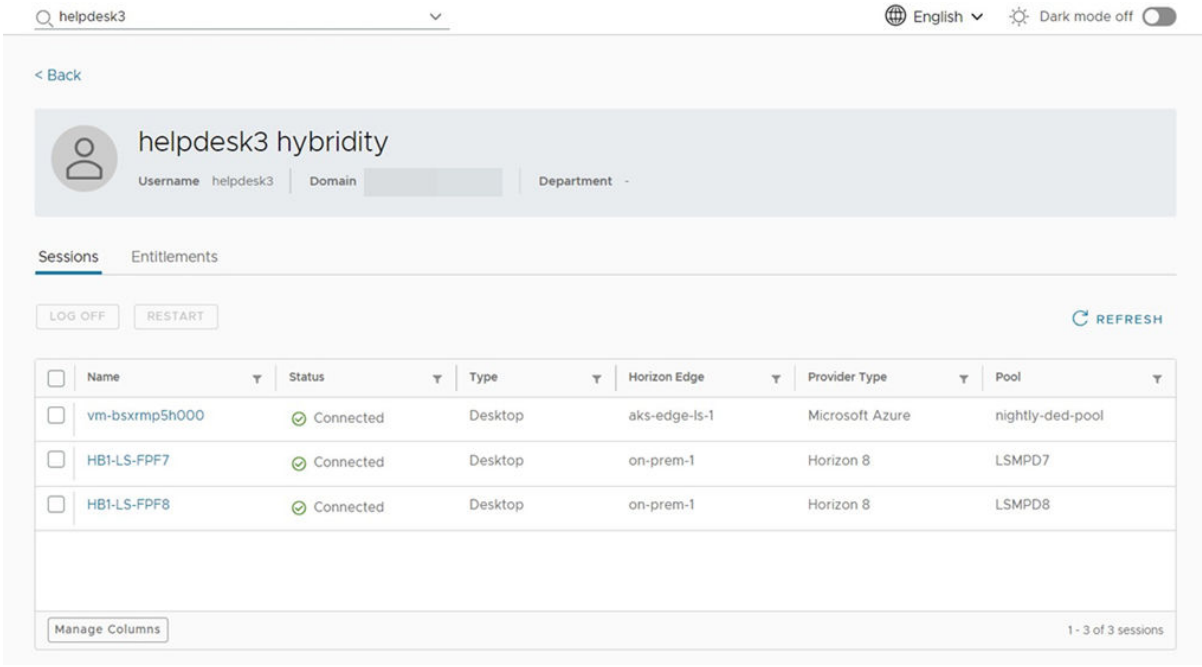
Horizon Universal Console でアクセス可能なユーザー カード機能をダッシュボードとして使用し、特定のエンド ユーザーの割り当て済みリソース（そのエンド ユーザーのデスクトップとアプリケーションなど）を処理します。ユーザーを検索して、ヘルプ デスク機能へのアクセスを開始します。

特定のエンド ユーザーのカードを表示するには、Horizon Universal Console の検索機能を使用します。エンド ユーザーの検索方法については、コンソールの検索機能の使用を参照してください。検索結果でエンド ユーザーの名前をクリックすると、そのエンド ユーザーのカードが表示されます。

特定のエンド ユーザーのコンテキストにおける情報データ、およびそのエンド ユーザーのアクティブなセッションと資格に関する情報データを表示できます。

セッション

ユーザーのアクティブなセッションに関する情報を取得するには、ユーザー カードに移動します。

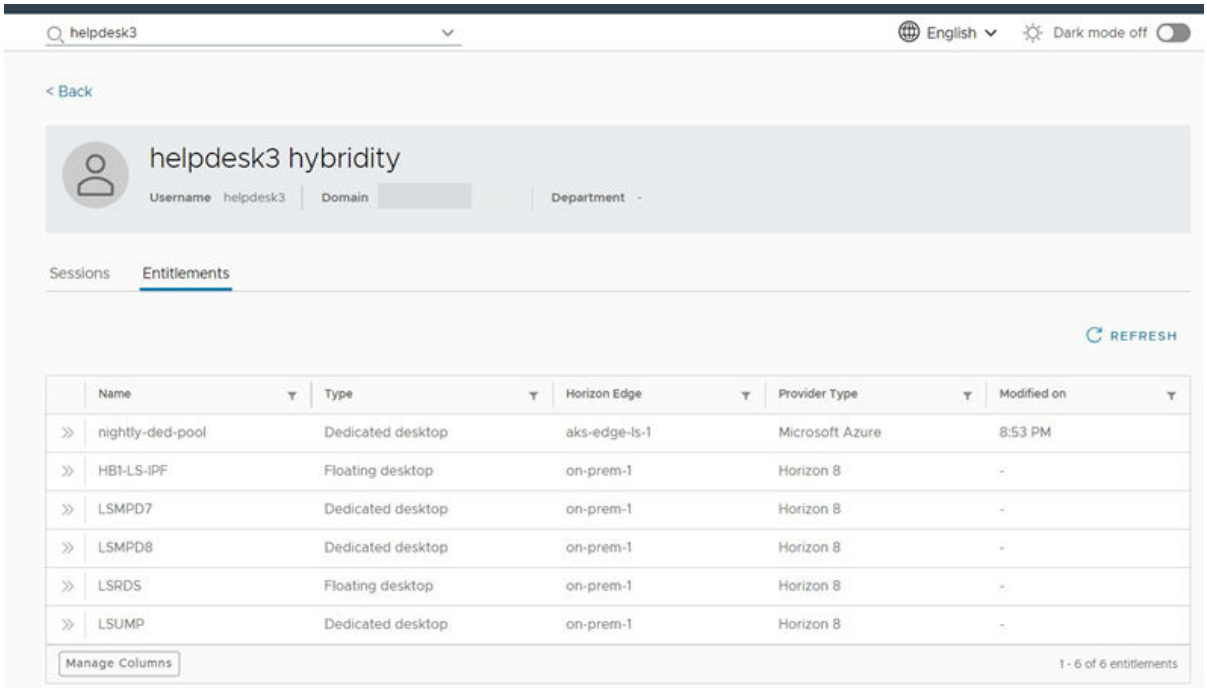


[セッション] タブでは、次の操作を実行できます。

- アプリケーションとセッションの両方を含むセッション リストを表示します。
- 特定のセッションのチェック ボックスをオンにして、次のアクションを有効にします。
  - [ログオフ] によりセッションからログオフします。
  - [再起動] によりセッションを再起動します。
- セッションの [名前] をクリックして、特定のセッションの詳細を表示します。
  - 使用可能な詳細は、プロバイダのタイプによって異なります。
  - セッションの詳細には、クライアントマシンの詳細およびその他の詳細（最新のアクティブなセッションの仮想マシン、セッション、CPU 使用率、メモリ使用量、ログイン セグメント仲介統計情報）が含まれます。

資格

ユーザー資格に関する情報を取得するには、ユーザー カードに移動し、[資格] タブを選択します。



[資格] タブでは、次の操作を実行できます。

- 特定のエンド ユーザーに使用資格が付与された仮想デスクトップまたはアプリケーションを表示します。
- 資格を展開して、仮想マシンまたはアプリケーションの詳細を表示します。
- デスクトップに対して操作を実行できます。
  - パワーオン
  - パワーオフ
  - シャットダウン
  - 再起動

注： Horizon 8 仮想マシンの場合は、[再起動] 操作のみを実行できます。

- エンド ユーザーがデスクトップに対してアクティブなセッションを行っていない場合でも、エンド ユーザーに割り当てられた専用デスクトップに関する情報を取得できます。

注： Horizon 8 環境の場合、ヘルプ デスク機能には次の制限があります。

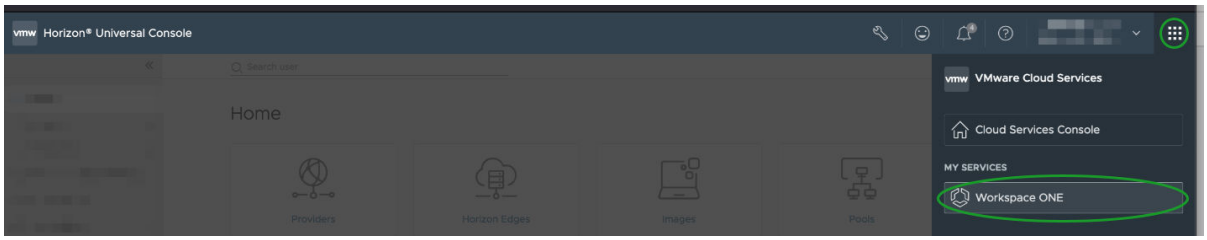
- 現在、Horizon Connection Server に対してローカルなデスクトップ セッションと資格のみがサポートされています。
- アプリケーション セッションと資格は表示されません。
- ペアリングされた Horizon Connection Server によって仲介され、リモート Horizon Edge でホストされているグローバル セッションは表示されません。
- Horizon 8 仮想マシンでは、次の操作はサポートされていません。
  - パワーオフ
  - シャットダウン
  - パワーオン

Pendo 分析とガイドのオプトアウト方法

次の手順に従って Workspace ONE を使用して Pendo 分析とガイドをオプトアウトできます。

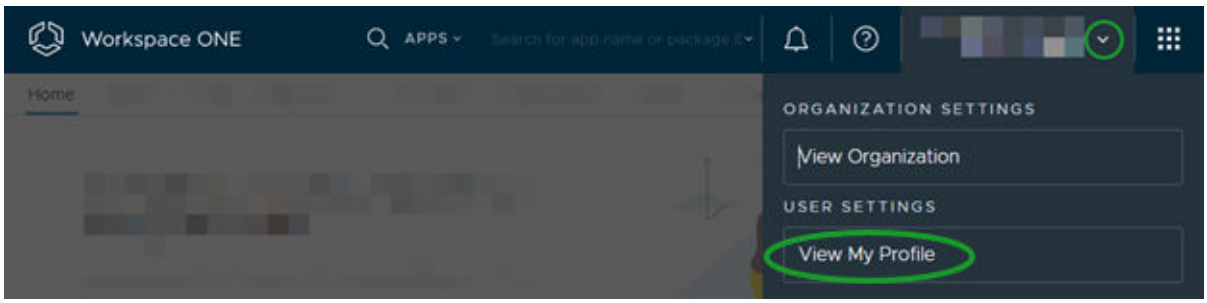
手順

1 Horizon Universal Console で、VMware Cloud Services アプリケーション メニュー（）をクリックして、Workspace ONE を選択します。



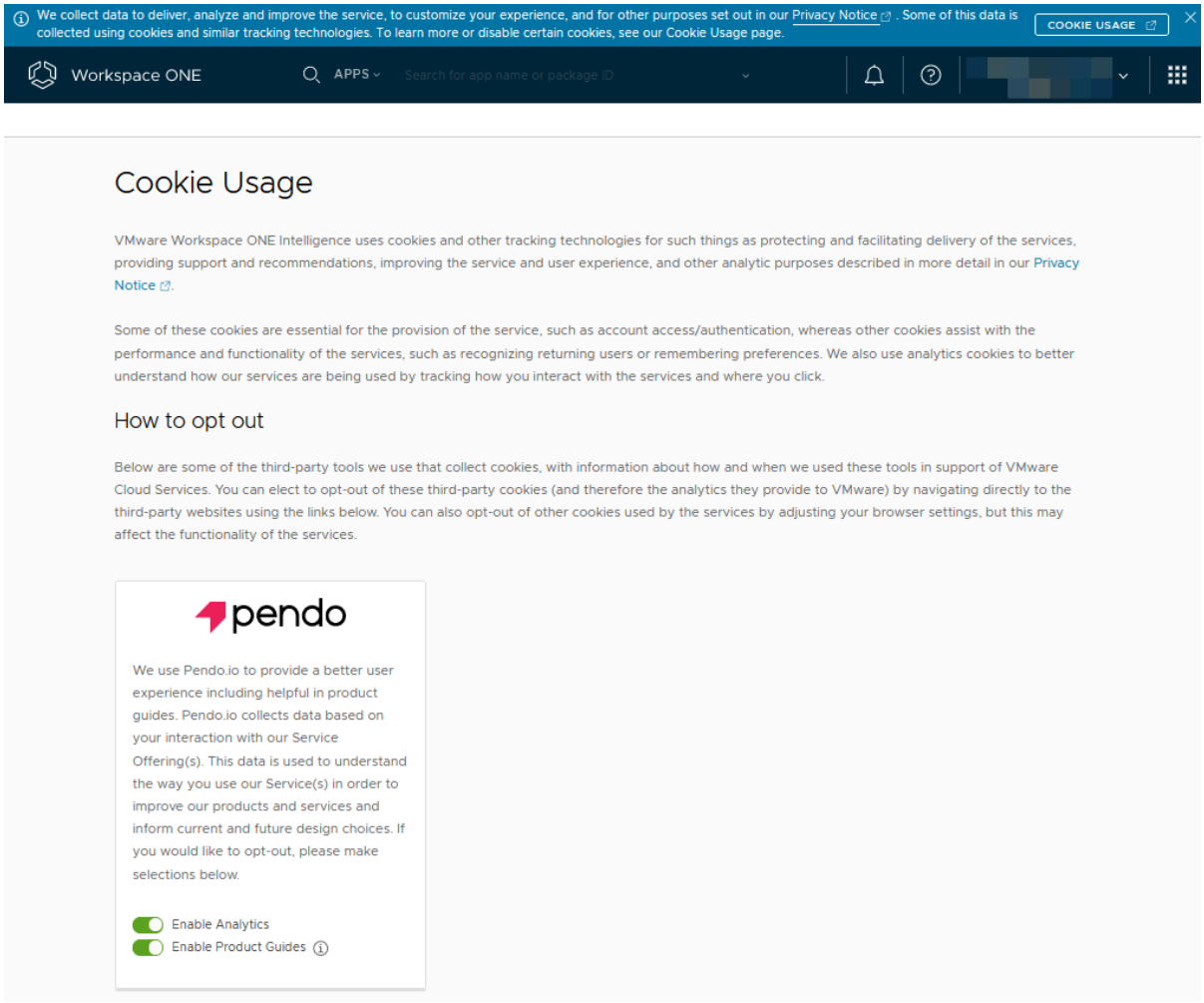
Workspace ONE Cloud Admin Hub コンソールが開きます。

2 Workspace ONE Cloud Admin Hub コンソールで、[ユーザー/組織設定] ドロップダウン メニューの下矢印をクリックし、[マイ プロファイルの表示] を選択します。



3 Cookie セクションまでスクロールし、[Cookie の使用方法] をクリックします。

次のスクリーンショットに示すように、[Cookie の使用方法] ページが表示されます。



4 [分析を有効にする] と [製品ガイドを有効にする] の両方をオプトアウトするか、[製品ガイドを有効にする] のみをオプトアウトするかに応じて、適切な手順を実行します。

- 両方をオプトアウトする場合は、[分析を有効にする] トグルをクリックします。
- [製品ガイドを有効にする] をオプトアウトするには、[製品ガイドを有効にする] トグルをクリックします。

ホーム ページからの Horizon Cloud リソースのステータスの監視

Horizon Cloud 環境が Workspace ONE Intelligence と統合されている場合は、Horizon Universal Console のホーム ページを使用してリソースを監視できます。

注： 表示されるデータとインサイトの一部は遅延する可能性があり、リアルタイムではないことに注意してください。監視データは Horizon Agent から取得され、Workspace ONE Cloud データ レイクに送信されます。Horizon Universal Console は、データ レイクをクエリしてダッシュボードに入力します。最悪のシナリオでは、このエンドツーエンドの処理によって最大 30 分の遅延が発生する可能性があります。

監視の観点から、ホーム ページの目的は、管理者が以下の項目を迅速に特定するのに役立つ情報に焦点を当てることです。

- Horizon Cloud 環境の全体的な健全性。

  たとえば、次の情報を指定します。

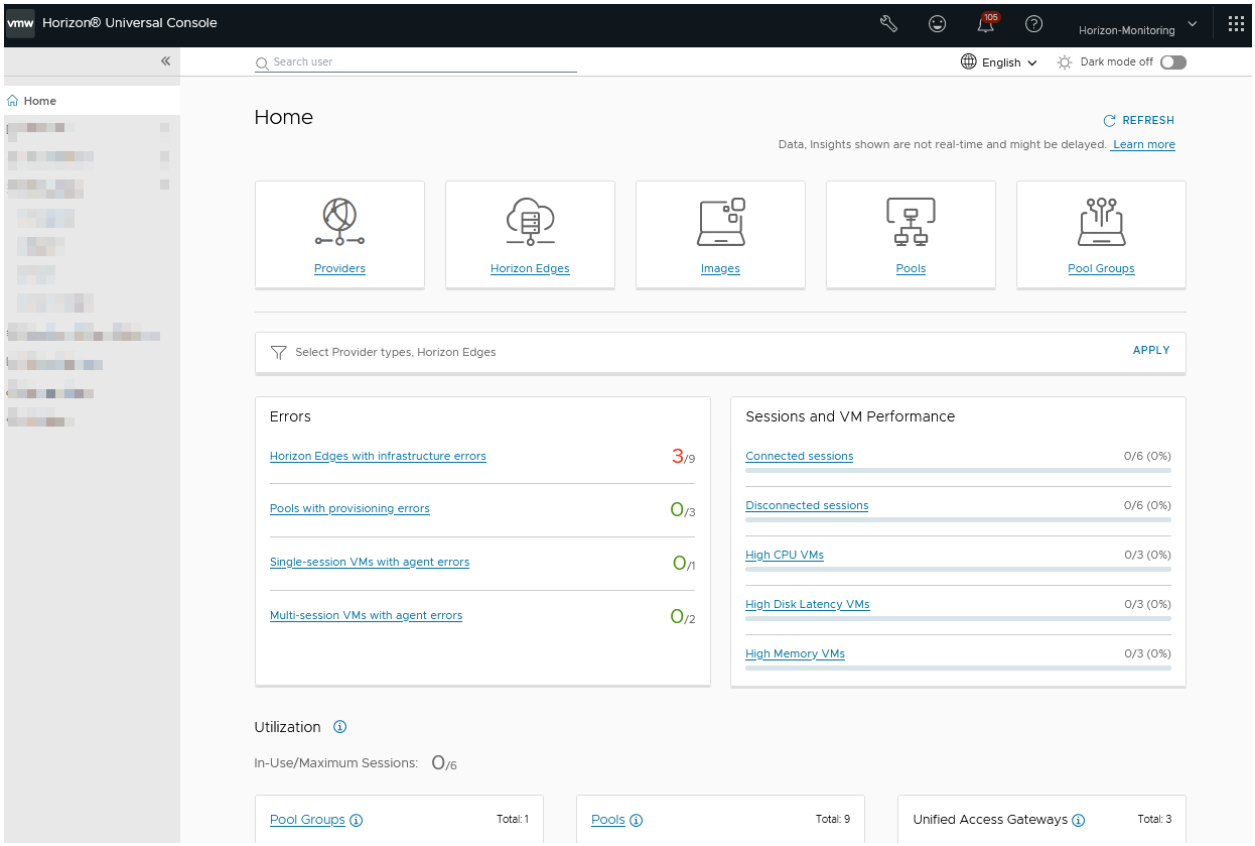
  - Horizon Edge インフラストラクチャ エラー
  - プールのプロビジョニング エラー
  - Horizon Agent エラー（マルチセッションおよび単一セッションの仮想マシン内で実行されているエージェントの場合）

  Horizon Cloud 環境の全体的な健全性の監視の観点から、ホーム ページは、管理者が存在する問題のタイプを特定するのに役立ちます（存在する場合）。次のようなタイプの問題があります。

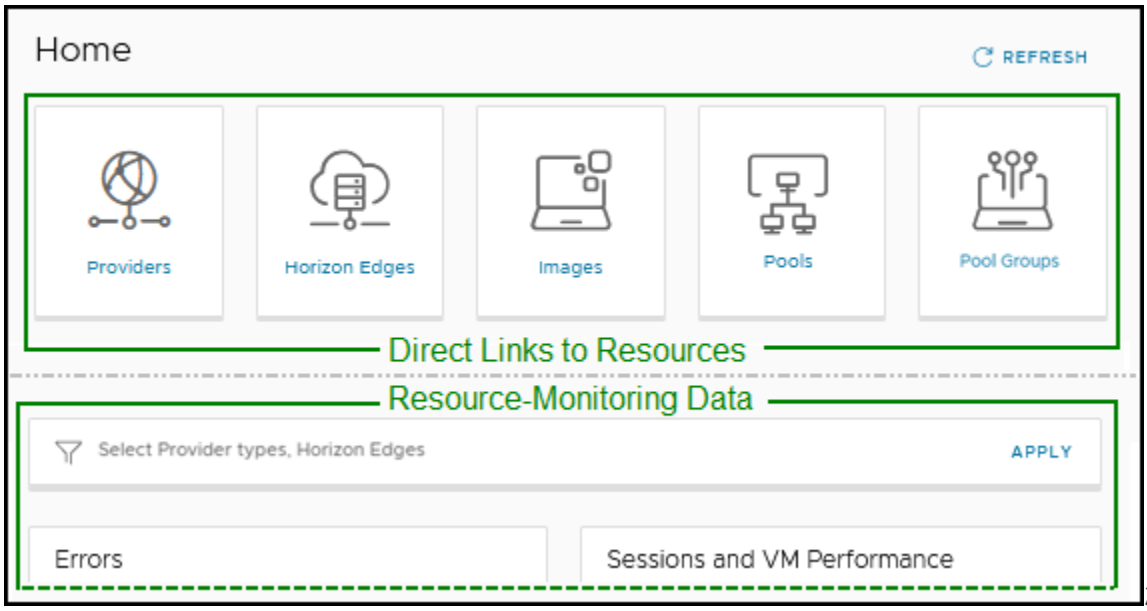
  - 明確に識別可能な問題
  - さらに調査が必要であることを示す問題
  - 管理者が短期的な監視アプローチを適用できることを示す問題
  - 迅速な対策が必要な問題
- 接続されたセッションと切断されたセッションの実際の数。
- CPU、メモリ、ディスクの使用量が高いなど、パフォーマンスの問題が発生している仮想マシンの実際の数。
- 上位 3 つのプール グループ、プール、および Unified Access Gateway の使用量を含む、キャパシティ使用量データ。

ホーム ページから、エンド ユーザーの環境で現在デスクトップまたはアプリケーションにアクセスするときに問題が発生していることを示すデータ、またはアクションを実行しない限りすぐに問題が発生する可能性があることを示すデータを表示したり、簡単にデータに移動したりできます。

Horizon Edge をデプロイし、Horizon Cloud が Workspace ONE Intelligence と統合された後、ホーム ページでリソース監視データの表示と操作を開始できます。Horizon Cloud のデプロイを続行すると、より多くのリソース監視データが利用可能になります。



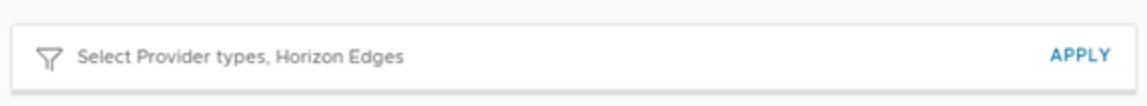
ホーム ページは 2 つのセクションで構成されています。ホーム ページの上部には、リソース ボタンがあります。リソース ボタンは、Horizon Cloud リソースへの直接リンクです。リソース ボタンの下にはリソースに関するデータがあり、表示および操作できます。



次の情報では、[ホーム] ページで使用可能なリソース監視データを操作する方法について説明します。

監視する Horizon Edge の選択

[プロバイダ タイプ、Horizon Edge を選択] フィルタを使用すると、[ホーム] ページにリソース監視が表示されます。プロバイダ タイプと、選択したプロバイダ タイプに属する Horizon Edge でフィルタリングし、[適用] をクリックして、Microsoft Azure や Horizon 8 などのさまざまなプロバイダ タイプのエンド ユーザーの [セッションと仮想マシンのパフォーマンス] に関する [エラー] データとライブ情報を表示できます。



デフォルトでは、ホーム ページには、すべての Horizon Edge のリソース監視データが表示されます。ただし、プール データは除きます。

注： [使用率] セクションの [プール] ボックスは、[Horizon Edge の選択] フィルタを使用して選択した Horizon Edge に関係なく、すべての Horizon Edge のすべてのプールに適用されます。

Horizon Agent 監視データは Workspace ONE Intelligence に伝達され、ライセンスに応じて VMware Horizon® Cloud Service™ - next-gen または Splunk と統合されます。Horizon Agent 監視を有効にすると、VMware Horizon® Cloud Service™ - next-gen との Workspace ONE Intelligence のデータ統合が有効になります。詳細については、Workspace ONE を使用した Horizon Edge の Horizon Edge エージェント データ監視の構成を参照してください。Splunk との VMware Horizon® Cloud Service™ - next-gen のデータ統合を構成する必要があります。詳細については、Splunk Enterprise を使用した Horizon 8 Edge の監視の構成を参照してください。

リソース監視データ：エラー

ホーム ページの [エラー] セクションには、Horizon Edge エラー、プールのプロビジョニング エラー、単一セッション仮想マシン エラー、マルチセッション仮想マシン エラーが一覧表示されます。

リソース エラー タイプごとに、[エラー] セクションには 2/10 などの割合が表示されます。これは、該当のリソースの使用可能な 10 個のインスタンスのうち 2 つでエラーが発生していることを示しています。次の一般的な例では、さらに詳細を示します。

汎用リソース エラー タイプの例

たとえば、[エラー] セクションでリソース エラー タイプの後に 2/10 という割合が表示されている場合、2/10 は、[Horizon Edge の選択] フィルタで選択された Horizon Edge について、それぞれのリソース タイプの 10 個のインスタンスが使用可能で、10 個のインスタンスのうち 2 つでエラーが発生していることを示しています。

注： 2/10 などの割合は、エラーの数を示すものではありません。

エラーが発生している 2 つのリソース（この例の場合）とはどれか、エラーの合計数、エラーの正確な内容など、詳細を取得するには、リソース エラー タイプのリンクをクリックし、次のページのオブジェクト間を移動して、その特定のリソース エラー タイプで使用可能なさまざまなオプションについて確認します。

該当する場合、次のページには、Horizon Universal Console または VMware Cloud Services コンソールの他のページへのリンクが含まれており、そのページが役に立つ場合があります。

次の表に、ホーム ページの [エラー] セクションに表示されるリソース エラー タイプを示します。この表は、各リソース エラー タイプの具体的な例を示します。例の列には、割合の例とその詳細が記載されています。

表 6-1. 特定のリソース エラー タイプの例

リソース エラー タイプ	説明	例
[インフラストラクチャ エラーのある Horizon Edge]	インフラストラクチャ エラーが発生している Horizon Edge。これらのエラーには、Horizon Edge デプロイ エラーは含まれません。 [インフラストラクチャ エラーのある Horizon Edge] ページには、次のコンポーネントから送信されたエラーが含まれます。 ■ Microsoft Azure 環境の Horizon Edge Gateway ■ これらのエラー メッセージには、Microsoft Azure 環境の Horizon Edge Gateway が関係しており、Horizon Edge Gateway でのサービスのデプロイや、Horizon Edge Gateway のサービスの Horizon Cloud Service 制御プレーンとの接続に関するエラーが含まれます。 例として、次のようなエラー メッセージになります。 ■ `Failed to pull module image` ■ `Module is terminating multiple times` ■ `EdgeDevice is disconnected from IoTHub` ■ Microsoft Azure 環境での Unified Access Gateway ■ これらのエラー メッセージには、Unified Access Gateway が関係しており、Edge サービス、認証ブローカ、UT サーバ、Blast サービス、PCOIP プロトコル、およびトンネル RDP などの UAG および関連テクノロジーに関するエラーが含まれます。 例として、次のようなエラー メッセージになります。 ■ `Tunnel Rdp is down` ■ `Failed to fetch UAG certificate` ■ Active Directory ■ これらのエラー メッセージには、Active Directory 関連の接続エラーが関係しており、Active Directory サーバ、バインド アカウント、および参加アカウントに関するエラーが含まれます。例として、次のようなエラー メッセージになります。 `Failed to connect to AD Server {domainName}`	[インフラストラクチャ エラーのある Horizon Edge] リソース エラー タイプ。割合は 2/2。 この 2/2 の例では、2 つの Horizon Edge が使用可能で、両方ともエラーが発生しています。 エラーの合計数やエラーの正確な内容などの詳細を取得するには、[インフラストラクチャ エラーのある Horizon Edge] をクリックして、ページのオブジェクト間を移動します。
[プロビジョニング エラーのあるプール]	プロビジョニング エラーが発生しているプール。	[プロビジョニング エラーのあるプール] リソース エラー タイプ。割合は 3/16。 この 3/16 の例では、16 個のプールが使用可能で、そのうちの 3 つのプールでエラーが発生しています。 エラーが発生しているプール、エラーの合計数、エラーの正確な内容、発生したタイミングなどの詳細を取得するには、[プロビジョニング エラーのあるプール] をクリックします。その後、ページのオ

表 6-1. 特定のリソース エラー タイプの例 （続き）

リソース エラー タイプ	説明	例
		ブジェクト間を移動できます。これには、ページに表示されるプールのフィルタリングが含まれます。

表 6-1. 特定のリソース エラー タイプの例 （続き）

リソース エラー タイプ	説明	例
[エージェント エラーのある単一セッション仮想マシン]	エージェント エラーが発生している単一セッション仮想マシン。 エージェント エラーのある仮想マシンでは、次のエラーの重要度レベルが適用されます。 **重大** 至急の対応が必要です。エージェント内のサービスが停止している可能性があり、エンド ユーザーがデスクトップに接続できない場合があります。 **警告** 潜在的な接続の問題を示します。	[エージェント エラーのある単一セッション仮想マシン] リソース エラー タイプ。割合は 4/34。 この 4/34 の例では、34 台の単一セッション仮想マシンが使用可能で、そのうちの 4 台でエラーが発生しています。 エラーが発生している仮想マシン、エラーの合計数、各エラーの重要度、各エラーに関連付けられているエージェントのバージョン、エラーの正確な内容、発生したタイミングなどの詳細を取得するには、[エージェント エラーのある単一セッション仮想マシン] をクリックして、ページのオブジェクト間を移動します。 また、このページでは、縦に並んだ 3 つのドットをクリックしたときに表示される [ログの生成] オプションを使用して、エラーごとにエージェント ログを収集する便利な方法を提供します。関連するエージェント ログ情報については、Horizon Universal Console を使用した Horizon Agent ログの収集を参照してください。
[エージェント エラーのあるマルチセッション仮想マシン]	エージェント エラーが発生しているマルチセッション仮想マシン。 エージェント エラーのある仮想マシンでは、次のエラーの重要度レベルが適用されます。 **重大** 至急の対応が必要です。エージェント内のサービスが停止している可能性があり、エンド ユーザーがデスクトップに接続できない場合があります。 **警告** 潜在的な接続の問題を示します。	[エージェント エラーのあるマルチセッション仮想マシン] リソース エラー タイプ。割合は 5/52。 この 5/52 の例では、52 台のマルチセッション仮想マシンが使用可能で、そのうちの 5 台でエラーが発生しています。 エラーが発生している仮想マシン、エラーの合計数、各エラーの重要度、各エラーに関連付けられているエージェントのバージョン、エラーの正確な内容、発生したタイミングなどの詳細を取得するには、[エージェント エラーのあるマルチセッション仮想マシン] をクリックして、ページ上のオブジェクトを移動します。 また、このページでは、縦に並んだ 3 つのドットをクリックしたときに表示される [ログの生成] オプションを使用して、エラーごとにエージェント ログを収集す

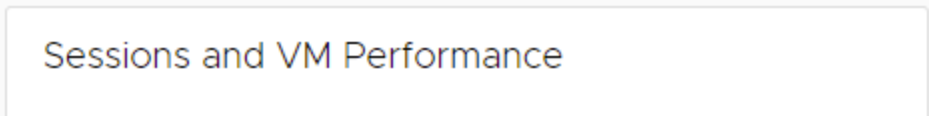
表 6-1. 特定のリソース エラー タイプの例 （続き）

リソース エラー タイプ	説明	例
		る便利な方法を提供します。関連するエージェント ログ情報については、Horizon Universal Console を使用した Horizon Agent ログの収集を参照してください。

リソース監視データ：セッションと仮想マシンのパフォーマンス

ホーム ページの [セッションと仮想マシンのパフォーマンス] セクションには、セッション データと仮想マシンのパフォーマンス データの両方が表示されます。このセクションでは、セッション データを接続済みや切断済みなどのセッション タイプごとに分離し、仮想マシン データを高 CPU、高ディスク遅延、高メモリなどのパフォーマンス カテゴリで分離します。リストされているセッションまたは仮想マシンのパフォーマンス データのタイプに関する詳細を取得するには、監視する特定のセッション タイプまたは仮想マシン パフォーマンス データ タイプへのリンクをクリックし、次のページでオブジェクト間を移動して、使用可能なさまざまなオプションについて確認します。

該当する場合、次のページには、Horizon Universal Console または VMware Cloud Services コンソールの他のページへのリンクが含まれており、そのページが役に立つ場合があります。



セッション

次の詳細は、[セッションとパフォーマンス] セクションで使用可能なセッション データに適用されます。

- セッション タイプ：
  - [接続されたセッション]

    エンド ユーザーのデスクトップまたはアプリケーション セッションが接続されていることを示します。接続されたセッションには、アクティブ セッションとアイドル セッションの両方が含まれます。
  - [切断されたセッション]

    エンド ユーザーのデスクトップまたはアプリケーション セッションが切断されていることを示します。切断されたセッションとログオフされたセッションの違いは、切断されたセッションはキャパシティを消費し続けますが、ログオフされたセッションは消費しないことです。
- セッションの割合の例、5/37 (13%)：

  5/37 (13%) の例は、接続されたセッションと切断されたセッションの両方に適用できます。より具体的な例にするため、セッションが接続されていると仮定します。したがって、37 セッションの合計キャパシティのうち、5 つのセッションが接続されています（アクティブ セッションとアイドル セッションの状態を含む）。これは、合計キャパシティの 13% に相当します。
- プール タイプあたりのセッション数：

セッション タイプをクリックすると、そのセッション タイプのセッション ページが表示されます。セッション ページの上部には、プール タイプ別にセッションを表示するチャートがあります。

前述の例では、[接続されたセッション] が 5/37 と表示されています。[接続されたセッション] をクリックすると、[接続されたセッション] ページには 5 つの接続されたセッションがプール タイプ間でどのように分割されるかを示すチャートが表示されます。内訳は次のようになります。

- RDSH デスクトップ = 2 セッション
- VDI デスクトップ = 1 セッション
- RDSH アプリケーション = 2 セッション

- セッション データ：

  セッション ページには、プール タイプ、セッション状態、ユーザー名、ログイン時間など、さまざまなセッション関連データも表示されます。

  ヒント: ページでのセッション データの表示方法を変更するには、[プール タイプ]、[セッション状態]、[ユーザー名]、[Horizon Edge] など、ページで使用可能な各種のフィルタを使用します。

  2 文字以上入力すると、入力に応じてフィルタリングが開始されます。

- 切断されたセッションからのログオフ：

  切断されたセッションをセッション ページから直接ログオフできます。

仮想マシンのパフォーマンス

次の詳細は、[セッションとパフォーマンス] セクションで使用可能な仮想マシンのパフォーマンス データに適用されます。

- 仮想マシンのパフォーマンス タイプ：

  ヒント: 次の仮想マシンのパフォーマンス タイプでは、[デスクトップ]、[プール]、[Horizon Edge] など、ページで使用可能なフィルタのいずれかを使用して、各ページでパフォーマンス データを表示する方法を変更できます。

  2 文字以上入力すると、入力に応じてフィルタリングが開始されます。

  - [高 CPU 仮想マシン]

    CPU 使用率が 80% 以上の仮想マシンを表示します。

  - [ディスク遅延が大きい仮想マシン]

    ディスク遅延が 20 ミリ秒以上の仮想マシンを表示します。

  - [高メモリ仮想マシン]

    メモリ使用率が 80% 以上の仮想マシンを表示します。

- 仮想マシンのパフォーマンスの割合の例、3/42 (7%)：

3/42 (7%) の例は、すべての仮想マシンのパフォーマンス タイプに適用されます。42 台の仮想マシンのうち、3 台（つまり 7%）がそれぞれのパフォーマンス タイプのフラグをトリガしています。

注： 各仮想マシンのパフォーマンス タイプについて、いずれかの仮想マシンがフラグをトリガすると、次のようにそれぞれの割合の値と相関するラベルに色分けされたバーが表示されます。

- 0 ～ 60% は緑色で、そのパフォーマンス タイプに関する相対的な安全性を示している可能性があります。デプロイの特徴を考慮して、問題のある割合かどうかを判断する必要があります。より具体的な例にするため、仮想マシンのパフォーマンス タイプが「高 CPU 仮想マシン」であると仮定します。したがって、仮想マシンの 60% 以下で CPU 使用率が 80% を超えています。
- 61 ～ 80% は黄色で、そのパフォーマンス タイプに関する潜在的な問題を示しています。
- 81 ～ 100% は赤色で、至急の対応が必要であることを示します。

リソース監視データ：使用率

ホーム ページの [使用率] セクションには、それぞれのリソースの上位、つまり使用率が最も高い 3 つのインスタンスが表示されます。

次の詳細が [使用率] セクションに適用されます。

- 使用中/最大セッション数の割合の例、4/42：

  4/42 の例では、[使用率] セクションにリストされたリソース タイプについて、4 個のセッションがアクティブ、アイドル、または切断済みで、38 個のセッションは使用可能だが使用されていないことを示しています。

- リソース タイプと合計：

  各リソースに付けられたラベル「合計」は、リソース タイプの使用可能なインスタンス数を示します。たとえば、「[プール グループ] 合計 4」は、4 つのプール グループが使用可能であることを示します。

  注： [プール グループ] ボックスは、すべての Horizon Edge のすべてのプール グループに常に適用されます。ただし、[プール] ボックスと [Unified Access Gateway] ボックスは、ホーム ページの [Horizon Edge の選択] フィルタを使用して選択した Horizon Edge に関連付けられているプール グループと Unified Access Gateway インスタンスにのみ適用されます。

- リソース インスタンス
  - 各リソース ボックスには、指定されたリソース タイプの最も使用率の高い 3 つのインスタンスの名前が付けられます。ボックスには、各リソース インスタンスのセッション数を示す棒グラフが含まれています。

    Unified Access Gateway のセッション メトリックは、次のようにプール グループおよびプールのセッション メトリックとは異なります。

    プール グループ

セッション数は、アクティブ セッション、アイドル セッション、および切断されたセッションの合計です。

プール

セッション数は、アクティブ セッション、アイドル セッション、および切断されたセッションの合計です。

Unified Access Gateway

セッション数は、アクティブ セッションとアイドル セッションの合計です。

ヒント: インスタンス バーにカーソルを合わせると、そのリソース インスタンスに関するセッションの詳細が表示されます。

Horizon Agent データに基づくネットワークの監視

インストール済みの Horizon Cloud インスタンスからの通信に基づいて、エンド ユーザーのデスクトップ ネットワークの問題が Horizon Agent インフラストラクチャによって検出されます。Horizon Cloud は、これらのネットワークの問題についてユーザーと通信するために、通知を使用します。

Horizon Agent は、ネットワーク パケット ロス、ネットワーク遅延などのネットワーク トラフィック データを、Horizon Cloud に対して通信します。Horizon Cloud はデータを分析し、直接 Horizon Universal Console へ通知を送信します。通知に関する一般的な情報については、Horizon Cloud Service - next-gen の通知を参照してください。

Horizon Universal Console に「ネットワーク低下が検出されました」などのネットワーク関連の通知が表示されたら、その通知をクリックして、影響を受けるデスクトップの数の詳細を確認できます。影響を受けたデスクトップは、Workspace ONE Intelligence レポートで表示できます。Horizon Universal Console ホーム ページから Workspace ONE Intelligence にアクセスできます。ネットワークの問題を解決するには、エンド ユーザーのデスクトップ ネットワーク インフラストラクチャを確認し、修正を適用します。

エージェント ログの収集

通常、Horizon Agent 診断ログを収集する目的は、管理者に発生している問題を VMware サポートが分析できるようにすることです。このプロセスには、特定の仮想マシンからの診断ログ バンドルの収集が含まれ、最終的には VMware サポートが問題を診断します。DCT バンドル（データ収集ツール バンドル）という用語は、このタイプのログ バンドルに関連して、VMware サポートによって頻繁に使用されます。

Horizon Agent 診断ログの収集は、次の方法で実行できます。

顧客管理者は、Horizon Universal Console を使用してエージェント ログを収集します。

管理者は、テクニカル サポート リクエスト (SR) を発行した後、その SR に応答する際に、割り当てられたサポート チームが、問題を診断するために特定の仮想マシンからの診断ログ バンドルが必要であると判断した場合に、Horizon Universal Console を使用してエージェント ログを収集する傾向があります。

エージェント ログの収集方法の詳細については、「Horizon Universal Console を使用した Horizon Agent ログの収集」を参照してください。

VMware オペレーションがエージェント診断ログにアクセスできるようにオプトインしている顧客の場合、VMware Operations チームは仮想マシン関連のエンドユーザーの問題をデバッグするためにエージェント ログを直接生成します。

問題をより迅速に解決するために、VMware オペレーションは Horizon Agent 診断ログを使用して、仮想マシン関連のエンドユーザーの問題をデバッグします。

- 顧客管理者は、Horizon Universal Console で生成されたログの表示および削除を完全に制御できます。
- Horizon Agent ログは 15 日後に自動的に削除されます。
- エージェント ログをダウンロードするための URL は、ログの有効期限で指定された一定期間のみ有効です。
- この機能をオプトアウトした場合、VMware Operations はエージェント ログを生成、表示、または削除できません。保守性を向上させるために、オプトインしたままにしておきます。

VMware オペレーションによるエージェント ログの収集を許可する方法の詳細については、「VMware Operations による Horizon Agent ログの収集を許可または禁止する」を参照してください。

重要：

- エージェント ログが生成されると、ログは [エージェント ログ] ページに一覧表示され、[監視] - [エージェント ログ] を選択してアクセスできます。[エージェント ログ] ページの [開始者] 列には、組織内の管理者または VMware Operations のどちらによってエージェント ログが生成されたかに関する情報が表示されます。
- エージェント ログが生成または削除されると、[アクティビティ ログ] ページにアクティビティが記録され、確認することができます。[アクティビティ ログ] ページからの管理者とエンド ユーザーのアクティビティの監視を参照してください。
- 診断ログには、Microsoft Windows オペレーティング システム（Windows イベント ログなど）や VMware ソフトウェア コンポーネントなど、デバッグに必要な両方のサードパーティ コンポーネントによって生成されたデータが含まれる場合があります。

  診断ログには、ユーザー名、E メールなどの個人を特定できる情報が含まれる可能性があります。VMware は、診断のコンテキストを失うことなく、このようなデータを難読化することはできません。VMware は、このデータを厳密に診断目的で使用し、他の目的は使用しません。

Horizon Universal Console を使用した Horizon Agent ログの収集

Horizon Universal Console を使用して、特定の仮想マシンのログを生成、ダウンロード、および削除できます。

続行する前に、エージェント ログに関する背景情報を確認します。エージェント ログの収集を参照してください。

管理者は通常、テクニカル サポート リクエスト (SR) を発行した後に、その SR に応答する過程で、割り当てられたサポート チームによって、問題を診断するために特定の仮想マシンからの診断ログ バンドルが必要であると判断した場合に、この機能を使用します。既存のログ エントリは、新しく生成されたログに置き換えられます。将来参照する必要がある既存のログはダウンロードすることができ、不要になれば削除することができます。DCT バンドル（データ収集ツール バンドル）という用語は、このタイプのログ バンドルに関連して、VMware サポート チームによって頻繁に使用されます。

収集するエージェント ログには、次のセキュリティ関連の特性が適用されます。

- Horizon Universal Console で生成されたログを表示および削除する完全な制御が可能です。
- Horizon Agent ログは 15 日後に自動的に削除されます。
- エージェント ログをダウンロードするための URL は、ログの有効期限で指定された一定期間のみ有効です。

- この機能をオプトアウトした場合、VMware Operations はエージェント ログを生成、表示、または削除できません。保守性を向上させるために、オプトインしたままにしておきます。

前提条件

- Horizon Edge Gateway インスタンス、Unified Access Gateway インスタンス、およびプールが準備完了状態であることを確認します。
- 仮想マシン上のエージェントが使用可能であることを確認します。
- この記事は、Microsoft Azure Edge にのみ適用されます。

手順

1 [監視] - [エージェント ログ] の順に選択します。

2 [追加] をクリックします。

3 ログを生成するプールを選択し、[次へ] をクリックします。単一セッション プールまたはマルチセッション プールから選択できます。準備完了状態の仮想マシンのみを使用できます。

4 ログを作成するすべての仮想マシンを選択し、[生成] をクリックします。

[タスクの状況] 列に緑色のチェックマークが表示されている仮想マシンはどれでも選択できます。タスクの状況は、ログ作成中に変化します。この処理には数分かかることがあります。

5 ダウンロードする各ログの [ログのダウンロード] をクリックします。

ログはブラウザを使用してダウンロードされます。

次のステップ

ログ エントリを削除する場合は、削除するログ エントリを選択し、[削除] をクリックして、もう一度 [削除] をクリックします。

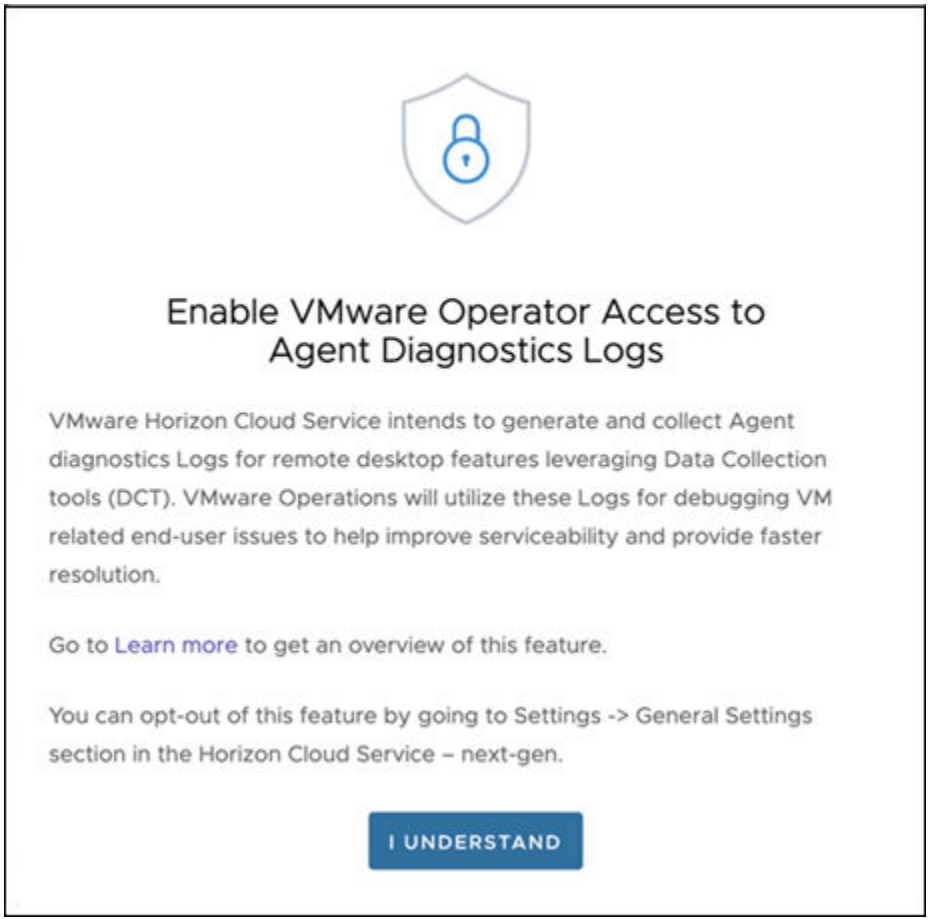
注： 同じプールを使用する場合は、複数のログを選択して削除できます。

VMware Operations による Horizon Agent ログの収集を許可または禁止する

この機能のリリースでは、次に Horizon Universal Console にログインするとき、または Horizon Cloud Service - next-gen への最初のオンボーディングを実行するときに、この機能の目的を説明するダイアログ ボックスが表示されます。確認を行うと、この機能にオプトインされ、VMware Operations が仮想マシンからエージェント診断ログを収集できるようになります。この機能はいつでもオプトアウトすることができます。

続行する前に、エージェント ログに関する背景情報を確認します。エージェント ログの収集を参照してください。

次のスクリーンショットは、VMware Operations がエージェント診断ログにアクセスすることを許可するために表示されるダイアログ ボックスです。



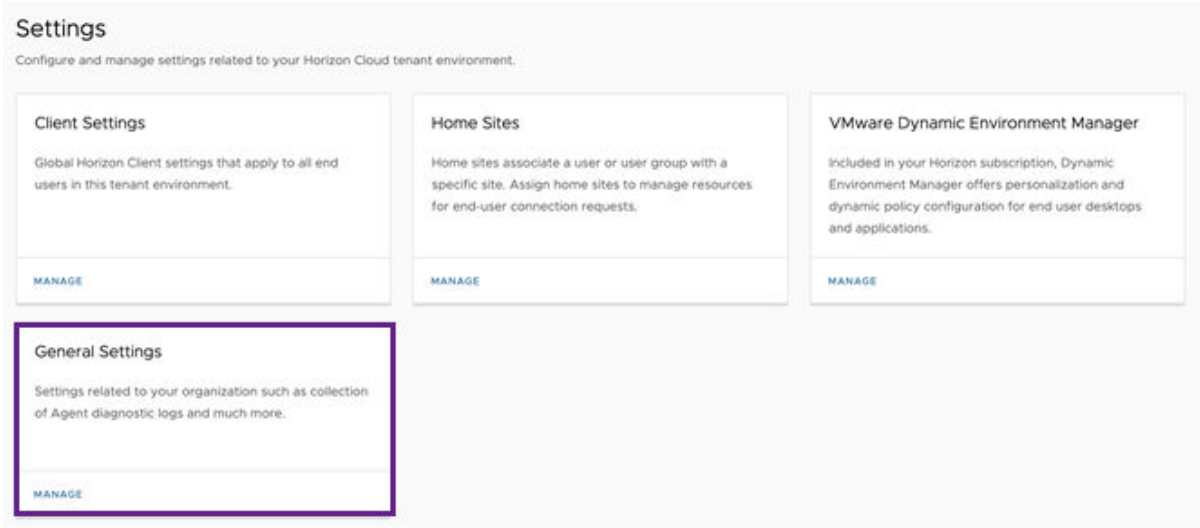
[理解しました] をクリックすると、VMware Operations チームは、特定の問題を解決するために、必要に応じて仮想マシン上にエージェント診断ログを生成し、アクセスできるようになります。

[理解しました] をクリックした後、VMware Operations が Horizon Agent 診断ログを生成および収集することを禁止する場合は、次の手順を実行できます。また、アクセスを禁止することを選択した後で、これらと同じ手順を実行してアクセスを再度許可することができます。

注： プールを作成すると、デフォルトでは、オプトアウトしない限り VMware Operations が仮想マシン上のエージェント診断ログにアクセスすることが許可されます。連絡は E メールと通知によって行われます。通知はページの右上隅にあるベル ( ) アイコンで確認できます。

手順

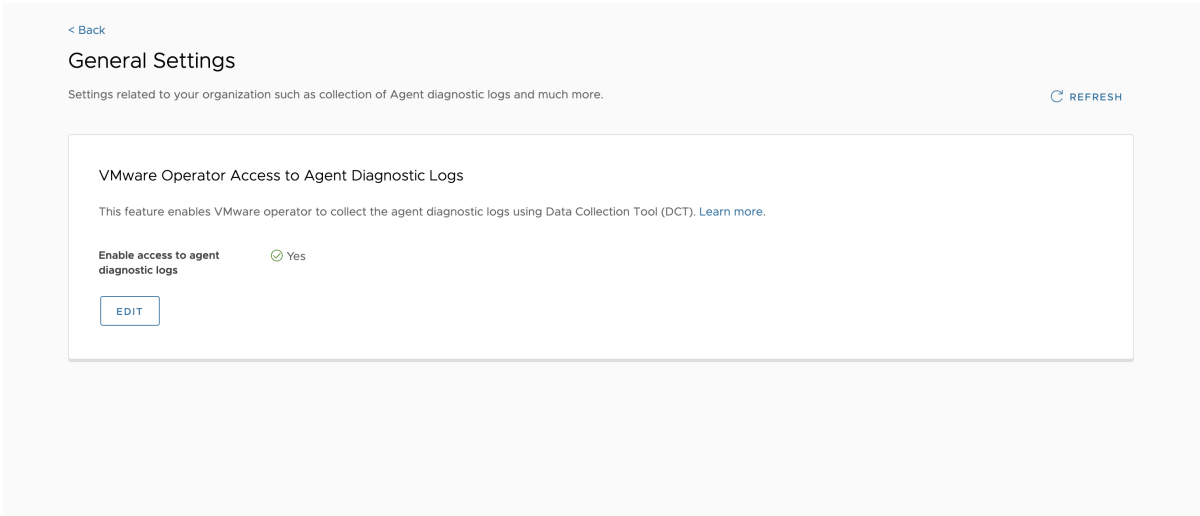
1 Horizon Universal Console で [設定] を選択し、[全般設定] タイルで [管理] をクリックします。



2 [全般設定] ページで、[編集] をクリックします。

3 [エージェント診断ログへのアクセスを有効にする] トグルをクリックして現在の設定を反転します。

4 [保存] をクリックして設定を保存します。



[アクティビティ ログ] ページからの管理者とエンド ユーザーのアクティビティの監視

[アクティビティ] ページには、システムの現在および過去のイベントに関するデータが表示されます。

[アクティビティ ログ] ページにアクセスするには、[監視] - [アクティビティ ログ] を選択します。このページには、監査ログとシステム アクティビティのための [管理者] タブと、ユーザー イベントのための [エンド ユーザー] タブが含まれています。次のタスクを実行できます。

- 各タブで使用可能なフィルタ ツールを使用して、表示されるイベントをフィルタリングする。

- リストを更新する。
- イベント ログを、ダウンロード可能な CSV ファイルにエクスポートします。

管理者イベント

[管理者] タブには、管理者イベントとシステムが開始したイベントの両方に関する情報が表形式で表示されます。イベントを展開して、関連イベント、リソース イベント履歴、サブタスクに関する情報などの詳細を表示します。

イベントのテーブルは、[イベント]、[ステータス]、[タイプ] などのタイトルを含む複数の列で構成されます。[タイプ] 列には、次の 2 つのタイプの管理者イベントが表示されます。

システム

システム アクティビティを示します。

監査

監査ログを示します。監査ログは、管理者および VMware オペレータによって開始されたさまざまな操作によって生成されます。一部の監査ログではアクションの実行が必要になる場合がありますが、多くは情報提供のみを目的としています。たとえば、Horizon Edge Gateway の更新に関連する監査は情報提供のみを目的としています。

次のフィルタ オプションは、[管理者] タブで使用できます。

- タブの上部にあるフィルタを使用して、特定の期間または特定の操作名のイベントのみを表示します。
- 各列のフィルタ ツールを使用してテーブルに表示されるイベントをフィルタします。

ユーザー イベント

[エンド ユーザー] タブには、エンド ユーザー イベントのユーザー名、アクション、ステータス、およびログに記録された時間が表示されます。

これらのフィルタ オプションは、[エンド ユーザー] タブで使用できます。

- タブの上部にあるフィルタを使用して、特定の期間のイベントのみを表示します。
- 各列のフィルタ ツールを使用してテーブルに表示されるイベントをフィルタします。

アクティビティ ログのエクスポート

管理者は、過去 90 日間までの管理者のアクティビティ ログをエクスポートできます。ログは CSV 形式で保存されます。ファイル名にはデフォルトでタイムスタンプが含まれますが、必要に応じてファイル名をカスタマイズできます。

1 Horizon Universal Console のホーム ページで、左側のメニューの [アクティビティ ログ] をクリックします。

2 [イベント] テーブルの上で、すべてのイベントを表示するか、イベントのサブセットを表示するかを選択します。

3 テーブルの列フィルタと、表示する期間（過去 24 時間から 90 日間の範囲）を選択します。

4 [エクスポート] をクリックします。

5 [イベントのエクスポート] ダイアログ ボックスで、エクスポートする csv ファイルの名前を入力し、[エクスポート] をクリックします。[アクティビティ ログ] ページに戻り、ページの上部にステータス メッセージが表示されます。

6 ファイルをダウンロードするには、左側のメニューで [ダウンロード] をクリックします。

7 エクスポートされたファイルの [アクション] 列で、[ダウンロード] リンクをクリックします。

8 ファイルの内容を表示するには、[ダウンロード] リストでファイルをダブルクリックします。イベント名、説明、タイプ、開始者、ステータス、サイト名、Edge 名、時間、リソース名と ID、および重要度のフィールドがファイルに含まれます。

Horizon Universal Console リアルタイム データの詳細

Horizon Universal Console の特定の画面に表示されるデータとインサイトは遅延する可能性があり、リアルタイムではないことに注意してください。監視データは Horizon Agent から取得され、Workspace ONE Intelligence データ レイクに送信されます。Horizon Universal Console は、データ レイクをクエリしてダッシュボードに入力します。

エージェントから報告された監視データのエンドツーエンドの処理には時間がかかり、Horizon Universal Console に表示されるまでに遅延が発生する可能性があります。遅延は平均で約 5 分です。最悪のシナリオでは、このエンドツーエンドの処理によって最大 30 分の遅延が発生する可能性があります。

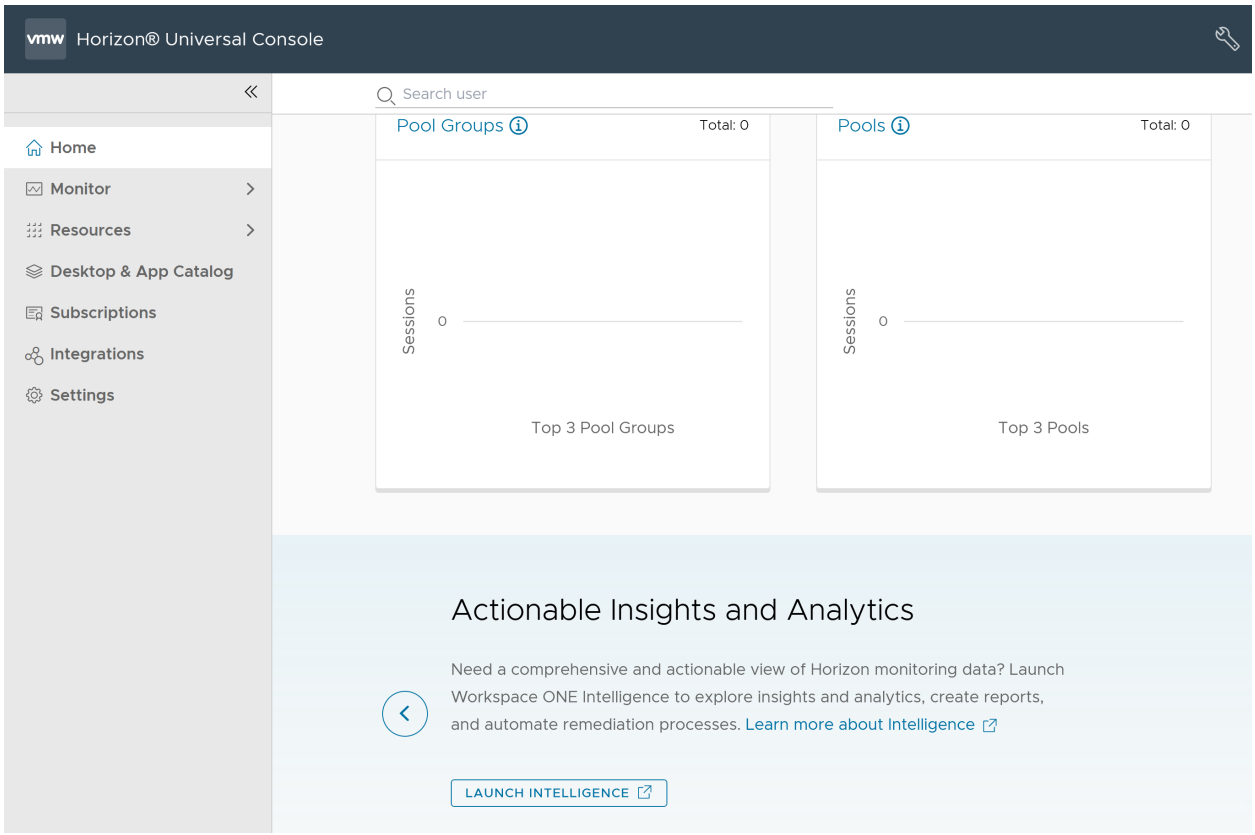
次の Horizon Universal Console 画面では、Workspace ONE Intelligence データ レイクからデータを取得するときに遅延が発生することがあります。

- Horizon Universal Console のホーム ページ。
  - エラー
  - セッションと仮想マシンのパフォーマンス
  - プール グループ、プール、および Unified Access Gateway について表示される使用率データ
- 次のページに表示される Horizon セッション情報。
  - [リソース] - [プール] で、特定のプールの名前をクリックすると、その特定のプールで起動されたセッションの詳細が表示されます。
    - [概要] ページ
    - [セッション] ページ
  - [リソース] - [プール グループ] で、特定のプール グループの名前をクリックすると、その特定のプール グループで起動されたセッションの詳細が表示されます。
    - [概要] ページ
    - [セッション] ページ
  - ヘルプ デスク/ユーザー カード機能を使用しているとき（管理者が [仮想マシンの詳細] ページで特定の仮想マシンまたはセッションの詳細にアクセスしようとするとき）。

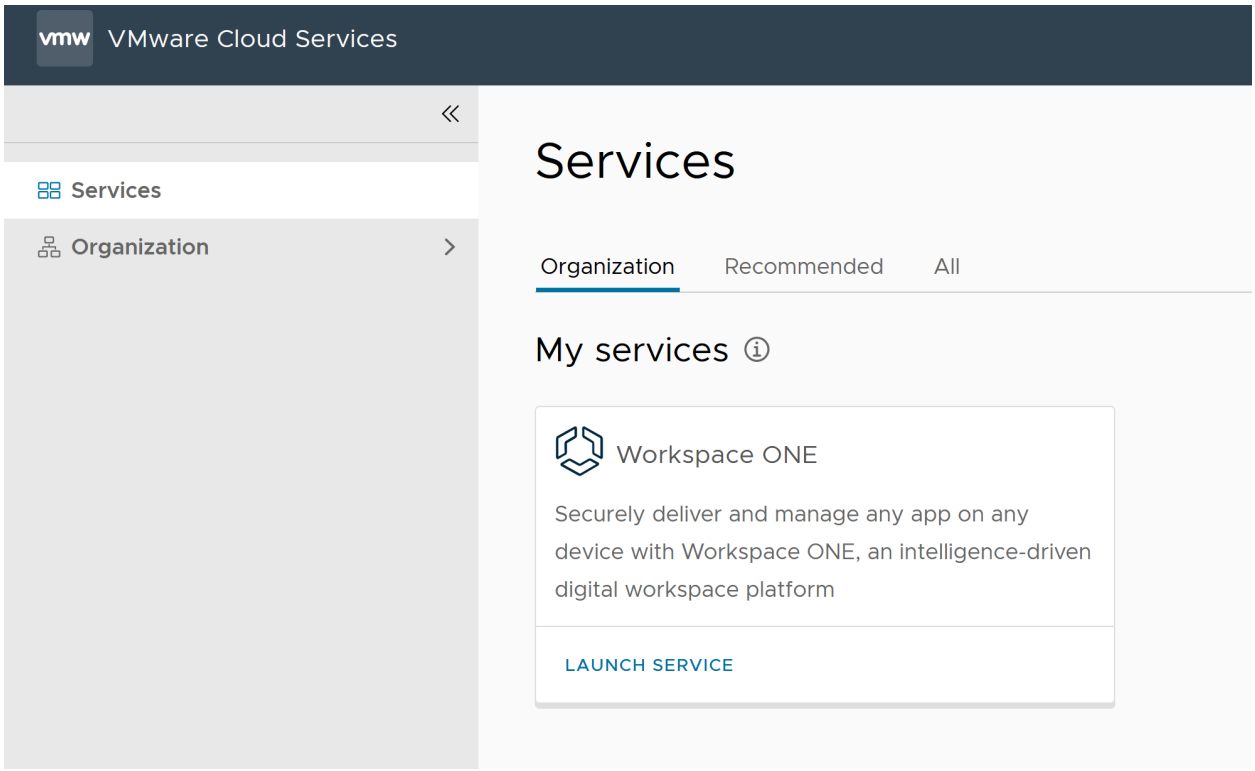
Workspace ONE Intelligence での Horizon Cloud の監視

Horizon Cloud デプロイが Workspace ONE Intelligence と統合されている場合は、Workspace ONE Intelligence を使用して Horizon Cloud ダッシュボードを表示し、レポートを作成できます。

Workspace ONE Intelligence は、Horizon Universal Console のホーム ページの [実行可能なインサイトと分析] セクションで確認できます。



Workspace ONE サービスを起動すると、ライセンスで表示する資格があるすべてのサービスが表示されます。



Horizon Cloud ダッシュボードの移動と表示、レポートの作成の詳細については、VMware Workspace ONE Intelligence 製品ドキュメントのトピック「VMware Horizon 統合」を参照してください。

Workspace ONE を使用した Horizon Edge の Horizon Edge エージェント データ監視の構成

Horizon Agent バージョン 2212 の場合、Horizon Edge（Horizon 8 と Microsoft Azure）の Horizon Agent 監視を手動で有効にすることで、Workspace ONE および Horizon Universal Console に表示される仮想マシンからメトリックを収集できます。

手順

1 vCenter Server コンソールにログインします。

2 Horizon Agent をダウンロードしてインストールします。

- Horizon Agent バージョン 2212 の場合は、Horizon Agent をダウンロードし、パラメータ `HORIZON_MONITOR_ENABLED=1` を渡すサイレント インストール（たとえば、`horizon.exe /s /v "/qn HORIZON_MONITOR_ENABLED=1"`）を実行します。詳細については、Horizon Agent のサイレント インストール プロパティを参照してください。
- Horizon Agent バージョン 2303 以降の場合は、Horizon Agent をダウンロードしてインストールします。Horizon Agent のバージョンが 2303 の場合、監視はデフォルトで有効になっており、データは Workspace ONE クラウドに送信されます。

  注： エージェントによるメトリックの収集を停止し、監視を無効にしたい場合は、カスタマー サポートにお問い合わせください。

3 仮想マシンを再起動します。

4 Horizon Agent バージョン 2212 の場合のみ、レジストリに移動し、`HKLM\Software\VMware, Inc.\VMware HzMon\enabled=1` フラグが有効になっているかどうかを確認します。

5 セッションと仮想マシンの使用率データが Workspace ONE ダッシュボードと Horizon Universal Console で表示できることを確認します。

Horizon 8 環境での Horizon Edge Gateway および Unified Access Gateway のインフラストラクチャ データの監視

Horizon Universal ライセンスを持っている場合に、Horizon 8 環境に Horizon Edge をデプロイすると、[インフラストラクチャ監視] タブにアクセスできます。このタブでは、その Horizon Edge のインフラストラクチャ コンポーネントを監視できます。インフラストラクチャ データは現在、その Horizon Edge の Unified Access Gateway および Horizon Connection Server インスタンスに関する情報で構成されています。

[インフラストラクチャ監視] タブにアクセスするには、[リソース] - [キャパシティ] の順に選択し、Horizon Edge ページで、ソース列に「プライベート データセンター」の値がある Horizon Edge の名前をクリックします。Horizon Edge の詳細ページで、[インフラストラクチャ監視] タブをクリックします。その Horizon Edge に対して変更を行うには、特定の Horizon Edge の詳細を表示し、アクションを実行するを参照してください。

Connection Server

Connection Server セクションには、その特定の Horizon Edge にデプロイされたすべての Horizon Connection Server インスタンスが一覧表示されます。特定の Horizon Connection Server インスタンスに関するインフラストラクチャ データを表示するには、そのインスタンスの [表示] をクリックします。この Horizon Connection Server インスタンスに関する詳細を示すページが開きます。

データには、その特定の Horizon Connection Server インスタンスに関する次の情報が含まれます。

- 指定した期間（最大 24 時間）、使用中の利用可能な CPU の割合
- 指定した期間（最大 24 時間）、使用中の使用可能なメモリの割合
- 現在使用中のセッション数
- 現在のユーザー数
- [サービス] セクションの Horizon Connection Server の依存コンポーネントの健全性
- [証明書] セクションの Horizon Connection Server 証明書の有効性

このデータは、Horizon Connection Server インスタンスおよび関連サービスの健全性と使用状況を判断するのに役立ちます。また、個々の Horizon Connection Server インスタンスおよびその Horizon Edge のクラスタのサイズ要件を決める上でもデータは有用です。

Unified Access Gateway

UAG アプライアンスとその全体的なステータスを表示できます。特定の UAG サーバを監視するには、その UAG インスタンスの [表示] をクリックします。ページが開き、次の情報が表示されます。

- 指定した期間（最大 24 時間）、使用中の利用可能な CPU の割合
- 指定した期間（最大 24 時間）、使用中の使用可能なメモリの割合

- 現在使用中のセッション数
- [サービス] セクションで、UAG モジュールの健全性
- [構成] セクションで、UAG サーバの構成の詳細

SNMP を使用した Horizon Edge Gateway の監視

この記事では、Horizon Edge Gateway の簡易ネットワーク管理プロトコル (SNMP) の設定を有効にして構成する方法について説明します。この構成により、ネットワーク管理システムを介して主要な Horizon Edge Gateway イベントを監視できます。

Horizon Edge Gateway での SNMP 監視の仕組み

Horizon Edge Gateway は、特定のイベントが発生したときに Horizon Edge Gateway アプライアンスから発生する SNMP トラップの使用による監視をサポートします。これらのトラップは、ネットワーク管理システムにトリガ イベントや条件を通知します。

注： Horizon Edge Gateway はトラップ エミッタとしてのみ機能し、`GET`、`GETBULK`、`GETNEXT` の操作の受信など、その他の SNMP 操作はサポートしません。

Horizon Edge Gateway の SNMP 監視を有効にするには、この記事の説明に従って SNMP 監視を構成する必要があります。

MIB（Management Information Base）ファイルでは、管理対象デバイスから提供可能な情報を定義する、トラップ定義が含まれています。MIB ファイルには、オブジェクト識別子 (OID) 別に記述された管理対象オブジェクトと階層別に整理された変数が定義されています。この記事の後半で提供するリンクを使用して、必要な MIB ファイルをダウンロードできます。

SNMP トラップで監視できる Horizon Edge Gateway イベント

アプライアンスの SNMP サービスを有効にして構成すると、Horizon Edge Gateway は以下のイベントの SNMP トラップをサポートします。

- 現在、ライセンス プッシュ失敗の監視がサポートされています。

各イベントにより、アプライアンスからネットワーク管理システムへの SNMP トラップの送信がトリガされます。

Horizon Edge Gateway の SNMP 監視の構成方法

SNMP 構成プロセスの手順全体の概要は以下のとおりです。

- 手順 1：ネットワーク管理システムで使用する VMware MIB ファイルをダウンロードします。
- 手順 2：Horizon Universal Console で SNMP サービスを有効にして構成します。
- 手順 3：Horizon Universal Console を使用して、Horizon Edge Gateway エンジン ID を表示します。

前提条件および各手順の詳細については、以降のセクションを参照してください。

前提条件

- Horizon Plus ライセンスまたは Horizon ユニバーサル ライセンスを使用して Horizon Edge をデプロイします。「リソース キャパシティ プロバイダへの Horizon Edge のデプロイ」を参照してください

- SNMP トラップを受信できる SNMPv3 トラップ レシーバが構成されている必要があります。
- Horizon Edge Gateway が SNMP レシーバにアクセスできることを確認します。通常、SNMP トラップのデフォルト ポートは 162 です。

> **注：** SNMP ベースの監視は、Horizon Edge Gateway でのみサポートされます。

手順 1：VMware MIB ファイルと OID のダウンロード

管理情報の構造 (SMI) に関する RFC 2578 標準は、特定の製品および機能の管理情報ベース (MIB) ファイルの記述に使用される構文です。これらの MIB ファイルは、製品とは別にバージョン管理され、イベント タイプおよびイベント データ関連情報の識別に使用できます。

これらの MIB ファイルをダウンロードするには、「VMware ナレッジベースの記事 KB1013445」を参照して、VMware-mibs-8.6.0NX-22397641 をダウンロードしてください。

MIB ファイルで使用されるオブジェクト識別子 (OID) をダウンロードするには、VMware ナレッジベースの記事 KB2054359 を参照してください。

手順 2：Horizon Universal Console を使用した SNMP サービスの有効化と構成

SNMP サービスの設定には、Horizon Universal Console からアクセスできます。

1 Horizon Universal Console で [統合] を選択し、SNMP タイルで [管理] をクリックします。

2 [SNMP] 画面で、[追加] をクリックします。

[SNMP の追加] ウィザードが起動します。

3 構成名、ユーザー名、およびセキュリティ レベルの設定を、次の表の記載どおりに指定します。

設定	説明
[SNMP バージョン]	このリリースは、SNMPv3 のみをサポートしています。
[SNMPv3 構成名]	受信者の構成を識別するためのユーザー指定の名前。
[SNMPv3 USM ユーザー名]	SNMP 監視情報にアクセスできる、SNMPv3 USM（ユーザーに基づくセキュリティ モデル）のユーザーを構成します。ユーザー名は、8 文字から 31 文字の長さで、英数字のみを使用する必要があります。
[SNMPv3 セキュリティ レベル]	SNMP サービスで、プライバシー アルゴリズムの有無にかかわらず、オプションの認証アルゴリズムを使用するかどうかを指定します。認証は、ユーザーの ID を確認するために使用します。プライバシーを使用すると、SNMPv3 メッセージを暗号化してデータの機密性を保証できます。 認証およびプライバシーは、どちらもオプションです。ただし、プライバシーを有効にするには、認証を有効にする必要があります。

4 （オプション）認証を含むセキュリティ レベルを指定した場合は、次の表の記載内容に従って認証の詳細を構成します。

設定	説明
[SNMPv3 認証アルゴリズム]	SNMP ユーザーの ID を確立するために使用する認証アルゴリズムを指定します。
[SNMPv3 認証パスワード]	ユーザーの ID を確立するための認証アルゴリズムに必要なパスワードを構成します。認証パスワードの長さは 8 文字から 31 文字までにする必要があります。
[認証パスワードの確認]	認証パスワードを再入力します。

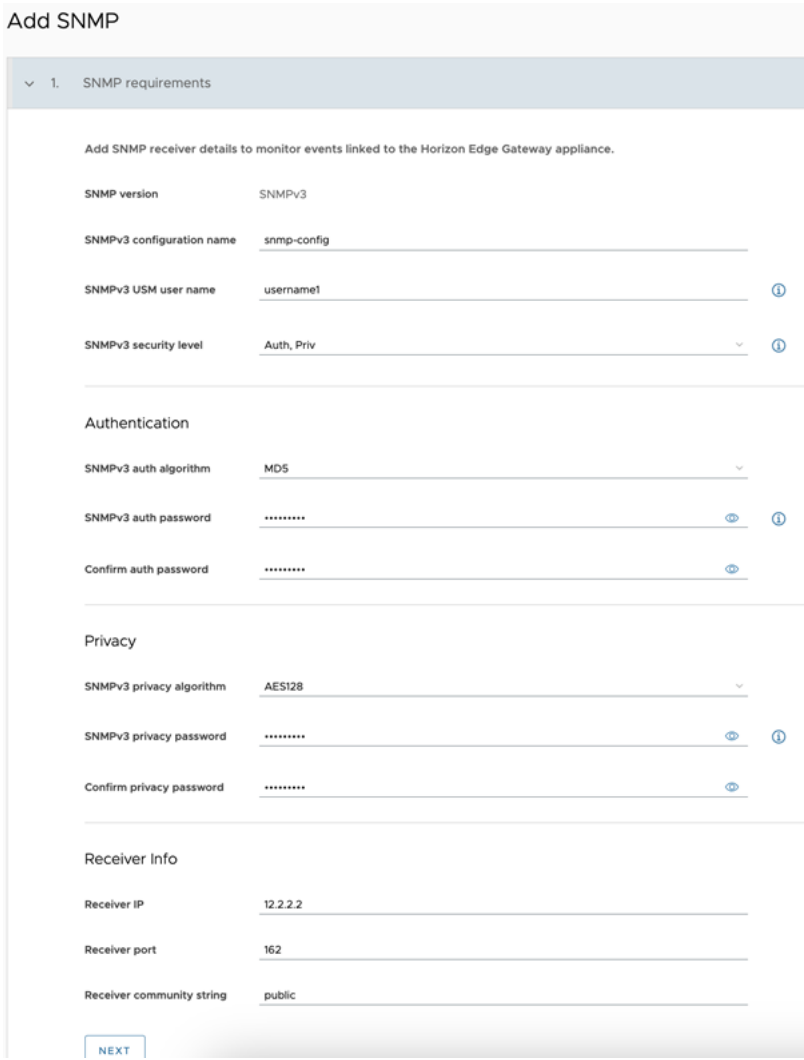
5 （オプション）認証とプライバシーの両方を含むセキュリティ レベルを指定した場合は、次の表の記載内容に従ってプライバシーの詳細を構成します。

設定	説明
[SNMPv3 プライバシー アルゴリズム]	SNMP メッセージの暗号化に使用するプライバシー アルゴリズムを指定します。
[SNMPv3 プライバシー パスワード]	暗号化キーを生成するためのプライバシー アルゴリズムに必要なパスワードを構成します。プライバシー パスワードの長さは 8 文字から 31 文字までにする必要があります。
[プライバシー パスワードの確認]	プライバシー パスワードを再入力します。

6 次の表の説明に従って、Horizon Edge Gateway から SNMP トラップを受信できる SNMP レシーバの IP アドレスとポートの詳細を指定し、[次へ] をクリックします。

設定	説明
[レシーバの IP アドレス]	SNMP トラップを受信できる、ネットワーク管理システムの IP アドレスを指定します。
[レシーバ ポート]	トラップを受信するためのネットワーク管理システムが使用するポート番号を指定します。
[レシーバのコミュニティ文字列]	受信したトラップが Horizon Edge Gateway から発生していることを検証するために、ネットワーク管理システムが使用するコミュニティ文字列を入力します。

次のスクリーンショットは、設定が構成された [SNMP の追加] フォームの例を示しています。

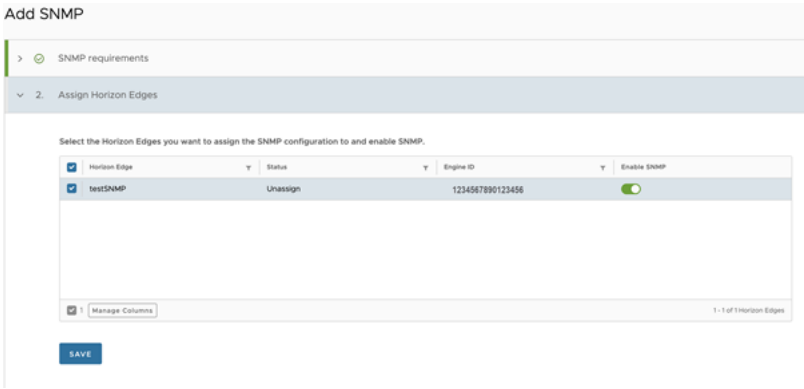


構成に成功すると、SNMP 構成が追加されたことを示すメッセージが表示されます。

7 [Horizon Edge の割り当て] セクションで、SNMP 構成に割り当てる Horizon Edge を選択します。

複数の Horizon Edge を単一の SNMP の構成に割り当てることができます。ただし、複数の SNMP 構成に Horizon Edge を割り当てることはできません。Horizon Edge が SNMP 構成に割り当てられると、Horizon Edge のリストに表示されなくなります。

SNMP 構成を Horizon Edge に割り当てると、エンジン ID が作成されます。



8 選択した Horizon Edge の SNMP 監視を有効にするには、[SNMP を有効にする] トグルがオンになっていることを確認します。

注： [SNMP を有効にする] トグルのデフォルトの状態は、Horizon Edge の関連付け中にオンになっています。

9 [保存] をクリックします。

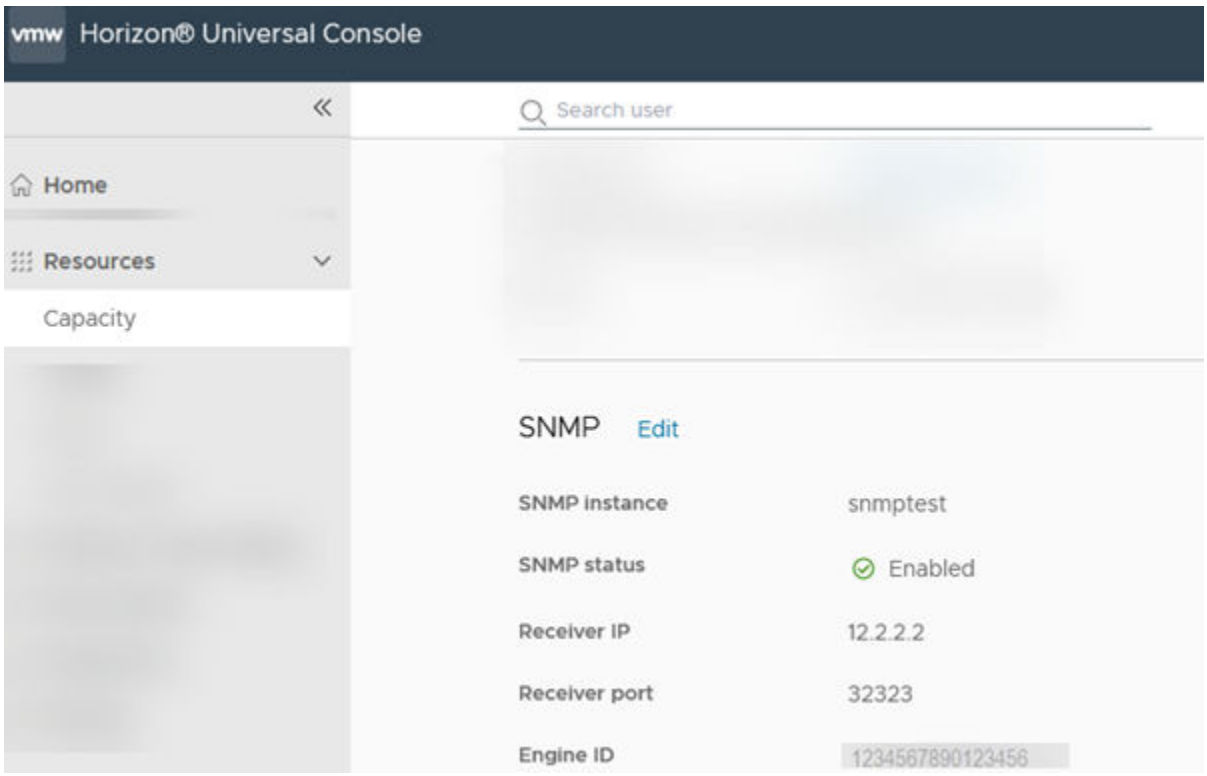
手順 3：Horizon Universal Console を使用して特定の Horizon Edge Gateway の SNMP エンジン ID を取得する

SNMP の有効化プロセス中に、ネットワーク管理システムで使用する一意の SNMP エンジン ID が、Horizon Edge Gateway によって自動生成されます。エンジン ID は、ハッシュ機能によって、SNMP v3 メッセージの認証と暗号化のための鍵を生成するために使用されます。

注： SNMP レシーバを構成し、その Horizon Edge Gateway から送信される SNMP トラップ メッセージを識別するには、SNMP エンジン ID が必要です。

- Horizon Universal Console を使用して、Horizon Edge の SNMP エンジン ID に移動します。
  a [リソース] - [キャパシティ] - [] の順に選択します。
  b SNMP 構成を割り当てた Horizon Edge の名前をクリックします。
  c [SNMP] セクションまでスクロールし、[エンジン ID] の値を見つけます。

  次のスクリーンショットは、Horizon Universal Console に表示される自動生成された SNMP エンジン ID の例を示すものです。



次の手順

[SNMP] 画面にいつでも戻って、既存の SNMP 構成を編集または削除することができます。SNMP 構成を編集して、SNMP レシーバの詳細または SNMP の関連付けを変更できます。SNMP 構成を削除するには、まず構成を編集して、割り当てられた Horizon Edge の割り当てを解除します。

Horizon 8 Edge の Horizon サブスクリプション ライセンスの監視

Horizon サブスクリプション ライセンスは、Horizon Edge デプロイ、Horizon Connection Server、および Horizon Cloud ライセンス サービス間で動作可能な通信チェーンに依存します。ライセンス サービスは 24 時間ごとに Horizon 8 Edge と同期します。ライセンスの同期に失敗し、サービスが中断する可能性があります。Horizon Cloud Service - next-gen は、さまざまな方法でライセンス同期の失敗を通知しようとします。常に通知を受け取る方法の 1 つは、Horizon Universal Console を使用してサブスクリプション ライセンスのライセンス同期ステータスを監視し、同期の問題をトラブルシューティングすることです。

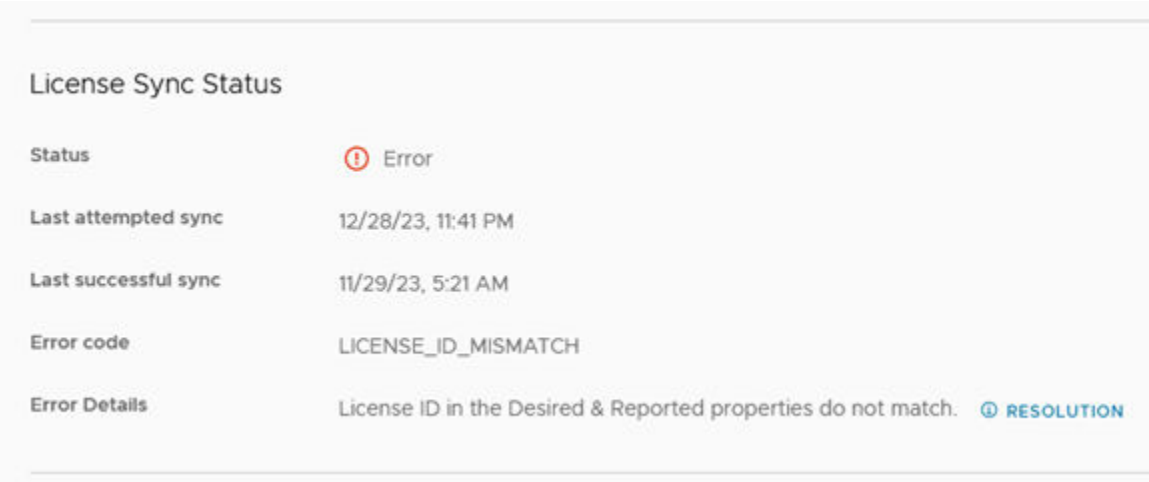
ライセンス通信チェーンのいずれかのリンクが動作不能になると、ライセンスの同期は失敗し、Horizon 8 Edge はサブスクリプション ライセンスの使用許諾契約書の条件に準拠しなくなります。ただし、サブスクリプション ライセンスおよび Horizon Edge は動作可能なままなので、同期エラーの原因を調査して修正するための時間があります。エラーが長時間続くと、Horizon Edge へのサービスが中断され、Horizon Edge は動作不能になります。その後、エンド ユーザーは Horizon Edge 上のリモート デスクトップおよびアプリケーションに接続できなくなります。

以下のセクションでは、Horizon Cloud Service - next-gen がライセンス同期ステータス情報を提供するいくつかの方法について説明します。

Horizon Edge の詳細ページでのサブスクリプション ライセンスの同期ステータス

サブスクリプション ライセンスの同期のステータスは、特定の Horizon 8 Edge の詳細ページで確認できます。ライセンスの同期に失敗した場合は、サブスクリプション ライセンスの同期ステータス情報を使用して失敗のトラブルシューティングを行うことができます。

[リソース] - [キャパシティ] を選択し、[Horizon Edge] タブを選択して、Horizon 8 Edge の名前をクリックし、[サブスクリプション ライセンスの同期ステータス] セクションまでスクロールします。



注： [サブスクリプション ライセンスの同期ステータス] セクションは、Horizon 8 タイプの Edge でのみ使用できます。

[サブスクリプション ライセンスの同期ステータス] セクションには、次のタイプの情報が一覧表示されます。

ステータス	ライセンス同期のステータスは、次のいずれかになります。 ■ [エラー] ■ [成功]
最後に試行された同期	ライセンス同期ジョブの最終実行日
最後の正常同期	ライセンス同期の最終成功日
エラー コード	エラー コード（ある場合）。
エラーの詳細	解決のヒントなど、エラーに関する具体的な情報。

管理アクティビティ ログのサブスクリプション ライセンス同期ステータス

管理アクティビティ ログには、ライセンス同期ステータスに関する情報が含まれます。

[アクティビティ ログ] ページにアクセスするには、[監視] - [アクティビティ ログ] を選択します。ページが開き、[管理] タブが選択されます。[アクティビティ ログ] ページからの管理者とエンド ユーザーのアクティビティの監視を参照してください。

ライセンス同期のアラート通知

ライセンス同期の失敗が数日続けて発生すると、3 日目から、影響を受ける各 Horizon 8 Edge はライセンス同期の失敗に関する通知を Horizon Universal Console に送信します。Horizon Cloud Service - next-gen の通知を参照してください。

ライセンス同期のアラート E メール

ライセンス同期の失敗が数日続けて発生すると、3 日目から、システムはサブスクリプション ライセンスの同期の失敗を知らせる E メールを送信します。

Horizon Agent ソフトウェアの管理

Horizon Agent は、仮想マシンを Horizon Cloud とペアリングするために必要なエージェント ソフトウェアです。エージェントを管理して、最新の機能とバグ修正が適用された最新の状態に保つ必要があります。

仮想マシン上で、このエージェントは Horizon Cloud Service と通信して、仲介、接続の監視、統合印刷、ローカルに接続された USB デバイスへのアクセスなどの機能を提供します。

Horizon Agent バージョンを最新の状態に保つ

Horizon Cloud では、さまざまな方法を使用して、仮想マシンにデプロイされた Horizon Agent ソフトウェアが使用可能な最新バージョンでないことを通知します。

プール、プール グループ、イメージに関連するいくつかの Horizon Universal Console ページでは、関連付けられた Horizon Agent が最新ではないとユーザーに通知されます。ベスト プラクティスとして、エージェントのバージョンを最新の状態に保ちます。

Horizon Agent のバージョン ラベル

Horizon Agent のバージョン ラベルは、リソース（プール グループ、プール、またはイメージ）のエージェント バージョンが最新かどうかを示します。エージェントが最新でない場合、ラベルはさらにエージェントがどの程度古いかを示します。

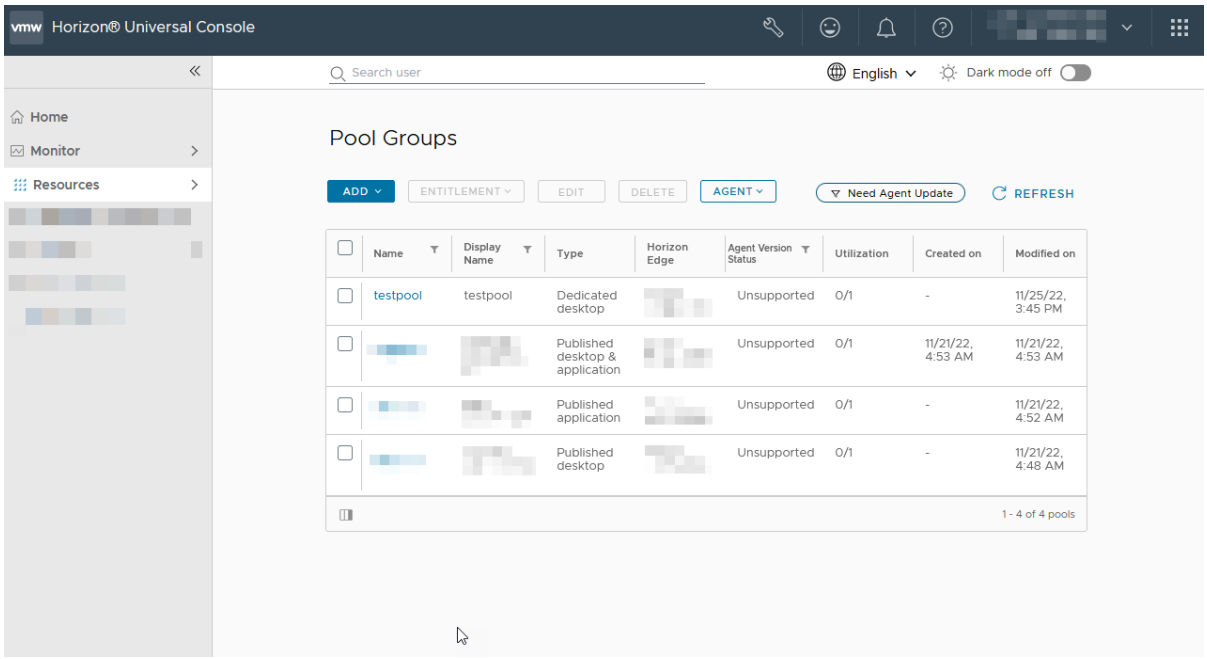
Horizon Agent のバージョン ラベル	説明
[最新]	最新のエージェント バージョンが仮想マシンにインストールされています。
[期限切れ]	一部の仮想マシンには、期限切れのエージェントがあります。
[サポート対象外]	一部の仮想マシンには、期限切れでサポートされないエージェントがあります。
[リスクあり]	一部の仮想マシンには、セキュリティまたは機能に関する重大な問題が発生しているエージェントがあります。

Horizon Agent バージョン情報の例

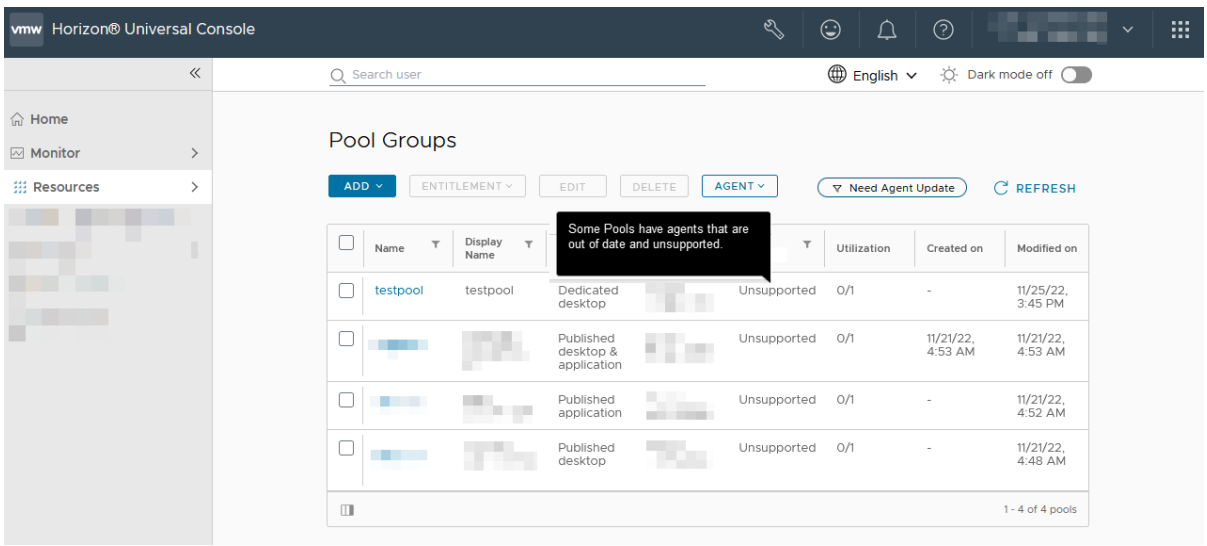
次のスクリーンショットは、Horizon Agent バージョン統計情報の表示方法の例を示しています。これは、[プール グループ] ページの例です。

[プール グループ] ページの例

[プール グループ] ページには、[エージェント バージョンのステータス] 列があります。次のスクリーンショットでは、各プール グループの [エージェント バージョンのステータス] ラベルが [サポート対象外] になっています。



次のスクリーンショットに示すように、[エージェント バージョンのステータス] ラベルにカーソルを合わせると、説明が表示されます。



専用デスクトップ仮想マシンでの Horizon Agent ソフトウェアの更新

Horizon Agent の更新には、新機能やバグ修正が含まれる場合があります。この手順を使用して、専用デスクトップ仮想マシンにインストールされている Horizon Agent ソフトウェアを更新します。

注： 次世代環境にまだ完了していない第 1 世代の移行が含まれている場合、システムでは、次世代環境で直接作成されたプール グループでも、このエージェントの更新手順を実行できません。このシナリオでは、[エージェントの更新] をクリックすると、移行を完了する必要についてのガイダンス メッセージがコンソールに表示されます。

専用デスクトップ仮想マシンにインストールされている Horizon Agent ソフトウェアを更新するには、Horizon Universal Console を使用します。[プール グループ] ページでエージェントの更新プロセスを開始すると、プロセスのフォーカスがプール グループからプールに移動します。次に、プール レベルでエージェントの更新を有効にします。システムは専用デスクトップ仮想マシンの Horizon Agent ソフトウェアを使用可能な最新バージョンに更新します。

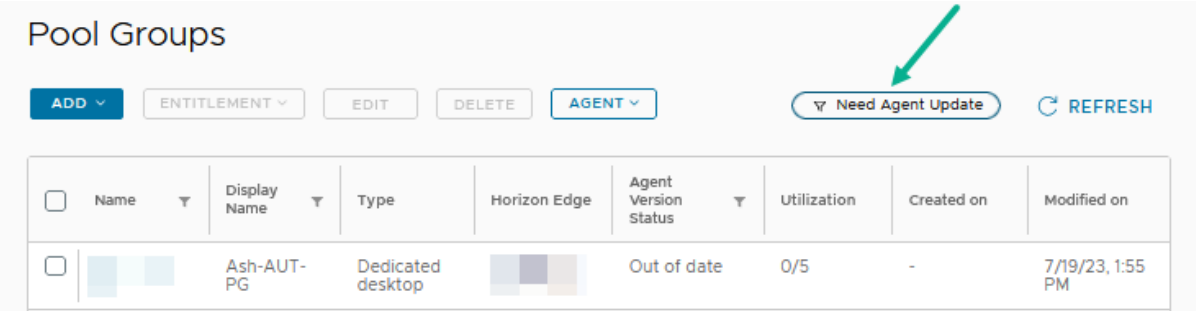
注意： エージェントの更新処理が進行中のときには、プール グループのデスクトップ仮想マシンのいずれかに電源変更操作が発生する可能性のある他のアクティビティが予定されていないことを確認する必要があります。たとえば、他の管理者に対して、これらのデスクトップ仮想マシンを手動でパワーオフまたはパワーオンしないように通知したり、このプール グループ内で構成された電源管理スケジュールによって、エージェントの更新タスクの実行中にデスクトップのパワーオンやパワーオフが行われないようにします。システムで仮想マシンのエージェントの更新タスクを実行しているときに、デスクトップ仮想マシンにおいて電源変更操作が行われると、予期しない結果が発生し、デスクトップ仮想マシンが手動でリカバリしなくてはならない状態になる可能性があります。

ベスト プラクティスは、プール グループを編集し、構成された電源管理スケジュールをすべて削除することで、エージェントの更新タスクの実行中に電源変更操作が行われないようにすることです。

手順

1 Horizon Universal Console で、[プール グループ] ページに移動します。

[プール グループ] ページの次のスクリーンショットは [エージェントの更新が必要] オプションを示しています。



2 （オプション）[エージェントの更新が必要] フィルタで最新のエージェントの更新を使用できるようにするには、エージェントの更新がないか確認するためにプール グループをスキャンできます。

注： プール グループおよびプールの数によっては、更新のスキャンに数分かかる場合があります。

Horizon Cloud は、エージェントの更新について、プール グループ全体のデスクトップを毎日自動的にスキャンします。[更新のスキャン] アクション ラベルには、最後にスキャンされた時間が表示されます。プール グループについてエージェントを直ちにスキャンする場合は、次のように [更新のスキャン] アクションを使用します。

a [エージェント] - [更新のスキャン] の順に選択します。

このプロセスはバックグラウンドで実行されます。ステータスは [アクティビティ ログ] ページに表示されます。

b 進行状況を表示するには、[アクティビティ ログ] ページに移動します。

アクティビティ ログの詳細については、[アクティビティ ログ] ページからの管理者とエンド ユーザーのアクティビティの監視を参照してください。

3 エージェントの更新の対象となるデスクトップ仮想マシンを含むプール グループのみで構成されるようにリストをフィルタリングするには、[エージェントの更新が必要] をクリックします。

前述の手順で更新をスキャンした場合、このリストのデータには、スキャン中に検出された更新が含まれます。そうでない場合、リストは自動化された日次スキャンや特定のイベントなど、以前のスキャンで計算されたデータで構成されます。

4 プール グループを 1 つ以上選択します。

5 [エージェント] - [エージェントの更新] の順に選択します。

注： 環境にまだ完了していない第 1 世代の移行が含まれている場合、コンソールではエージェントの更新ウィザードを実行できません。

[エージェントの更新] ウィザードが起動し、選択したプール グループを対応するプールのリストに分割するページが表示されます。各プール テンプレートには、エージェントの更新の対象となる 1 台以上の仮想マシンが含まれます。

6 更新する仮想マシンを含むプールをリストから選択し、[次へ] をクリックします。

7 [詳細] フォームの入力を完了し、[保存] をクリックします。

オプション	説明
[アクティブなユーザーを含む仮想マシンのスキップ]	選択すると、アクティブなセッションまたは切断されたセッション用の Horizon Agent の更新をスキップします。このオプションが選択されていない場合、更新の開始時に仮想マシンにログインしたユーザーは 5 分間の警告が表示されてから強制的にログオフされます。
[ジョブのタイムアウト]	システムがエージェントの更新を自動的に試行し続ける期間を設定します。特定の期間にのみ更新を実行する場合は、複数のテンプレートと仮想マシンを選択している場合でも、短い期間を設定できます。仮想マシンの状態、およびその他の待機時間と実行中の再試行に応じて、仮想マシンの 1 つのバッチに 20 ～ 60 分かかることがあります。 たとえば、600 台を超える仮想マシンがあり、30 台の仮想マシンを同時に更新する場合、期間は次のように計算できます。 ■ バッチ数：600/30 = 20 バッチ ■ ジョブのタイムアウト：20*60 = 1200 分 ジョブのタイムアウトを 1200 分に設定します。これは、更新の実行に通常必要な期間よりもかなり長くなります。 **注：** 更新中にエラーが発生した仮想マシンの更新は再試行されません。
[同時実行]	システムがエージェントの更新を同時に試行する仮想マシンの数に制限を設定します。 この設定は、[障害のしきい値] 設定と並行して機能します。[同時実行] 設定は [障害のしきい値] 設定以下にすることが理想的です。
[障害のしきい値]	更新プロセスが停止となるまでに許容される、エージェントの更新が失敗する仮想マシンの数。このしきい値の設定により、大量の障害が発生するのを防ぎます。 仮想マシン エージェントの更新に失敗したことが原因で更新プロセスが停止した場合、設定した [障害のしきい値] よりも多くの障害が発生した仮想マシンが表示されることがあります。障害の数を [障害のしきい値] 設定で指定した数よりも少なくする必要がある場合は、[同時実行] の値を 1 に設定します。これは、一度に 1 台の仮想マシンを更新することになるため、エージェントの更新プロセスに長い時間がかかることを意味します。最適な結果を得るには、[同時実行] および [障害のしきい値] を適切に設定することをお勧めします。
[コマンドライン引数]	[コマンドライン引数] テキスト ボックスに、この更新に関連する可能性のあるコマンドライン オプションを追加します。

次のステップ

エージェントの更新プロセスはバックグラウンドで実行され、ステータスが [アクティビティ ログ] ページに表示されます。[アクティビティ ログ] ページに移動して進行状況を確認します。アクティビティ ログの詳細については、「[アクティビティ ログ] ページからの管理者とエンド ユーザーのアクティビティの監視」を参照してください。

フローティング デスクトップおよびマルチセッション デスクトップでの Horizon Agent の更新

フローティング デスクトップとマルチセッション デスクトップの Horizon Agent を更新するには、既存のイメージを更新するか、最新の Horizon Agent バージョンを使用して新しいイメージを作成し、デスクトップ プールに割り当てます。

フローティング デスクトップとマルチセッション デスクトップは、必要に応じて削除および再作成されるため、ユーザー データは OS ディスクに保持されません。プール内の各デスクトップの Horizon Agent を更新するには、イメージを最新バージョンで更新し、プールに割り当てます。イメージ マーカーを使用して更新されたイメージをプールに適用すると、サービスはこれらのデスクトップを再作成します。

既存のイメージを使用して Horizon Agent を更新するには、新しいイメージ バージョンを公開して、最新の Horizon Agent を使用してイメージ バージョンを作成します。

手順

1. 新しいイメージ バージョンのクローンを作成します。イメージ バージョンのクローン作成を参照してください。
2. 必要に応じて、ソフトウェアとアプリケーションを更新します。
3. 最新の Horizon Agent バージョンでイメージを公開します。エージェントのインストールと必要な機能を選択します。イメージの公開を参照してください。

   公開されたイメージ バージョンには、最新の Horizon Agent ソフトウェアが含まれます。
4. イメージ バージョンとマーカーをイメージの公開中に検証しない場合は、テスト プールで検証します。
5. 既存のプールに関連付けられているマーカーを選択し、このイメージ バージョンでマーカーを使用してすべてのプールを更新する場合は、このイメージ バージョンに更新します。プールを個別に更新する場合は、デスクトップ プールに割り当てるためのマーカーがこの公開されたイメージ バージョンに存在することを確認します。イメージ バージョンの編集を参照してください。

   マーカーが更新されると、サービスはこのデスクトップを構成された設定で更新し、更新されたすべてのデスクトップのエージェントが最新になります。

専用デスクトップ仮想マシンへの Horizon Agent ソフトウェアの再インストール

再インストール機能によって、仮想マシンから既存のエージェントをアンインストールし、最新のエージェント ソフトウェアを再インストールできます。再インストール機能を使用すると、強制インストールによるエージェントのアップデート失敗のリカバリ メカニズムが提供されます。また、次のユースケースで説明するように、エージェント ソフトウェアをアンインストールして再インストールする必要がある特別な状況で発生します。

次の使用事例は、エージェントを再インストールするタイミングを示しています。

- 専用デスクトップ仮想マシンでの Horizon Agent ソフトウェアの更新で説明されているように、仮想マシン上のエージェントの更新が一貫して失敗する場合。
- オペレーティング システムの更新またはデバイス ドライバの問題が原因でアンインストールおよび再インストールするエージェントがある場合。

注： 次世代環境に、まだ完了していない第 1 世代の移行がある場合、システムではこのエージェントの再インストール手順を実行できません。[エージェント] - [再インストール] の順にクリックすると、移行の完了に関するメッセージが表示されます。

手順

1 Horizon Universal Console で、[プール グループ] ページに移動します。

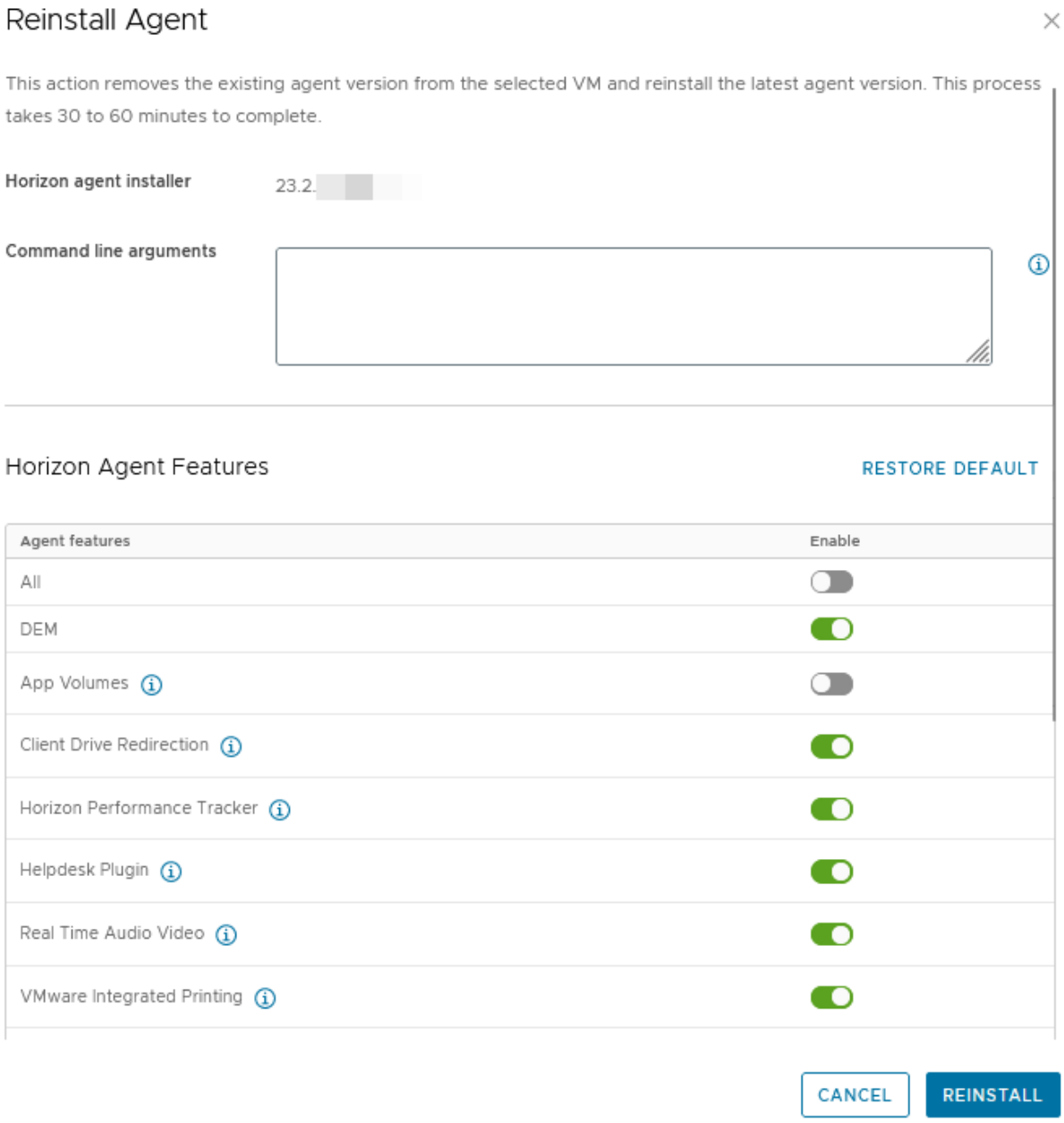
2 [仮想マシン] を選択します。

3 リストから 1 台以上の仮想マシンを選択します。

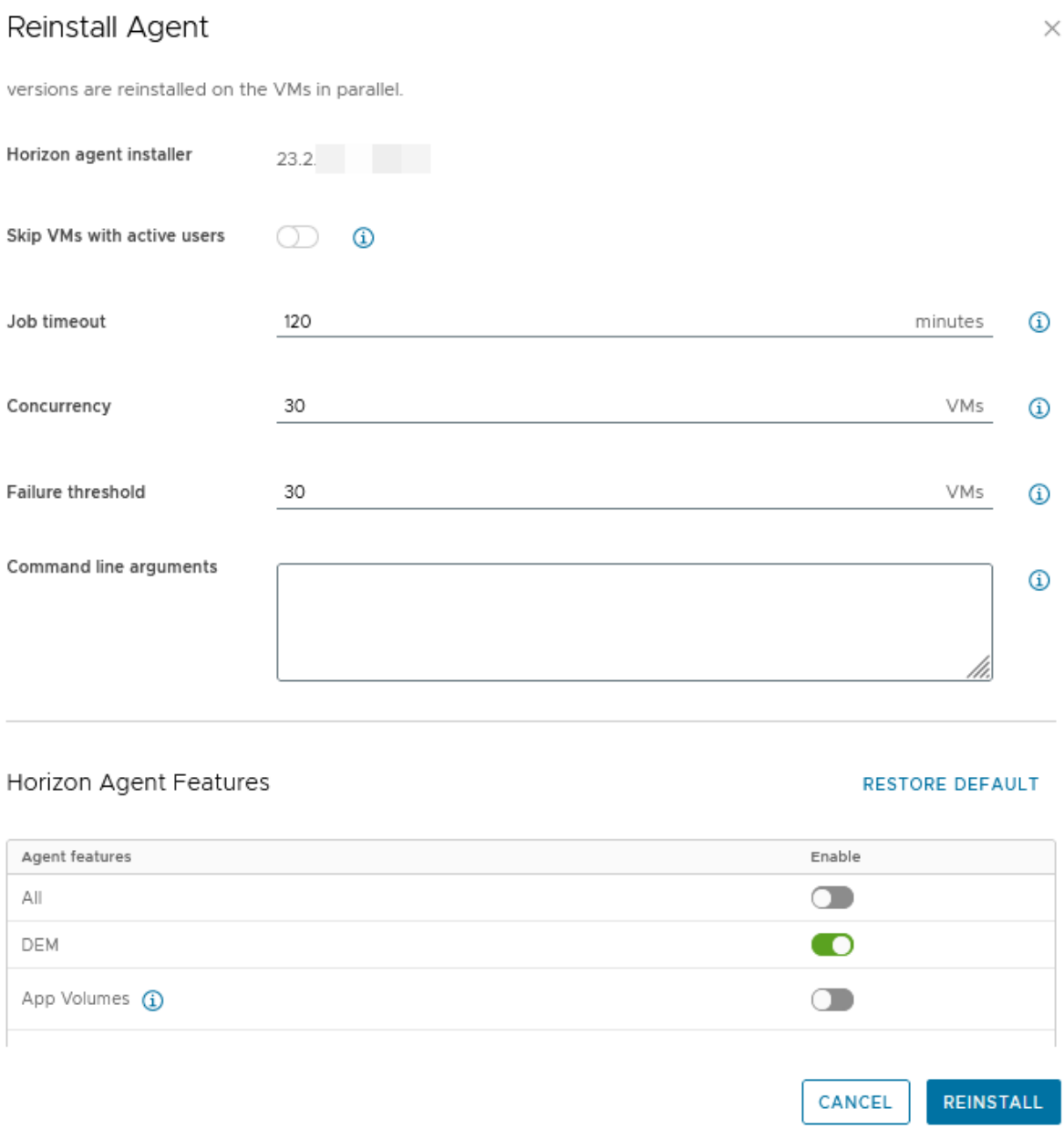
4 [エージェント] - [再インストール] の順に選択します。

エージェントの再インストール ページが開きます。ページに情報の入力を求めるプロンプトが表示されます。プロンプトは、1 台の仮想マシンを選択したか、複数の仮想マシンを選択したかによって異なります。

単一の仮想マシンが選択された [エージェントの再インストール] ページ



複数の仮想マシンが選択された [エージェントの再インストール] ページ



5 [エージェントの再インストール] フォームに入力し、[再インストール] をクリックします。

該当する次のプロンプトに適切な応答を入力します。[コマンドライン引数] は、単一のエージェントを選択したか、複数のエージェントを選択したかに関係なく適用されます。他のすべてのオプションは、複数のエージェントを選択した場合にのみ適用されます。

オプション	説明
[アクティブなユーザーを含む仮想マシンのスキップ]	アクティブなセッションまたは切断されたセッションの再インストール Horizon Agent をスキップする場合に選択します。このオプションが選択されていない場合、再インストールの開始時に仮想マシンにログインしたユーザーは 5 分間の警告が表示されてから強制的にログオフされます。
[ジョブのタイムアウト]	システムがエージェントの再インストールを自動的に試行し続ける期間を設定します。特定の期間にのみ再インストールを実行する場合は、複数のテンプレートと仮想マシンを選択している場合でも、短い期間を設定できます。仮想マシンの状態、およびその他の待機時間と実行中の再試行に応じて、仮想マシンの 1 つのバッチに 20 ～ 60 分かかることがあります。 たとえば、600 台を超える仮想マシンがあり、30 台の仮想マシンを同時に再インストールする場合、期間は次のように計算できます。 ■ バッチ数：600/30 = 20 バッチ ■ ジョブのタイムアウト：20*60 = 1200 分 ジョブのタイムアウトを 1200 分に設定します。これは、通常の再インストールの実行に必要な期間よりもはるかに長くなります。 **注：** 再インストール中にエラーが発生した仮想マシンの再インストールは再試行されません。
[同時実行]	システムがエージェントの再インストールを同時に試行する仮想マシンの数に制限を設定します。 この設定は、[障害のしきい値] 設定と並行して機能します。[同時実行] 設定は [障害のしきい値] 設定以下にすることが理想的です。
[障害のしきい値]	再インストール プロセスが停止となるまでに許容される、エージェントの再インストールが失敗する仮想マシンの数。このしきい値の設定により、大量の障害が発生するのを防ぎます。 仮想マシン エージェントの再インストールに失敗したことが原因で再インストール プロセスが停止した場合、設定した [障害のしきい値] よりも多くの障害が発生した仮想マシンが表示されることがあります。障害の数を [障害のしきい値] 設定で指定した数よりも少なくする必要がある場合は、[同時実行] の値を [1] に設定します。これは、一度に 1 台の仮想マシンを再インストールすることになるため、エージェントの再インストール プロセスに長い時間がかかることを意味します。最適な結果を得るには、[同時実行] および [障害のしきい値] を適切に設定することをお勧めします。
[コマンドライン引数]	[コマンドライン引数] テキスト ボックスに、この再インストールに関連する可能性のあるコマンドライン オプションを追加します。

次のステップ

エージェントの再インストール プロセスはバックグラウンドで実行されます。プロセスの進行状況は、[アクティビティ ログ] ページで確認できます。[アクティビティ ログ] ページからの管理者とエンド ユーザーのアクティビティの監視を参照してください。

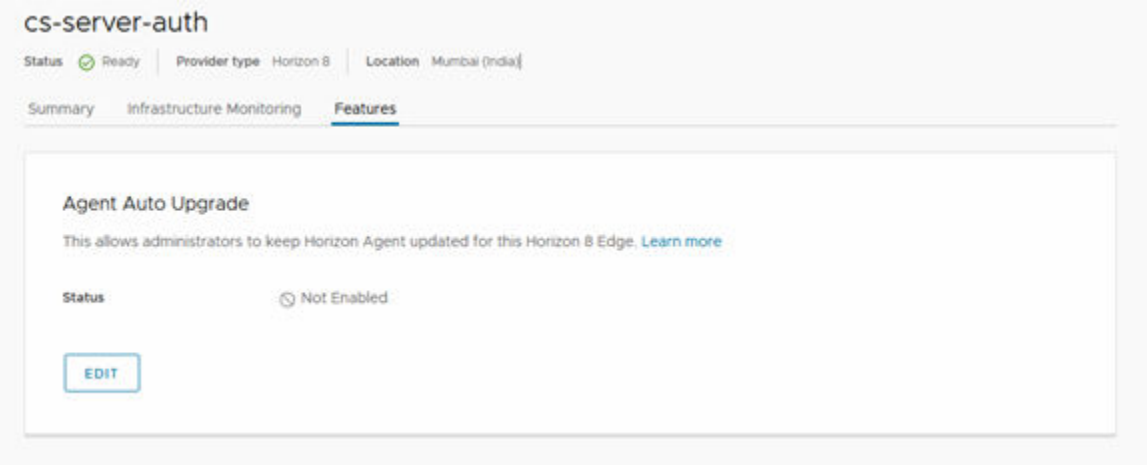
。

Horizon 8 Edge のエージェントの自動アップグレード機能の管理

Horizon Cloud Service - next-gen では、Horizon Universal または Horizon Plus のライセンスがあり、Horizon 8 環境に Horizon Edge を展開する場合は、Horizon Universal Console を使用して、指定した Horizon 8 Edge の Horizon Agent インスタンスを継続して更新できます。

Horizon Universal または Horizon Plus ライセンスがある場合は、Horizon Universal Console の [機能] タブにアクセスできます。これにより、エージェントの自動アップグレード機能を有効にできます。Horizon 8 のエージェントの自動アップグレード機能は、この手順中に Horizon Cloud Service - next-gen で有効にするエージェントの自動アップグレード機能の構成に依存します。

注： 次の手順を実行すると、機能が有効になります。その後、Horizon Connection Server からエージェントのアップグレードを管理できます。



前提条件

次の要件が満たされていることを確認します。

- 次のいずれかのライセンスを取得していること：
  - Horizon Universal
  - Horizon Plus
- Horizon Cloud Service - next-gen 用の Horizon 8 Edge をデプロイすること。
- Horizon Connection Server バージョンが 2312 以降であること。

手順

1 [リソース] - [キャパシティ] の順に選択します。

2 エージェントの自動アップグレード機能を有効にする Horizon 8 Edge の名前をクリックします。

3 [機能] タブをクリックします。

4 機能のステータスに [無効] と表示されており、有効にする場合は、[編集] をクリックします。

5 [ステータス] トグルをクリックして、機能を有効にします。

6 [保存] をクリックします。

結果

これで、Horizon 8 Edge でエージェントの自動アップグレード機能が有効になりました。

次の手順

「Horizon Agent の自動アップグレード」など、Horizon 8 トピックの適切なバージョンに記載されているように、Horizon Console を使用して Horizon Agent の自動アップグレードを管理します。

Horizon Cloud Service - next-gen での Horizon Edge のメンテナンスと更新

このページでは、デプロイされた Horizon Edge を構成するコンポーネントのソフトウェア コンポーネント メンテナンスについて知っておくべき重要な事項について説明します。

Unified Access Gateway (UAG)、Edge Gateway などの Horizon インフラストラクチャ製品などの更新が予定されている場合、E メール通知が届きます。

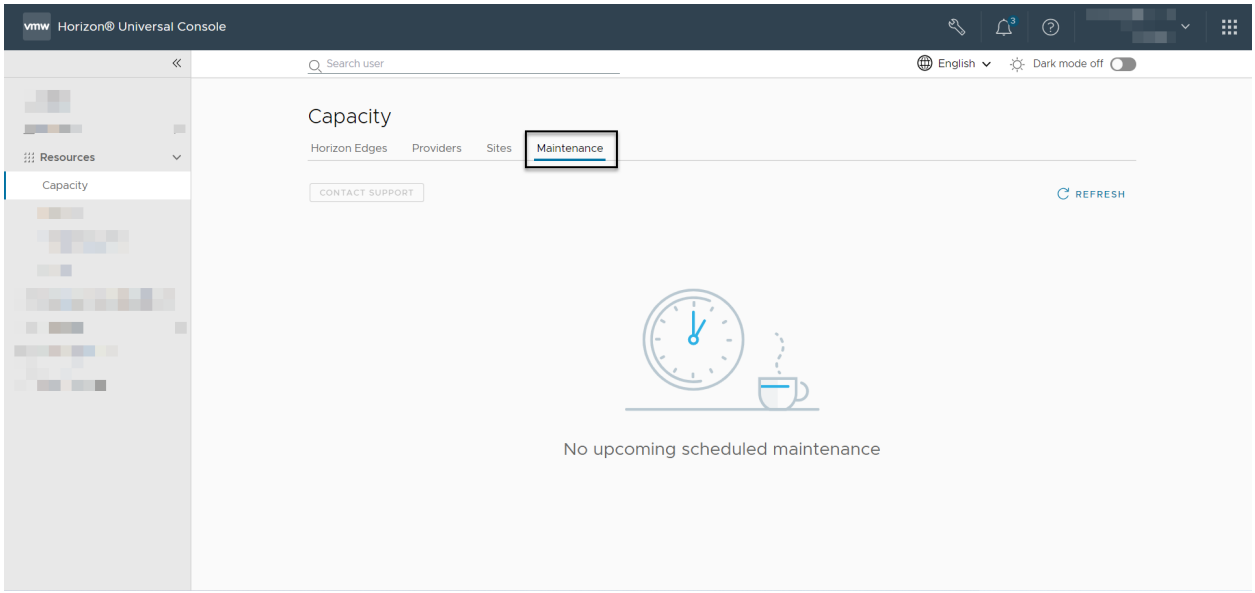
また、更新プロセスの各フェーズが開始、完了、再スケジュール、またはキャンセルされたときにも、E メール通知を受信します。

注： 製品の更新にはダウンタイムは必要なく、環境やワークロードに影響を与えることはありません。製品の更新を遅らせると、Horizon Cloud Service でサポートされていないソフトウェア バージョンが実行される可能性があるため、お勧めしません。

製品の更新プロセスが完了すると、更新された内容のサマリが E メール通知で届きます。

これらの重要な E メール通知を受信できるようにするには、E メールの許可リストにメール アドレス donotreply@vmware.com を追加します。

Unified Access Gateway、Edge Gateway、およびクラスタは、ローリング ベースで更新されます。Horizon Universal Console で製品の更新およびメンテナンスに関連する情報を表示するには、[リソース] - [キャパシティ] - [メンテナンス] の順に選択します。



スケジュール設定されたメンテナンスのタイミングが適さない場合は、[メンテナンス] ページの [サポートへの問い合わせ] ボタンをクリックしてサポートに連絡し、スケジュールを再設定します。

Horizon Cloud Service - next-gen ユーザーのリモート エクスペリエンスの構成

7

次の情報を使用して、Horizon Cloud Service - next-gen エンド ユーザーのリモート エクスペリエンスを構成できます。

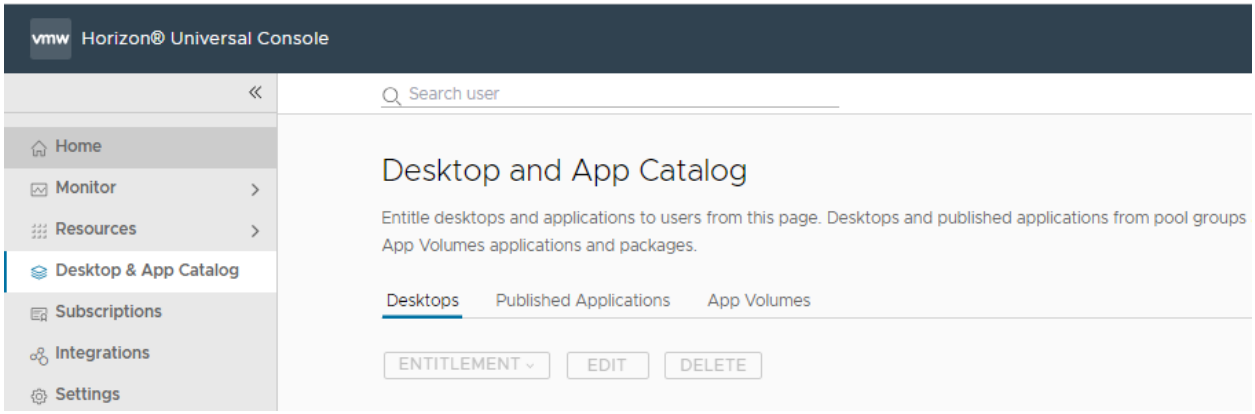
次のトピックを参照してください。

- エンド ユーザーへのデスクトップおよびアプリケーションの資格の付与
- 専用単一セッション プール グループ内の仮想マシンへの Horizon Cloud Service - next-gen ユーザーの割り当て
- Horizon Client によるデスクトップの起動
- Web クライアントの Horizon HTML Access を使用したデスクトップの起動
- Horizon Client を使用したアプリケーションの起動
- Web クライアントの Horizon HTML Access を使用したアプリケーションの起動
- グローバル Horizon Client 設定の構成
- Horizon クラウド資格オンランプの有効化による Horizon 8 および Horizon Cloud on Azure のデスクトップへのアクセス

エンド ユーザーへのデスクトップおよびアプリケーションの資格の付与

Horizon Cloud Service - next-gen の場合、次の手順に従い、Horizon Universal Console とコンソールの [デスクトップおよびアプリケーション カタログ] ページを使用して、デスクトップおよび公開アプリケーションの資格をエンド ユーザーに付与します。

次のスクリーンショットは、コンソールの [デスクトップおよびアプリケーション カタログ] ページを示しています。



以下の手順は、デスクトップと、複数セッション プール グループのアプリケーションである公開アプリケーションの使用資格を付与する方法を示しています。

環境内で App Volumes を使用する方法については、「App Volumes の使用」から始めてください。

前提条件

コンソールの [デスクトップおよびアプリケーション カタログ] ページを使用してデスクトップまたは公開アプリケーションの使用資格をエンド ユーザーに付与するには、それらのデスクトップと公開アプリケーションを環境に提供するプール グループが必要です。プール グループの作成からリンクされているページを参照してください。

手順

1 コンソールの左側のナビゲーションにある [デスクトップとアプリケーション カタログ] エントリをクリックして、[デスクトップおよびアプリケーション カタログ] ページを表示します。

2 デスクトップの資格を使用するには、[デスクトップ] をクリックします。

環境のプール グループのデスクトップが [デスクトップ] タブに一覧表示されます。

リストされたデスクトップを選択し、[資格] リストをクリックして、エンド ユーザーに対してデスクトップの [資格を付与] または [資格を解除] します。[資格を付与] をクリックすると、[デスクトップの資格を付与] ページが表示されます。これは次の手順で説明します。

この [デスクトップ] タブから、選択した内容を [編集] または [削除] することもできます。

3 [デスクトップの資格を付与] ページで、選択したデスクトップの資格を付与する際は、[ユーザー タイプ] を使用して [ユーザー] または [ユーザー グループ] を指定し、[ユーザー/ユーザー グループの検索] を使用して、[保存] をクリックします。

4 公開アプリケーションの資格を操作するには、[デスクトップおよびアプリケーション カタログ] ページで [公開アプリケーション] タブをクリックします。

環境のプール グループの公開アプリケーションが [公開アプリケーション] タブに一覧表示されます。

リストされたアプリケーションを選択し、[資格] リストをクリックして、エンド ユーザーに対してそのアプリケーションの [資格を付与] または [資格を解除] します。[資格を付与] をクリックすると、[公開アプリケーションの資格を付与] ページが表示されます。これは次の手順で説明します。

このタブから、公開アプリケーションを [編集] または [削除] することもできます。

5 [公開アプリケーションの資格を付与] ページで、選択したアプリケーションの資格を付与する際は、[ユーザー タイプ] を使用して [ユーザー] または [ユーザー グループ] を指定し、[ユーザー/ユーザー グループの検索] を使用して、[保存] をクリックします。

次のステップ

デスクトップまたは公開アプリケーションの使用資格がエンド ユーザーに付与されたら、ユーザーはそれらのデスクトップまたはアプリケーションを起動できます。

デスクトップの起動

- Web クライアントの Horizon HTML Access を使用したデスクトップの起動
- Horizon Client によるデスクトップの起動

公開アプリケーションの起動

- Web クライアントの Horizon HTML Access を使用したアプリケーションの起動
- Horizon Client を使用したアプリケーションの起動

専用単一セッション プール グループ内の仮想マシンへの Horizon Cloud Service - next-gen ユーザーの割り当て

[プール グループ] ページでは、ユーザーを専用の単一セッション プール グループに割り当てることができます。

注： 1 台のデスクトップに複数のユーザーを割り当てることができますが、一度に 1 台の仮想マシンでセッションを実行できるのは 1 人のユーザーのみです。タイムアウト処理設定を適切に構成して、仮想マシンの可用性を確保します。タイムアウト処理設定の構成の詳細については、「単一セッション プール グループの作成」を参照してください。

手順

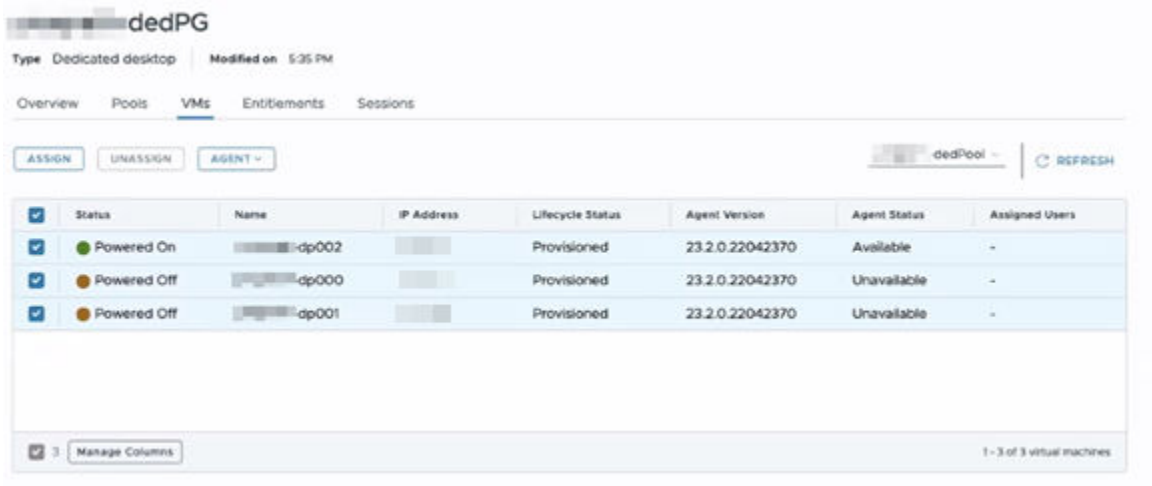
1 サイド ナビゲーションで、[リソース] - [プール グループ] を選択します。

2 専用デスクトップ プール グループの名前をクリックします。

3 [仮想マシン] タブをクリックします。

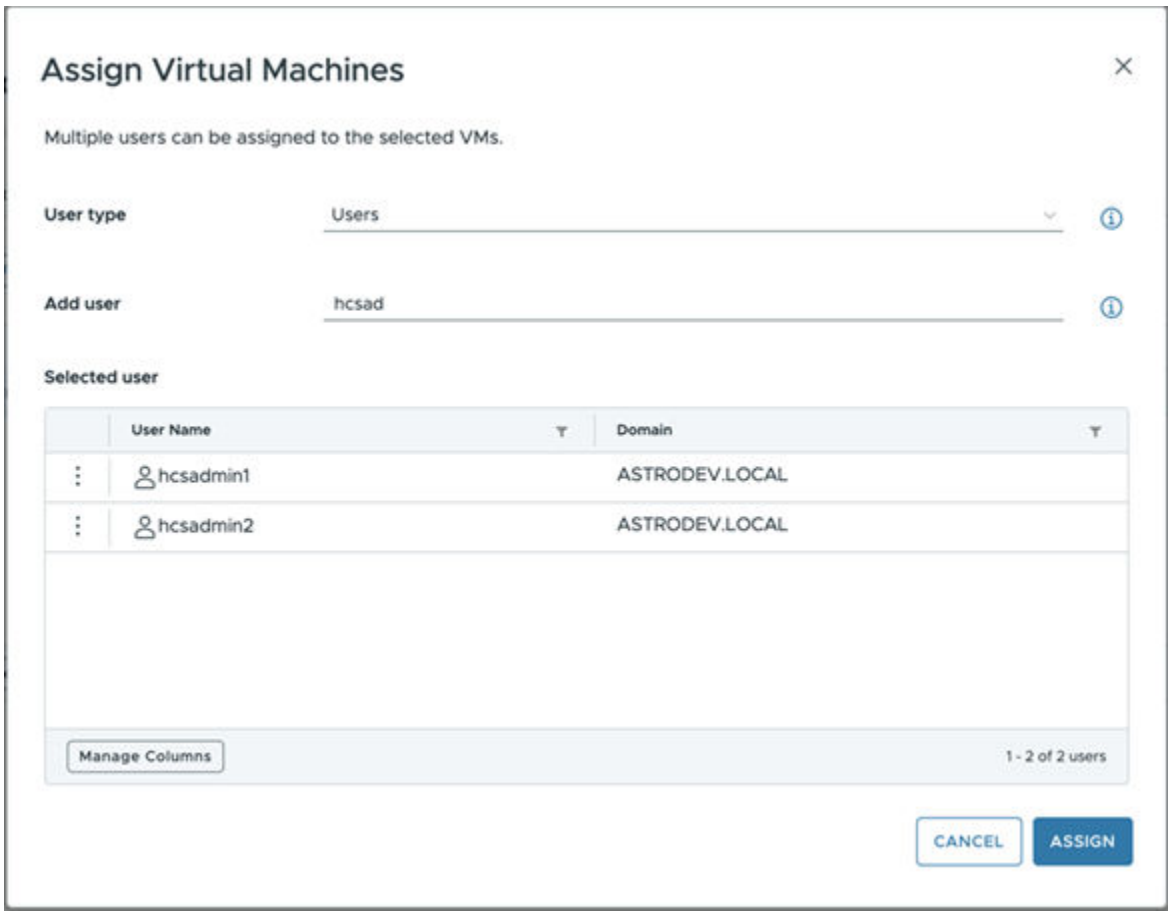
4 表の上で、[更新] リンクの左側にあるドロップダウン リストからプールを選択します。

5 ユーザーを割り当てる仮想マシンを選択して、[割り当て] をクリックします。



6 [ユーザーを追加] テキスト ボックスで、ユーザー名を入力し、表示されるユーザー名からユーザーの名前を選択します。

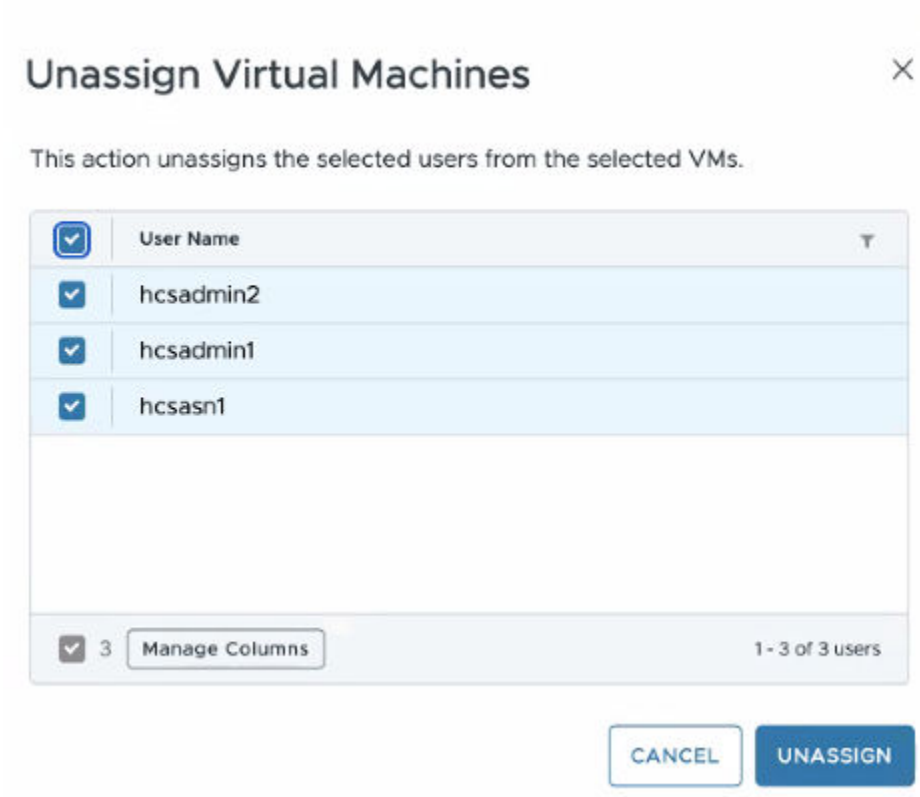
この手順を複数回繰り返して、他のユーザーを追加できます。



7 [割り当て] をクリックします。

8 ユーザーの割り当てを解除するには、1 台以上の仮想マシンを選択して、[割り当て解除] をクリックし、特定のユーザーを選択して、[割り当て解除] を再度クリックします。

複数の仮想マシンを選択すると、選択した仮想マシンに割り当てられているすべてのユーザーの統合リストが画面に表示されます。リストには、どのユーザーがどの仮想マシンに関連付けられているかは指定されていません。選択したすべてのユーザーは、割り当て解除が 1 台の仮想マシンから行われるか複数の仮想マシンから行われるかにかかわらず、すべての仮想マシンから割り当て解除されます。



Horizon Client によるデスクトップの起動

このドキュメント ページでは、Horizon Client を使用して、Horizon Cloud Service - next-gen 環境で提供される仮想デスクトップを起動する手順について説明します。

これらの手順には、ネイティブな Horizon Client をローカル クライアント システムにまだインストールしていない場合のインストール方法も含まれています。

前提条件

エンド ユーザーが割り当てられたデスクトップを起動する前に、環境にデスクトップを提供するため、少なくとも次のいずれかがあることを確認してください。

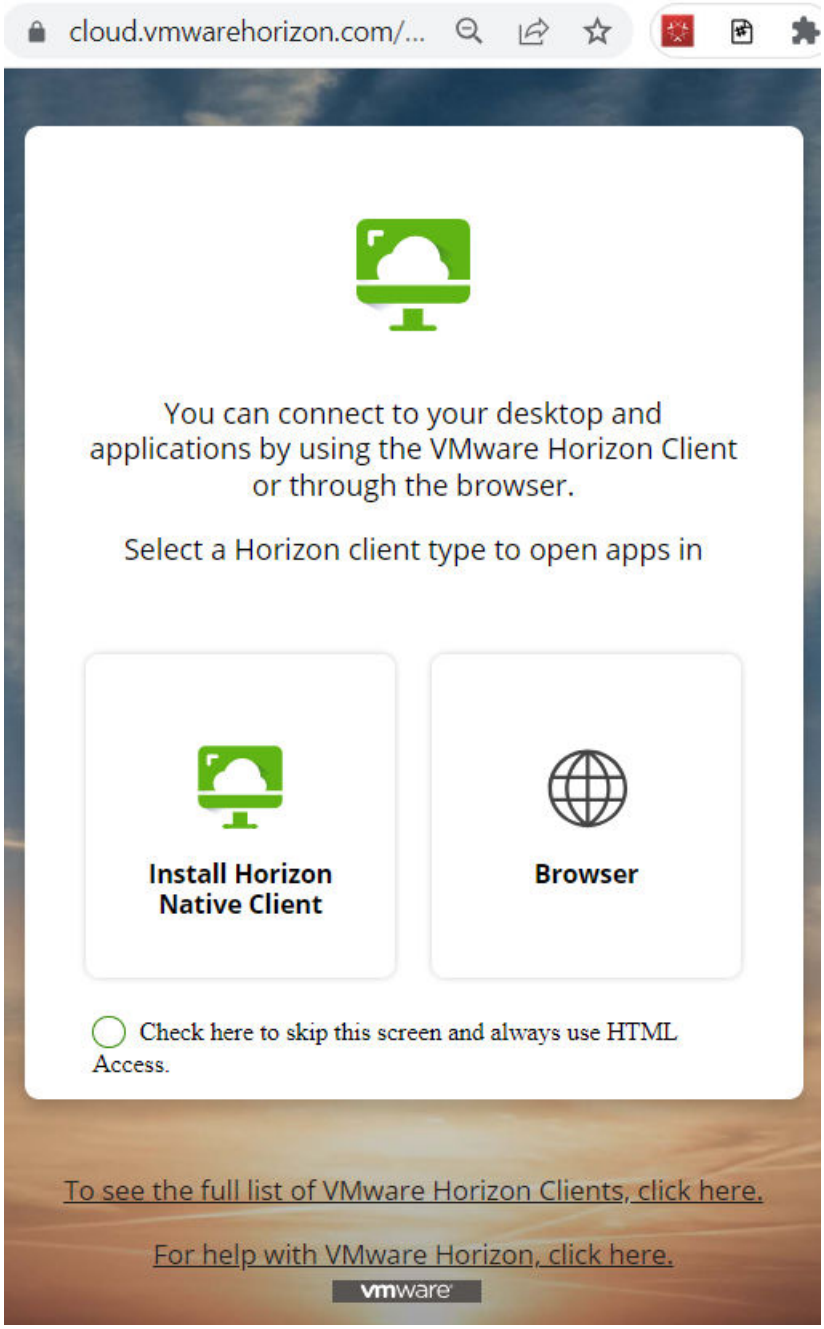
- 単一セッション プールの VDI イメージが正常に公開されました。
- 複数セッション プールのイメージが正常に公開されました。

また、エンド ユーザーが Horizon Cloud Service - next-gen 環境でサポートされているバージョンの Horizon Client を使用していることを確認してください。「Microsoft Azure Edge の要件に関するチェックリスト」ページにあるクライアントに関するセクションを参照してください。

手順

1 割り当てられたデスクトップにアクセスするには、https://cloud.vmwarehorizon.com/で Horizon ポータルを起動します。

次のスクリーンショットは、ブラウザでその URL に移動したときに表示されるポータルを示しています。



2 ネイティブ システムに Horizon Client がまだインストールされていない場合は、[Horizon ネイティブ クライアントのインストール] オプションを選択すると、Customer Connect サイトに自動的に移り、そこから使用中のオペレーティング システム用のネイティブ クライアントをダウンロードできます。

[Horizon ネイティブ クライアントのインストール] をクリックすると、VMware Horizon Client をダウンロードするための Customer Connect ページがブラウザに表示されます。画面上のガイダンスに沿って、使用中のシステムに対応するネイティブ クライアントのインストーラをダウンロードし、ネイティブ クライアントをインストールします。

3 インストールしたら、Horizon Client を起動します。

クライアントには、この Horizon Client で現在構成されているすべての Horizon サイトが表示されます。

4 表示された一連の構成済みサイトで、cloud.vmwarehorizon.com というラベルの付いたサイトを見つけてダブルクリックし、サイトに接続します。

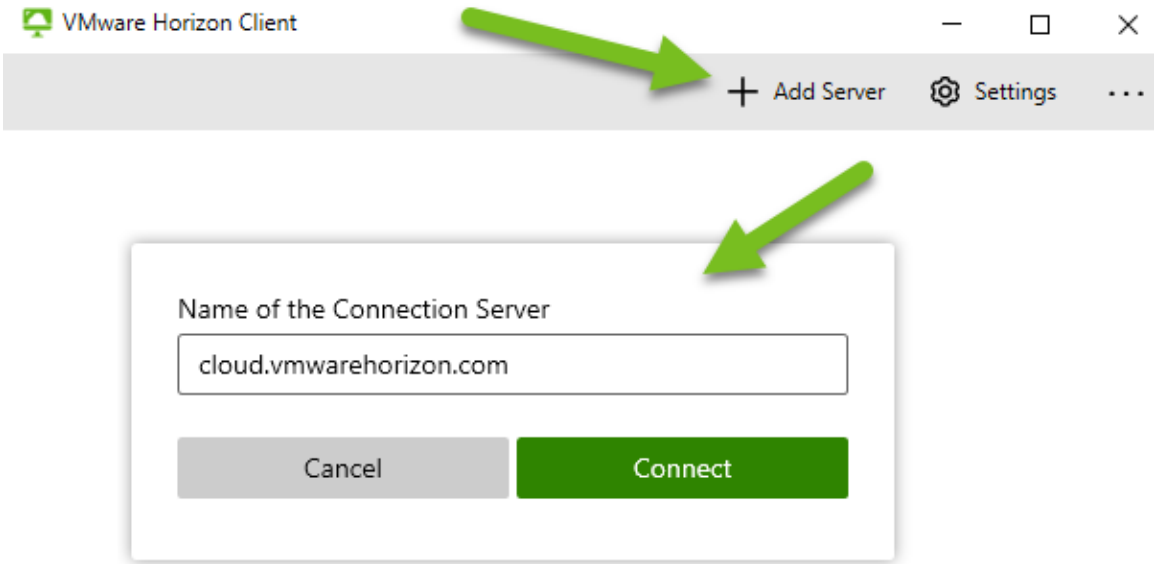
注： これがクライアントの初回インストールである場合、または Horizon Cloud Service - next-gen 環境からデスクトップまたはアプリケーションを起動するのが初めての場合、クライアントには cloud.vmwarehorizon.com 用に構成されたサイトがありません。

その場合は、クライアントの **サーバの追加** ボタンを使用して、[cloud.vmwarehorizon.com] という名前のサイトを追加する必要があります。

a cloud.vmwarehorizon.com というラベルの付いたアイコンが表示されない場合は、[サーバの追加] をクリックして追加します。

クライアントには、cloud.vmwarehorizon.com を入力するためのフィールドが表示されます。

次のスクリーンショットは、Horizon Client for Windows v2303 を使用した一連の手順を示しています。別のネイティブ クライアントまたはバージョンを使用している場合、ユーザー インターフェイスはこのスクリーンショットと異なる場合があります。基本的には、サイト名（サーバ名）を追加し、接続して、クライアントでそのサイトのアイコンを確認するという手順です。

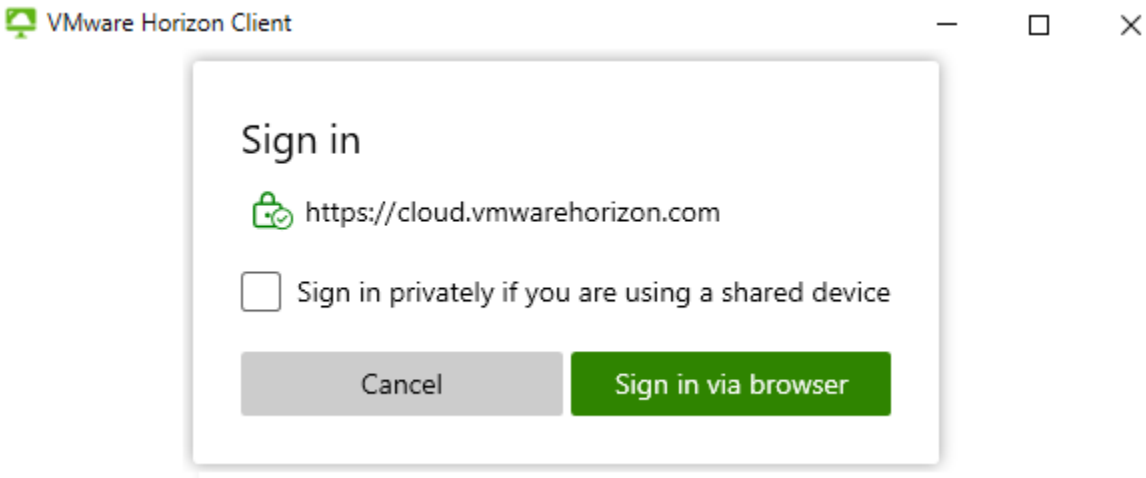


次に [接続] をクリックして、Horizon Client へのサイトの追加を完了します。

5 クライアントに cloud.vmwarehorizon.com のアイコンが表示されたら、そのアイコンをダブルクリックしてサイトに接続します。

表示されるユーザー インターフェイスは、使用しているネイティブ クライアントによって異なります。たとえば、Horizon Client for Windows には [ログイン] ダイアログが表示されますが、Horizon Client for Chrome の場合は [ログイン] ダイアログが表示されません。

次のスクリーンショットは、Horizon Client for Windows v2303 を使用した場合のこの手順を具体的に示しています。



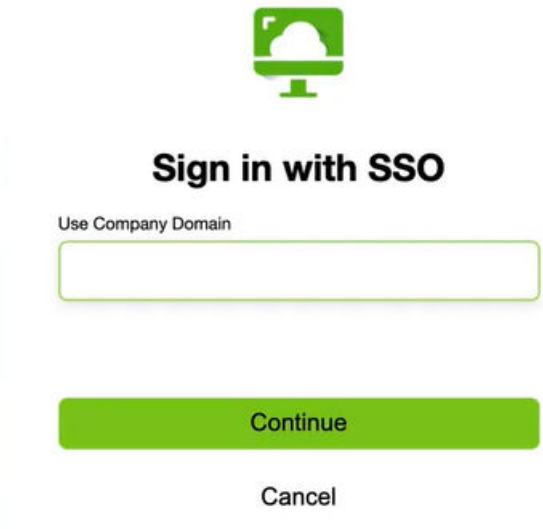
6 クライアントに表示される画面のプロンプトに沿って、ログインに進みます。

使用中のクライアントに [共有デバイスを使用している場合は、プライベートでログインする] オプションがある場合は、そのオプションを使用して、クライアントがデバイス上の情報をキャッシュしないようにすることができます。

注： Horizon Client for Chrome は常にプライベートでログインするため、このクライアントには [共有デバイスを使用している場合は、プライベートでログインする] オプションがありません。Horizon Client for Chrome のサーバ アイコンをクリックすると、クライアントによってブラウザに [SSO でログイン] ユーザー インターフェイスが表示されます。

画面上のプロンプトに沿ってログインすると、ブラウザに [SSO でログイン] ユーザー インターフェイスが表示されます。

次のスクリーンショットは、[SSO でログイン] というユーザー インターフェイスを示しています。



7 [SSO でログイン] で、この Horizon Cloud Service - next-gen 環境に関連付けられている会社のドメインの名前を入力し、[続行] をクリックします。

Horizon Universal Console では、管理者は ID プロバイダ構成で設定されている名前を確認できます。Horizon Cloud Service - next-gen 環境での ID とアクセス管理のページを参照してください。

[続行] をクリックしたら、画面のプロンプトに従います。ID プロバイダのログイン ユーザー インターフェイスが表示されます。その ID プロバイダに割り当てられた認証情報を使用してログインします。

ID プロバイダのログインが完了すると、Horizon 資格画面がクライアントに表示され、割り当てられたデスクトップとアプリケーションが一覧表示されます。

8 デスクトップ アイコンをクリックして、デスクトップを起動します。

Web クライアントの Horizon HTML Access を使用したデスクトップの起動

このドキュメント ページでは、Web クライアントである Horizon HTML Access を使用して、Horizon Cloud Service - next-gen 環境で提供されるデスクトップを起動する手順について説明します。

前提条件

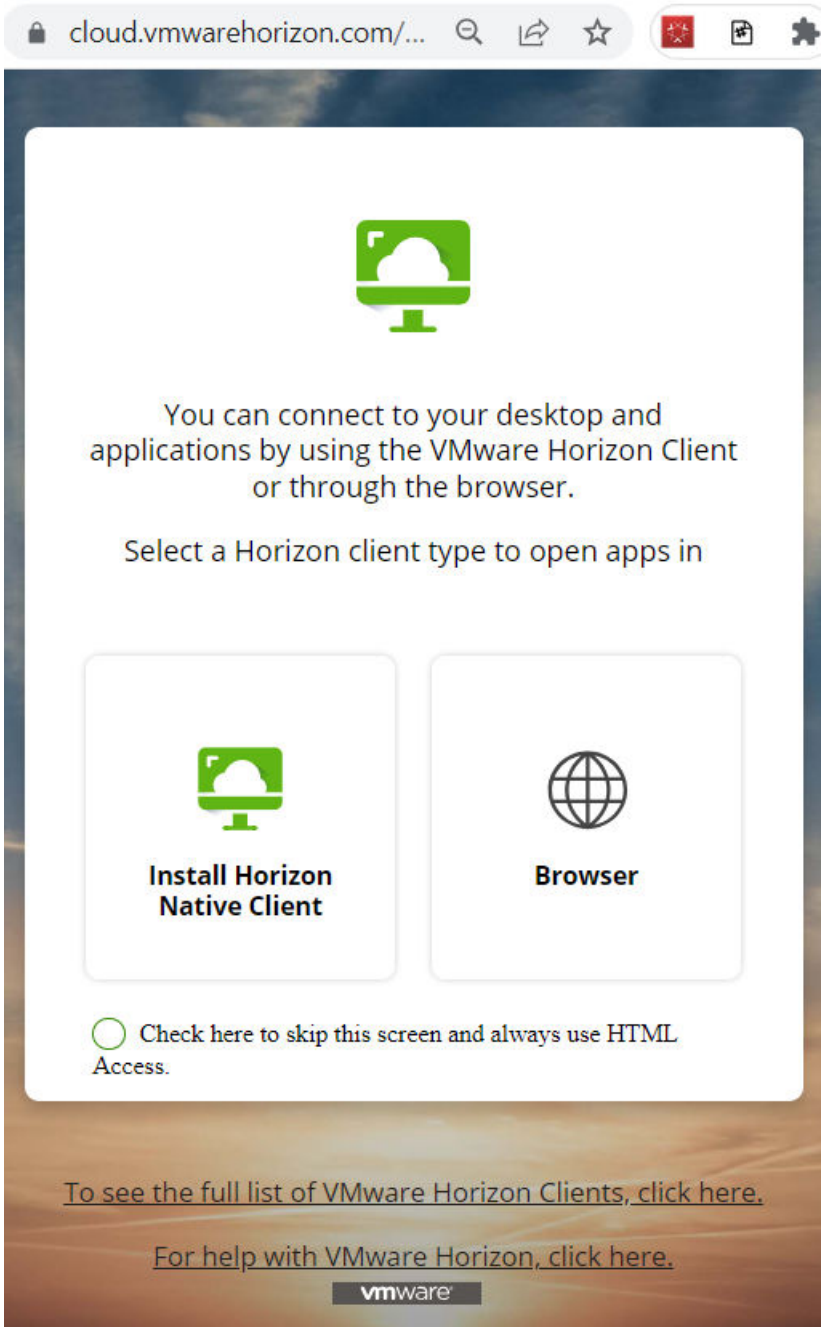
エンド ユーザーが割り当てられたデスクトップを起動する前に、環境にデスクトップを提供するため、少なくとも次のいずれかがあることを確認してください。

- 単一セッション プールの VDI イメージが正常に公開されました。
- 複数セッション プールのイメージが正常に公開されました。

手順

1 割り当てられたデスクトップにアクセスするには、https://cloud.vmwarehorizon.com/で Horizon ポータルを起動します。

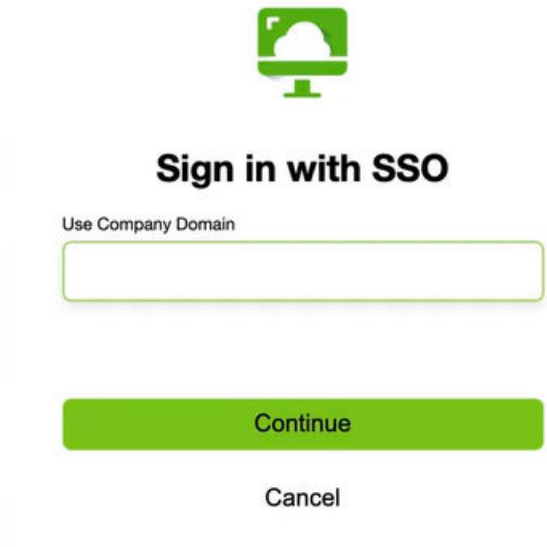
次のスクリーンショットは、ブラウザでその URL に移動したときに表示されるポータルを示しています。



2 [ブラウザ] をクリックし、Web クライアントを使用してデスクトップに接続します。

[ブラウザ] をクリックすると、ブラウザに [SSO でログイン] というユーザー インターフェイスが表示されます。

次のスクリーンショットは、[SSO でログイン] というユーザー インターフェイスを示しています。



3 [SSO でログイン] で、この Horizon Cloud Service - next-gen 環境に関連付けられている会社のドメインの名前を入力し、[続行] をクリックします。

Horizon Universal Console では、管理者は ID プロバイダ構成で設定されている名前を確認できます。Horizon Cloud Service - next-gen 環境での ID とアクセス管理のページを参照してください。

[続行] をクリックしたら、画面のプロンプトに従います。ID プロバイダのログイン ユーザー インターフェイスが表示されます。その ID プロバイダに割り当てられた認証情報を使用してログインします。

ID プロバイダのログインが完了すると、Horizon 資格画面が表示され、割り当てられたデスクトップとアプリケーションが一覧表示されます。

4 デスクトップを起動するには、表示されているアイコンをクリックします。

Horizon Client を使用したアプリケーションの起動

このドキュメント ページでは、Horizon Client を使用して、Horizon Cloud Service - next-gen 環境で提供されるアプリケーションを起動する手順について説明します。

これらの手順には、ネイティブな Horizon Client をローカル クライアント システムにまだインストールしていない場合のインストール方法も含まれています。

前提条件

エンド ユーザーが割り当てられたアプリケーションを起動する前に、Horizon Universal Console を使用して、それらのユーザーに公開アプリケーションの使用資格が付与されていることを確認します。

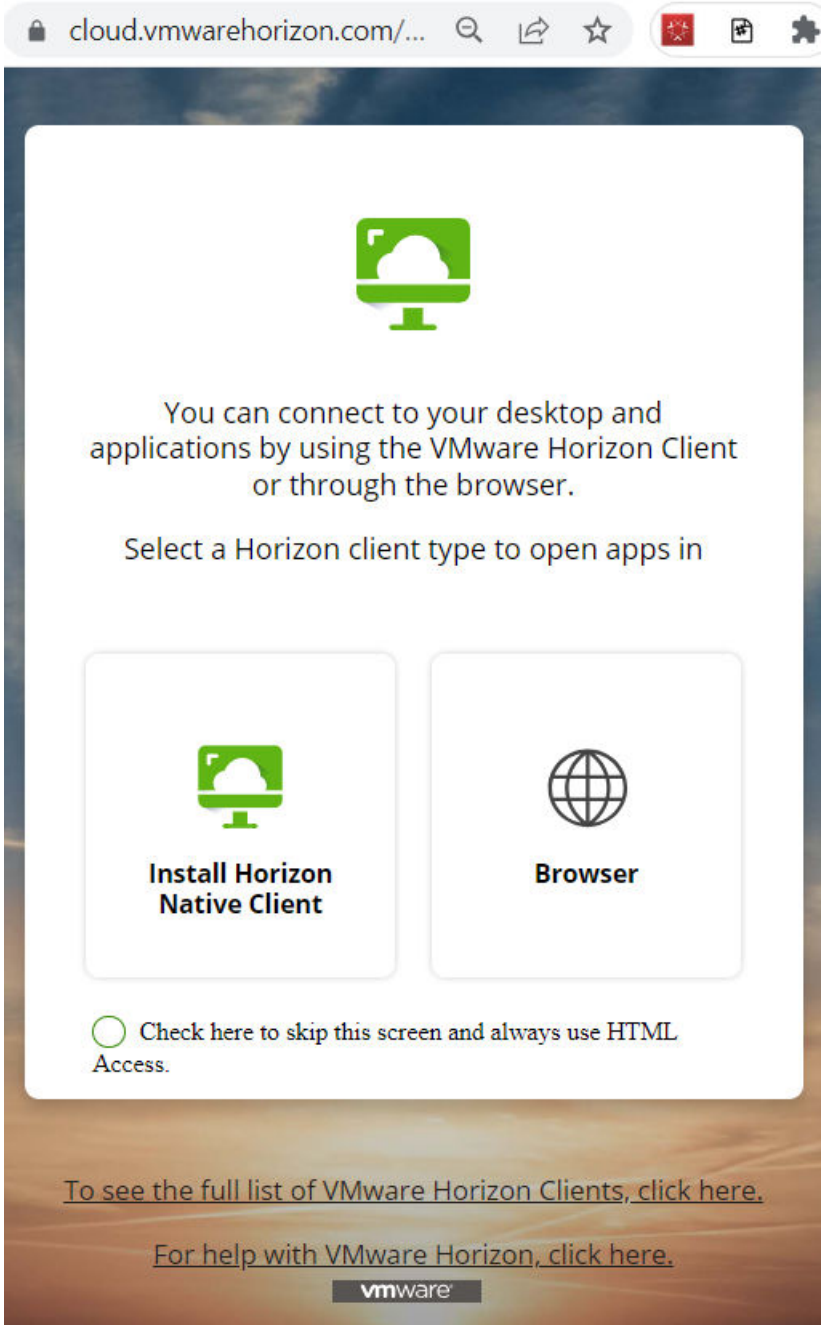
- マルチセッション プール グループから公開アプリケーションの使用資格を付与する方法については、エンド ユーザーへのデスクトップおよびアプリケーションの資格の付与を参照してください。

また、エンド ユーザーが Horizon Cloud Service - next-gen 環境でサポートされているバージョンの Horizon Client を使用していることを確認してください。「Microsoft Azure Edge の要件に関するチェックリスト」ページにあるクライアントに関するセクションを参照してください。

手順

1 割り当てられたアプリケーションにアクセスするには、Horizon ポータル (https://cloud.vmwarehorizon.com/) を起動します。

次のスクリーンショットは、ブラウザでその URL に移動したときに表示されるポータルを示しています。



2 ネイティブ システムに Horizon Client がまだインストールされていない場合は、[Horizon ネイティブ クライアントのインストール] オプションを選択すると、Customer Connect サイトに自動的に移り、そこから使用中のオペレーティング システム用のネイティブ クライアントをダウンロードできます。

[Horizon ネイティブ クライアントのインストール] をクリックすると、Horizon Client をダウンロードするための Customer Connect ページがブラウザに表示されます。画面上のガイダンスに沿って、使用中のシステムに対応するネイティブ クライアントのインストーラをダウンロードし、ネイティブ クライアントをインストールします。

3 インストールしたら、Horizon Client を起動します。

クライアントには、この Horizon Client で現在構成されているすべての Horizon サイトが表示されます。

4 表示された一連の構成済みサイトで、cloud.vmwarehorizon.com というラベルの付いたサイトを見つけてダブルクリックし、サイトに接続します。

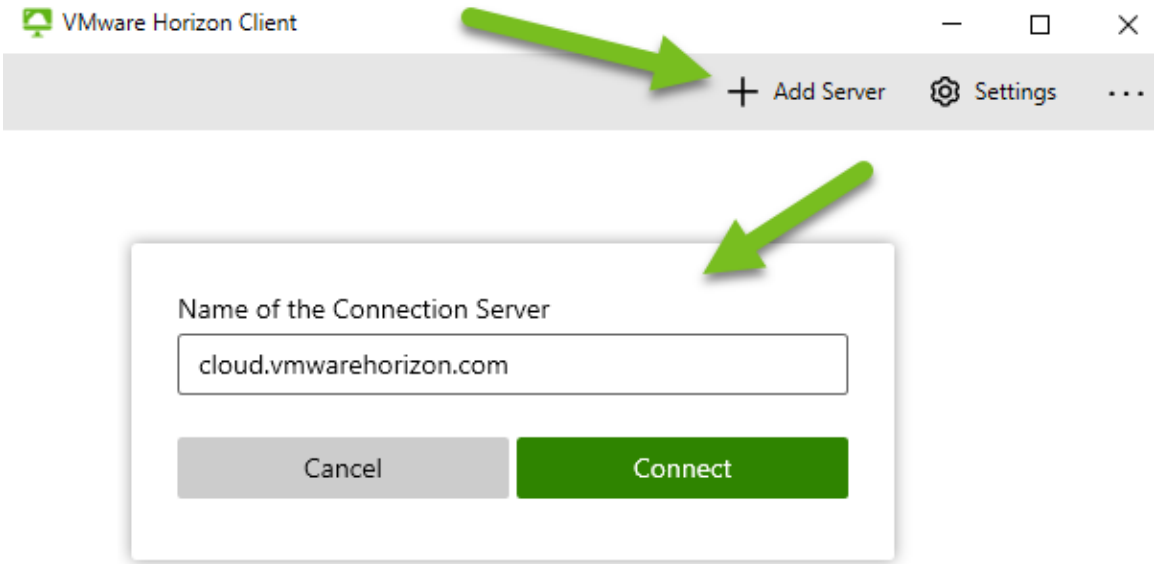
注： これがクライアントの初回インストールである場合、または Horizon Cloud Service - next-gen 環境からアプリケーションまたはデスクトップを起動するのが初めての場合、クライアントには cloud.vmwarehorizon.com 用に構成されたサイトがありません。

その場合は、クライアントの **サーバの追加** ボタンを使用して、[cloud.vmwarehorizon.com] という名前のサイトを追加する必要があります。

a cloud.vmwarehorizon.com というラベルの付いたアイコンが表示されない場合は、[サーバの追加] をクリックして追加します。

クライアントには、cloud.vmwarehorizon.com を入力するためのフィールドが表示されます。

次のスクリーンショットは、Horizon Client for Windows v2303 を使用した一連の手順を示しています。別のネイティブ クライアントまたはバージョンを使用している場合、ユーザー インターフェイスはこのスクリーンショットと異なる場合があります。基本的には、サイト名（サーバ名）を追加し、接続して、クライアントでそのサイトのアイコンを確認するという手順です。

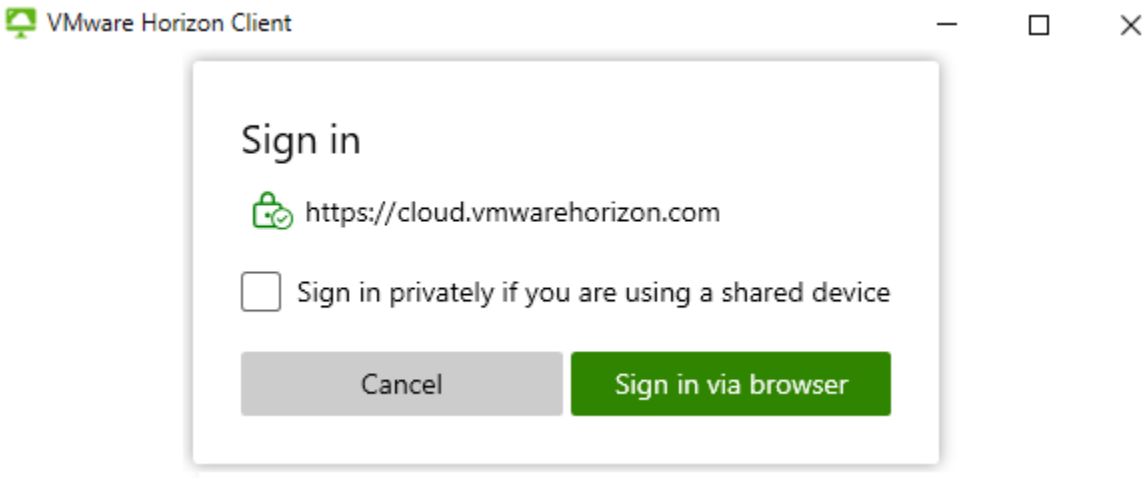


次に [接続] をクリックして、Horizon Client へのサイトの追加を完了します。

5 クライアントに cloud.vmwarehorizon.com のアイコンが表示されたら、そのアイコンをダブルクリックしてサイトに接続します。

表示されるユーザー インターフェイスは、使用しているネイティブ クライアントによって異なります。たとえば、Horizon Client for Windows には [ログイン] ダイアログが表示されますが、Horizon Client for Chrome の場合は [ログイン] ダイアログが表示されません。

次のスクリーンショットは、Horizon Client for Windows v2303 を使用した場合のこの手順を具体的に示しています。



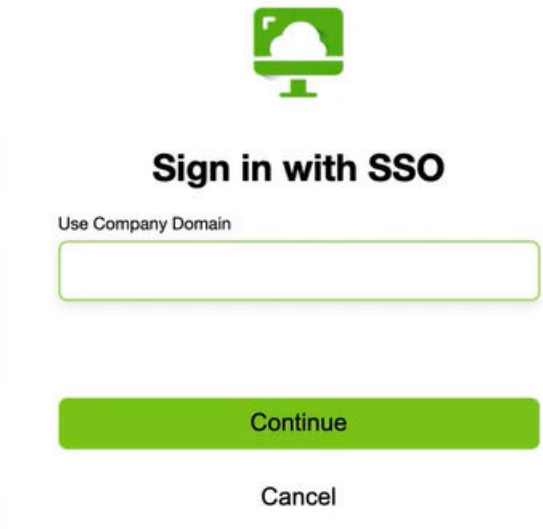
6 クライアントに表示される画面のプロンプトに沿って、ログインに進みます。

使用中のクライアントに [共有デバイスを使用している場合は、プライベートでログインする] オプションがある場合は、そのオプションを使用して、クライアントがデバイス上の情報をキャッシュしないようにすることができます。

注： Horizon Client for Chrome は常にプライベートでログインするため、このクライアントには [共有デバイスを使用している場合は、プライベートでログインする] オプションがありません。Horizon Client for Chrome のサーバ アイコンをクリックすると、クライアントによってブラウザに [SSO でログイン] ユーザー インターフェイスが表示されます。

画面上のプロンプトに沿ってログインすると、ブラウザに [SSO でログイン] ユーザー インターフェイスが表示されます。

次のスクリーンショットは、[SSO でログイン] というユーザー インターフェイスを示しています。



7 [SSO でログイン] で、この Horizon Cloud Service - next-gen 環境に関連付けられている会社のドメインの名前を入力し、[続行] をクリックします。

Horizon Universal Console では、管理者は ID プロバイダ構成で設定されている名前を確認できます。Horizon Cloud Service - next-gen 環境での ID とアクセス管理のページを参照してください。

[続行] をクリックしたら、画面のプロンプトに従います。ID プロバイダのログイン ユーザー インターフェイスが表示されます。その ID プロバイダに割り当てられた認証情報を使用してログインします。

ID プロバイダのログインが完了すると、Horizon 資格画面がクライアントに表示され、割り当てられたデスクトップとアプリケーションが一覧表示されます。

8 アプリケーションのアイコンをクリックして、アプリケーションを起動します。

Web クライアントの Horizon HTML Access を使用したアプリケーションの起動

このドキュメント ページでは、Web クライアントである Horizon HTML Access を使用して、Horizon Cloud Service - next-gen 環境で提供されるアプリケーションを起動する手順について説明します。

前提条件

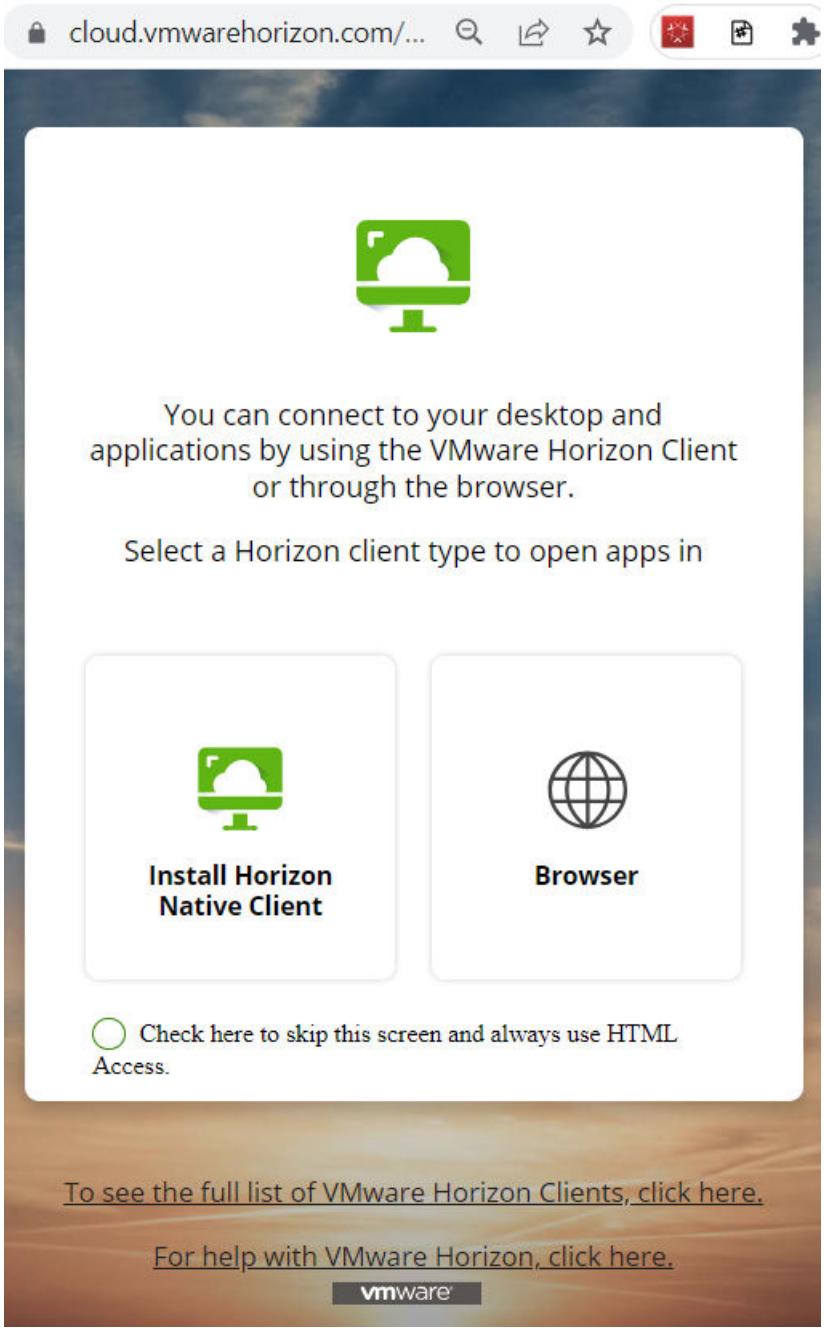
エンド ユーザーが割り当てられたアプリケーションを起動する前に、Horizon Universal Console を使用して、それらのユーザーにアプリケーションの使用資格が付与されていることを確認します。

- マルチセッション プール グループから公開アプリケーションの使用資格を付与する方法については、エンド ユーザーへのデスクトップおよびアプリケーションの資格の付与を参照してください。

手順

1 割り当てられたアプリケーションにアクセスするには、Horizon ポータル (https://cloud.vmwarehorizon.com/) を起動します。

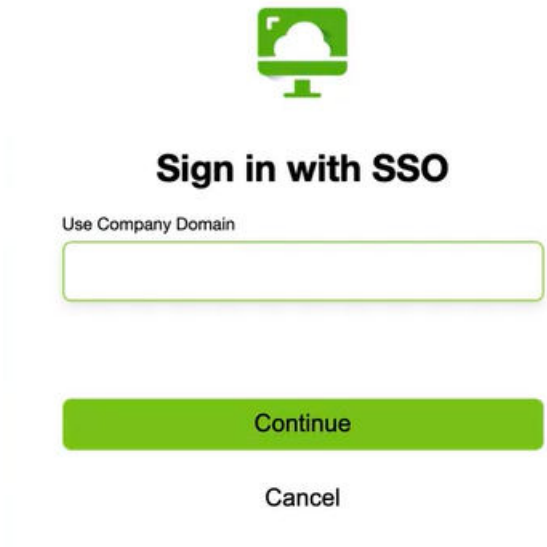
次のスクリーンショットは、ブラウザでその URL に移動したときに表示されるポータルを示しています。



2 [ブラウザ] をクリックし、Web クライアントを使用してアプリケーションに接続します。

[ブラウザ] をクリックすると、ブラウザに [SSO でログイン] というユーザー インターフェイスが表示されます。

次のスクリーンショットは、[SSO でログイン] というユーザー インターフェイスを示しています。



3 [SSO でログイン] で、この Horizon Cloud Service - next-gen 環境に関連付けられている会社のドメインの名前を入力し、[続行] をクリックします。

Horizon Universal Console では、管理者は ID プロバイダ構成で設定されている名前を確認できます。Horizon Cloud Service - next-gen 環境での ID とアクセス管理のページを参照してください。

[続行] をクリックしたら、画面のプロンプトに従います。ID プロバイダのログイン ユーザー インターフェイスが表示されます。その ID プロバイダに割り当てられた認証情報を使用してログインします。

ID プロバイダのログインが完了すると、Horizon 資格画面が表示され、割り当てられたデスクトップとアプリケーションが一覧表示されます。

4 アプリケーションのアイコンをクリックして、アプリケーションを起動します。

グローバル Horizon Client 設定の構成

Horizon Cloud Service - next-gen のテナント環境内のすべてのエンド ユーザーに適用されるグローバル Horizon Client 設定を構成できます。

Horizon Cloud Service - next-gen でのログイン前のメッセージの構成

エンド ユーザーが Horizon Client にログインする前に表示されるメッセージをカスタマイズできます。

手順

1 Horizon Cloud Service - next-gen にログインします。

2 ナビゲーション バーの [設定] をクリックします。

3 [クライアントの設定] タイルで [管理] をクリックします。

4 [クライアントの設定] ページで、[カスタム メッセージ] タブをクリックし、[編集] をクリックします。

5 [ログイン前のメッセージ] を含めるには、スイッチを切り替えます。

6 [ログイン前のメッセージ] フィールドを追加します。また、スイッチを元に戻して、[ログイン前のメッセージ] を無効にすることもできます。

Horizon Cloud Service - next-gen のブランディングを構成する

エンド ユーザーがデスクトップおよびアプリケーションに接続するためにアクセスする URL をカスタマイズできます。

前提条件

使用する URL またはサブドメインを決定します。次の詳細は、使用する URL またはサブドメインに適用されます。

- この URL またはサブドメインは、Horizon Client サービス全体で一意である必要があります。URL またはサブドメインが別のテナントによって使用されている場合、エラーが発生します。自分が所有する URL またはサブドメインが、組織が所有していない別のテナントによって使用されていると思われる場合は、サポート リクエストを提出して通知してください。
- カスタム URL のサブドメインの長さは 1 文字以上 63 文字以下にする必要があります。
- カスタム URL には、英字、数字、ダッシュ (-) のみを使用できます。
- 一部の文字列は、システムによって禁止または予約されています。この文字列のカテゴリには、`book` のような一般的な単語、`Gmail` および `protocol.coding` のような著名企業が所有する用語、および `php` や `sql` のようなオープンソースの用語が含まれます。またシステムは、`mail0`、`mail1`、`mail2` などの文字列のパターンのカテゴリを禁止します。
- 別の組織が所有している URL またはサブドメイン、または自分が所有していない著作権または商標に違反することが判明した URL またはサブドメインは削除されます。

手順

1 Horizon Cloud Service - next-gen にログインします。

2 ナビゲーション バーの [設定] をクリックします。

3 [クライアントの設定] タイルで [管理] をクリックします。

4 [クライアントの設定] ページで、[ブランディング] タブをクリックします。

5 [カスタム クライアント アクセス サブドメイン] を指定するには、次の手順を実行します。

   a [カスタム クライアント アクセス サブドメイン] セクションで、エンドユーザーがデスクトップおよびアプリケーションへの接続に使用するクライアント アクセス URL をカスタマイズするためのサブドメインを指定できます。

   b [編集] をクリックし、[カスタム クライアント アクセス サブドメインの有効化] トグルを選択して有効にします。

   [カスタム クライアント アクセス サブドメインの有効化] フィールドは無効になっており、デフォルトで使用可能なオプションは [いいえ] です。[編集] をクリックした後にのみ、トグルが有効になり、選択できます。

   c [カスタム クライアント アクセス サブドメイン] を追加します。

   カスタム クライアント サブドメインの構成と編集が有効になるまでに最大 10 分かかる場合があります。

6 [カスタム クライアント アクセス URL] を指定するには、次の手順を実行します。

a [カスタム クライアント アクセス URL] セクションで、エンドユーザーがデスクトップおよびアプリケーションへの接続に使用する URL をカスタマイズするための完全修飾ドメイン名を指定します。

注： FQDN を提供されたエンドポイントにマッピングする CNAME レコードを DNS サーバに作成して、エイリアスの関連付けを設定する必要があります。

b [構成] をクリックして URL を構成します。

c [カスタム クライアント アクセス URL] を指定します。

d [参照] をクリックして、以前に `PFX` 形式で入力したカスタム クライアント アクセス URL に対して有効な [証明書] を参照してアップロードします。

e 証明書の [パスワード] を追加します。[保存] をクリックします。

カスタム クライアント サブドメインの構成と編集が有効になるまでに最大 10 分かかる場合があります。

Horizon Cloud Service - next-gen 内部ユーザーを識別するためのネットワーク範囲の構成

このトピックでは、Horizon Client が接続しているオフィスまたはデータセンターのファイアウォールまたはルーターで出力方向 NAT パブリック IP アドレスを指定して、内部ネットワークの範囲を定義する方法について説明します。このように内部ネットワークを定義すると、ブローカは、Horizon Client からデスクトップへの直接接続を許可し、Unified Access Gateway をバイパスするなど、ネットワーク固有のポリシーを適用できます。

ブローカの内部ネットワークを定義するには、[クライアントの設定] ページの [ネットワーク範囲] タブを使用して、内部エンド ユーザー トラフィックに対応する出力方向 NAT のすべての範囲を指定します。

ブローカは、オフィスまたはデータセンターのルーターまたはファイアウォール上の指定された範囲の出力方向 NAT アドレスから接続している Horizon Client を、内部ネットワークから接続しているものとして認識します。これらの範囲内のパブリック IP アドレスから接続するユーザーは、内部ユーザーとみなされます。これらの範囲外のパブリック IP アドレスから接続するユーザーは、外部ユーザーとみなされます。

重要： ネットワーク構成が変更され、指定したアドレス範囲のいずれかが使用されなくなった場合は、[ネットワーク範囲] リストから使用されていない範囲を手動で削除する必要があります。ブローカでは、アドレス範囲が使用中であるかどうかが検出されず、リストから範囲が自動的に削除されることはありません。

前提条件

内部エンド ユーザー トラフィックに対応するオフィスまたはデータセンターのルーターまたはファイアウォールの出力方向ネットワーク アドレス変換 (NAT) アドレスを特定します。

手順

1 Horizon Cloud Service - next-gen にログインします。

2 ナビゲーション バーの [設定] をクリックします。

3 [クライアントの設定] タイルで [管理] をクリックします。

4 [クライアントの設定] ページで、[ネットワーク範囲] タブをクリックします。

[ネットワーク範囲] ページには、内部エンドユーザー トラフィックに対応するパブリック IP アドレス範囲のリストが表示されます。

5 出力方向 NAT アドレス範囲をリストに追加するには、[追加] をクリックします。

6 範囲タイプを選択し、そのタイプのアドレスまたは範囲を入力して、[保存] をクリックします。

オプション	説明
CIDR	[CIDR] を選択し、192.168.70.10/32 など、/1 から /32 までの許容範囲で範囲を入力します。
単一の IP アドレス	[単一の IP アドレス] を選択し、192.168.70.10 などの IP アドレスを入力します。
IP アドレス範囲	[IP アドレス範囲] を選択し、192.168.70.10-192.168.72.32 などの IP アドレス範囲を入力します。

7 内部ネットワーク トラフィックの全範囲を定義するまで、出力方向 NAT アドレス範囲をリストに追加し続けます。

次のステップ

[ネットワーク範囲] タブのコントロールを使用して、リスト内の範囲を [削除] することができます。

注： リストから範囲を削除する前に、次の点を考慮してください。

- 出力方向 NAT アドレス範囲を削除すると、ブローカは、その範囲が外部ネットワークの一部であると見なします。
- リストからすべての範囲を削除すると、ブローカはすべてのユーザーを外部ユーザーとして扱います。そのため、内部ユーザーに適用されたポリシーは有効ではなくなります。

Horizon クラウド資格オンランプの有効化による Horizon 8 および Horizon Cloud on Azure のデスクトップへのアクセス

Horizon クラウド資格オンランプ グローバル設定を使用すると、ユーザーは単一の Horizon Client for Windows の認証情報を使用して、Horizon 8 および Horizon Cloud on Azure の両方のデスクトップにアクセスできます。これにより、複数の URL の使用、複数回のログアウト、追加の認証が不要になります。

前提条件

- VMware Horizon Cloud Service - next-gen テナントで、サポートされている ID プロバイダ (IDP) -- Microsoft Entra ID または VMware Workspace ONE Access (オンプレミス/クラウド) -- が登録されていることを確認します。登録された ID プロバイダは、オンプレミスの Active Directory ユーザー ID をその ID プロバイダと同期します。
- Horizon Connection Server バージョン 2312 以降を実行していることを確認します。
- Horizon 8 Edge をデプロイして、Horizon 8 ポッドを Horizon Cloud Service - next-gen 制御プレーンに接続していることを確認します。

- Horizon Universal Console で、Microsoft Azure をキャパシティ プロバイダとして使用します。プールを作成して、デスクトップ インスタンスをデプロイし、資格を割り当てます。
- Horizon Console で、Horizon 8 プールを作成し、ローカルまたはクラウド ポッド アーキテクチャの資格を割り当てます。
- エンド ユーザーが Horizon Client 2312 for Windows 以降を実行していることを確認します。

Horizon クラウド資格オンランプの仕組み

Horizon クラウド資格オンランプ機能は、仲介メカニズムとして Connection Server を使用して、資格が付与された Horizon Cloud on Azure デスクトップへのアクセスをユーザーに許可します。VMware Horizon Cloud Service - next-gen テナントの ID プロバイダ (IDP) として Microsoft Entra ID または Workspace ONE Access（オンプレミス/クラウド）のいずれかを使用できます。

選択した ID プロバイダにより、オンプレミスの Active Directory からクラウドベースの ID プロバイダへのユーザー アカウント、グループ メンバーシップ、その他のディレクトリ オブジェクトの同期が行われます。この同期により、ユーザーがアクセスするのがオンプレミス リソースかクラウドベースのリソースかにかかわらず、一貫した認証が可能になります。

ID プロバイダとして Workspace ONE Access を使用すると、コネクタが展開され、ユーザー アカウントとグループ メンバーシップが Workspace ONE Access プラットフォームと同期されます。

ユーザーが Connection Server インスタンスに接続すると、Connection Server は、Horizon Cloud on Azure デスクトップに対するユーザーの資格を検証します。Horizon Client は、これらのデスクトップと Horizon 8 デスクトップを同じディスクトップおよびアプリケーションの選択ウィンドウに表示します。これにより、ユーザーは Connection Server または Unified Access Gateway FQDN を介して Horizon Cloud on Azure の資格に直接アクセスできます。VMware Horizon Cloud Service - next-gen ポータルの別の URL は不要になりました。

選択ウィンドウに表示される Horizon 8 の資格は、ローカル資格の場合もあれば、グローバル資格の場合もあります。選択ウィンドウでは、Horizon 8 の資格と Horizon Cloud on Azure の資格が個別のデスクトップとして表示されます。ユーザーは、接続先のデスクトップを選択する必要があります。現時点で、Horizon クラウド資格オンランプは、Horizon 8 の資格と Horizon Cloud on Azure の資格の接続ポリシーを定義する機能をサポートしていません。

重要： 次の機能制限に注意してください。

- 現在、この機能は Horizon Client 2312 for Windows 以降でのみサポートされています。今後、他の Horizon Client でサポートが利用可能になる予定です。
- Horizon Console と Horizon Universal Console の両方からのクライアント制限メッセージを構成した場合、これらのメッセージはクライアントに同時に表示されません。最初のメッセージが表示され、すぐに 2 番目のメッセージに置き換わります。

Horizon クラウド資格オンランプは、Horizon 8 ポッド レベルとユーザー レベルで有効にできます。デフォルトでは、すべてのユーザーに対して無効になっています。このページの次のセクションで説明するように、この機能は管理者が有効にする必要があります。

Horizon Cloud 制御プレーンでの Horizon クラウド資格オンランプの有効化

機能を有効にするプロセスの最初の部分は、Horizon Universal Console を使用して実行します。

1 Horizon Universal Console にログインします。

2 [ホーム] ページで、[Horizon Edge] タイルの [Horizon Edge] をクリックします。

3 [キャパシティ] ページの [Horizon Edge] タブで、[プロバイダ タイプ] が [Horizon 8] の Horizon Edge の名前をクリックして、[Horizon Edge] の詳細ページに移動します。

4 [クラウド資格オンランプ] タイルで、[有効にする] をクリックします。

Horizon Universal Console から Horizon Edge Gateway に Horizon 8 展開の構成がプッシュされます。さらに、この構成は Horizon Connection Server にプッシュされ、Horizon Console で Horizon クラウド資格オンランプ機能が有効になります。

5 このページの次のセクションに進み、Horizon Console でユーザー資格を追加します。

Horizon Console での Horizon クラウド資格オンランプの資格の追加

Horizon Cloud 制御プレーンで Horizon クラウド資格オンランプ機能を有効にした後、該当するユーザーとグループに対して、Horizon Console で [クラウド資格オンランプ] の資格を構成する必要があります。

1 Horizon Console にログインします。

2 [グローバル設定] で、[クラウド資格オンランプ] の設定が有効になっていることを確認します。

注： 設定が有効になっていない場合は、Horizon Edge Gateway、Horizon Universal Console、Horizon Connection Server の間のネットワーク接続を確認します。

3 [ユーザーとグループ] - [クラウド資格オンランプ] に移動し、[追加] をクリックします。

4 Horizon Cloud on Azure デスクトップにアクセスする必要があるユーザーとグループを追加します。

Horizon 制御プレーンと Horizon Cloud Service - next-gen 環境のトラブルシューティング

8

トラブルシューティングのガイダンスは、多くの場合、Horizon 制御プレーンと Horizon Cloud Service - next-gen の製品のユーザー インターフェイスと、該当するドキュメント トピックの両方で提供されます。

トラブルシューティングを支援するために、次のリソースを使用することもできます。

- VMware Customer Connect の Horizon Cloud Service に関するベンダー サポート、コミュニティ、およびナレッジベース (KB) の記事。
- Digital Workspace Tech Zone の Horizon Cloud Service に関するテクニカル マーケティング ブログ、ビデオ、および記事。

Edge のデプロイ ワークフロー中に問題やエラーが発生した場合のために、次のページではいくつかの問題とそのトラブルシューティング方法および修正手順について説明します。

- Horizon 8 Edge が接続保留中の状態で停止する
- 指定された Horizon Connection Server の認証情報が正しくないというエラー
- Connection Server のタイムアウト エラー
- 以前はすべてが機能していたが、現在は機能していない
- プロバイダの作成中に Horizon Connection Server の詳細が必要な古いフローが表示される

次のトピックを参照してください。

- Horizon Edge の診断 - Microsoft Azure デプロイの Active Directory 接続
- Horizon 8 Edge が接続保留中の状態で停止する
- 指定された Horizon Connection Server の認証情報が正しくないというエラー
- Connection Server のタイムアウト エラー
- 以前はすべてが機能していたが、現在は機能していない
- プロバイダの作成中に Horizon Connection Server の詳細が必要な古いフローが表示される

Horizon Edge の診断 - Microsoft Azure デプロイの Active Directory 接続

Horizon Edge でオンデマンド診断を実行できます。Active Directory 診断がサポートされます。Horizon Edge にリンクされた Active Directory の問題を検出した場合は、Horizon Universal Console を使用して、

特に [監視] - [診断] ページで問題の診断に役立ちます。次に、Active Directory 構成に直接移動して、適切な接続を妨げる原因を特定して修正します。

Microsoft Azure の Active Directory は、デプロイの早い段階で設定します。マシン ID の要件および Active Directory ドメインの設定を参照してください。Active Directory で構成の問題が発生している場合は、Horizon Universal Console の [診断] ページから、次の手順を行うテストを実行できます。

- Horizon Edge への Active Directory（1 つまたは複数のインスタンス）接続をテストします。
- Active Directory のドメイン認証情報（プライマリ ドメイン、補助ドメイン、SSO）をチェックします。

[診断] ページへのアクセス

Active Directory の問題を検出したら、[診断] ページにアクセスして詳細な調査を行います。

[診断] ページにアクセスするには、Horizon Universal Console で [監視] - [診断] を選択します。

注： [ホーム] - [インフラストラクチャ エラーのある Horizon Edge] ページで、Active Directory 関連のエラーに関する履歴情報を表示できます。リソース監視データ：エラーを参照してください。

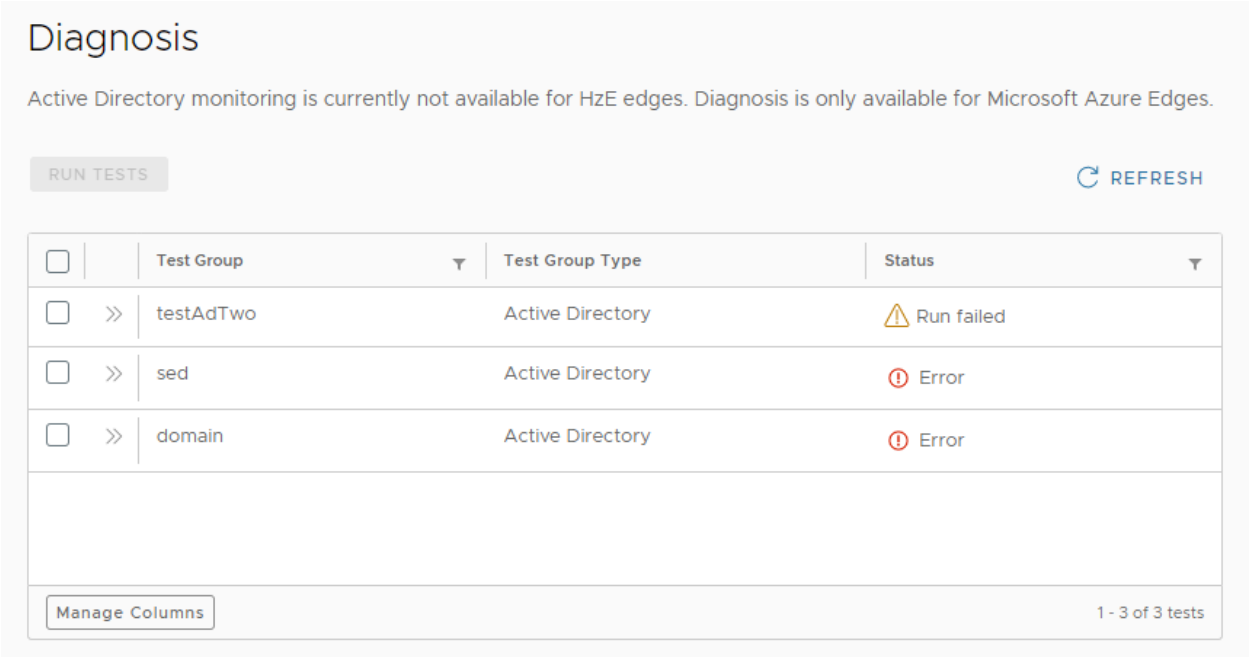
[診断] ページの表示

[診断] ページには、検出されたすべての Active Directory インスタンス（存在する場合）が一覧表示されます。

テスト グループ（Active Directory インスタンス）が一覧表示されると、次の情報が提供されます。

- 各テスト グループの名前。
- テスト グループの全体的な診断ステータス。

  全体的な診断ステータスには、Active Directory とすべての Microsoft Azure Edge 間の接続の概要が表示されます。1 台以上の Microsoft Azure Edge がエラー状態の場合、ステータスは [エラー] と表示されます。各 Microsoft Azure Edge のステータスを確認するには、テスト グループを展開する必要があります。



テストを実行

[診断] ページでは、すべての Microsoft Azure Edge で一覧表示されているテスト グループのいずれかで診断テストを実行できます。

1 テストするテスト グループの名前の横にあるチェック ボックスを選択します。

2 [テストを実行] をクリックします。

選択した各テスト グループに対してテストが実行されます。

Active Directory 接続の結果の確認

[診断] ページでは、各テスト グループのステータスを一度に 1 つずつ確認できます。

次のステータスの説明は、ステータス タイプを区別するのに役立ちます。

成功

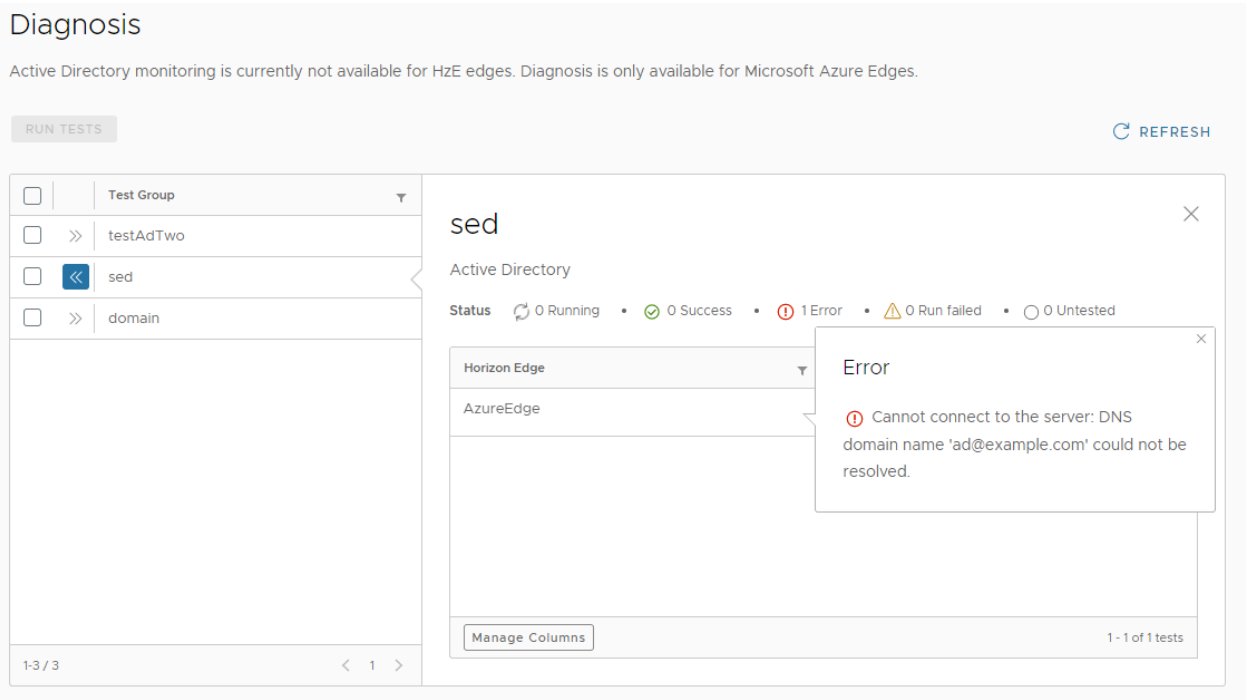
接続に成功しました（接続エラーはありません）。

エラー

接続の問題があります。エラー メッセージは、エラーの正確な原因を説明します。エラー メッセージの情報を使用して、Active Directory 構成に必要な変更を加えます。

実行に失敗しました

テストが完了しませんでした。テストを再実行します。



1 確認するテスト グループの横にある二重矢印をクリックします。

ペインが開き、そのテスト グループ内のすべての Microsoft Azure Edge の診断ステータスが表示されます。

2 エラーを確認するには、エラー メッセージを表示する Horizon Edge の [ステータス] 列で [エラー] をクリックします。

いくつかの異なるタイプのエラー メッセージが存在します。プライマリ バインド アカウントに関するエラー メッセージの例を次に示します。これは、プライマリ バインド アカウント (`Error connecting to AD server using Primary Bind Account`) に対して入力された認証情報を確認する必要があることを示しています。

3 エラー メッセージに記載されている情報を使用すると、後で Active Directory 構成にアクセスするときに問題のトラブルシューティングと修正に役立ちます。

Horizon 8 Edge が接続保留中の状態で停止する

問題

Horizon 8 Edge が [接続保留中] の状態で停止します。

原因

VMware vCenter に Horizon Edge Gateway をデプロイするときにペアリング コードが指定されませんでした。ペアリング コードは、他の状態の Edge をマークする（最大で 15 ～ 20 分かかる場合があります）ために必要なモジュールを持つ Horizon Edge Gateway に Kubernetes 名前空間を作成するのに必要です。ペアリング コードは、VMware vCenter の 2 番目の画面の root パスワードの下に表示されます。

ペアリング コードが正しく指定されている場合は、edge-deployments API 呼び出しを確認します。edge-deployments API 呼び出しは、次のサンプルのようになります。

```
admin/v2/edge-deployments/63da2d9216884348cf96a0f5?include_reported_status=true
```

ユーザー インターフェイスでは、Edge デプロイの詳細ページが開くと呼び出されます。[view-cs-module] が [registeredModules] の下にあり、[reportedStatus] - [moduleConnectionDetails] 内に [view-cs-module] が存在し、[CONNECTED] 状態になっていることを確認してください。

詳細については、https://kb.vmware.com/s/article/92056 を参照してください。

解決方法

[view-cs-module] が [registeredModules] の下にあり、[reportedStatus] - [moduleConnectionDetails] 内に [view-cs-module] が存在し、[CONNECTED] 状態になっていることを確認してください。

また、次のタスクも実行します。

1 Horizon Edge Gateway が正しくデプロイされ、パワーオン状態であることを確認してください。展開に何らかの問題がある場合は、ネットワーク、ストレージなどを確認します。

2 `ccadmin` ユーザーがログインするためのパブリック キーを指定する場合は、`2.3.1.0` 以降の Horizon Edge Gateway OVA バージョンを使用します。古いバージョンの OVA の場合、`ccadmin` ユーザーのパブリック キーが指定されていると Kubernetes の初期化中に問題が発生します。

3 診断スクリプトをデバッグ モードで実行します。詳細については、「https://kb.vmware.com/s/article/92056」を参照してください。[Kubernetes Cluster Section] には、Horizon Edge Gateway が初めてパワーオンされたときに作成された名前空間が表示されます。

   a そうではなく、名前空間が作成されていない場合は、手順 2 でネットワークが適切に構成されていないか、Edge Gateway OVA のデプロイ中に Edge Gateway の作成中にペアリング コードが指定されなかった可能性があります。

      ペアリング コードは、Horizon Edge Gateway アプライアンスのデプロイ中に指定されなかった場合、Horizon Edge Gateway アプライアンスのデプロイ後に構成できます。Horizon Edge Gateway アプライアンスのデプロイ後に、Horizon Universal Console からペアリング コードをコピーし、次のコマンドを実行してペアリング コードを構成します：`/opt/vmware/bin/pair-edge .sh '<Pairing_Code_Copied_From_Horizon_Universal_Console>`。

   b 名前空間が作成されても、Edge がまだ接続保留中のままになっている場合は、ネットワーク接続に問題があるか、クラウド URL が Edge からアクセスできない（プロキシ構成またはその他のネットワーク関連の問題が原因である可能性があります）、またはプロキシ構成が Edge で更新された可能性があります。

   c その後、名前空間が正常に作成されると、ユーザー インターフェイスで Edge が [未構成] 状態に表示されるか、API に [`POST_PROVISIONING_CONFIG_IN_PROGRESS`] と表示されるまでに 15 ～ 20 分かかることがあります。この問題が発生した場合は、Connection Server を構成できます。

      それでも問題が解決しない場合は、診断スクリプトを実行し、[Kubernetes Cluster Section] で `view-cs-module` ポッドが実行状態になるまで待機します。診断スクリプトをデバッグ モードで実行します。詳細については、「https://kb.vmware.com/s/article/92056」を参照してください。

指定された Horizon Connection Server の認証情報が正しくないというエラー

問題

たとえば、`VIEW_INCORRECT_CS_CREDENTIALS` のようなエラーがユーザーに表示されます。

原因

これは、指定された Horizon Connection Server の詳細が正しくない場合に発生する可能性が高くなります。

解決方法

以下の条件が満たされていることを確認してください。

Connection Server のユーザー名とパスワードが正しいこと。FQDN が、Connection Server の IP アドレスではなく、`https://cs83.hzeccad.com` などの実際の URL であること。Horizon Connection Server の詳細の例：

```
{
    "providerDetails": {
        "data": {
            "domain": "hzeccad.com",
            "viewPodURL": "https://cs83.hzeccad.com",
```

```
            "username": "Administrator",
            "password": "*******",
            "thumbprint": "E4:3B:70:DE:AF:0F:44:F8:6E:87:0C:F1:F6:2D:09:2F:A5:E3:4A:4B"
        }
    }
}
```

注： この例で、******* は実際のパスワードを表します。

Connection Server のタイムアウト エラー

問題

たとえば、「Connection Server への要求がタイムアウトしたため、Connection Server の認証情報を検証できません」などのエラーが表示されます。

原因

Horizon Connection Server が過負荷状態になっています。

解決方法

1 Connection Server が過負荷になっていないことを確認してください。

2 このエラーは、誤った Horizon Connection Server の詳細が指定された場合にも発生する可能性があるため、しばらくしてからやり直してください。

以前はすべてが機能していたが、現在は機能していない

問題

以前はすべてが機能していたが、現在は機能していません。

原因

Horizon Connection Server の詳細が Horizon Cloud Service - next-gen ではなく VMware vCenter で更新されました。

解決方法

Connection Server の詳細が Horizon Cloud Service - next-gen ではなく VMware vCenter で更新されていることを確認してください。また、証明書の有効期限を確認し、サムプリントが変更されていないことを確認してください。

プロバイダの作成中に Horizon Connection Server の詳細が必要な古いフローが表示される

問題

プロバイダの作成中に Horizon Connection Server の詳細が必要な古いフローが表示されるか、次の API エラーが表示されます。

```
domain:  SG_ADMIN
code:    PROVIDER_INSTANCE_CREDENTIALS_ERROR
message: Credential service error for Provider Instance
details: Cannot create a provider instance without any sensitive data!
```

原因

ユーザー インターフェイスの機能フラグ `astro-cs-sync-validation` と API の機能フラグ `cs-sync-flag` がユーザーに対して無効になっている可能性があります。

解決方法

これは、public-flag API 呼び出しで確認できます。これらが無効になっていると、プロバイダの手順で Horizon Connection Server の詳細が必要な古いフローが表示されます。ユーザーの組織でこれらの機能フラグがオンになっていることを確認してください。

Horizon Cloud Service - next-gen を操作する場合のベスト プラクティスおよび推奨事項

9

これらの役に立つベスト プラクティスと推奨されるワークフローに従って、組織内の Horizon Cloud Service - next-gen 機能のメリットを最大限に活用できます。

次のトピックを参照してください。

- Horizon Universal Console とテナントを使用する上でのヒント
- ヘルプ ボタンを使用したドキュメントとサポートへのアクセス
- 製品フィードバックの共有
- Cookie の使用方法とサードパーティ分析ツール
- ページを離れる

Horizon Universal Console とテナントを使用する上でのヒント

Horizon Universal Console には、テナントの最新の状態に基づいて機能の要素が動的に表示されます。

これらの状態には、サブスクリプションの提供内容、購入したアドオン サービスの提供内容、テナント内の Edge デプロイのタイプなどが含まれます。サブスクリプションによって管理される内容のタイプについては、「Horizon サブスクリプション比較マトリックス」を参照してください。サブスクリプションでサポートされていない機能、または Horizon Universal サブスクリプションで使用するために購入されたアドオン サービスによって提供される機能については、Horizon Universal Console に要素が表示されません。

Horizon Universal Console 機能の詳細については、次のトピックを参照してください。

ヘルプ ボタンを使用したドキュメントとサポートへのアクセス

ヘルプ ボタンを使用すると、Horizon Cloud Service - next-gen および関連する製品ドキュメントを参照して質問への回答を見つけたり、Customer Connect にアクセスしてサポートを受け取ったり、チケットを発行したり、チケット履歴を表示したりできます。

前提条件

オンボーディング プロセスが完了していること。

手順

1 Horizon Universal Console にログインします。

2 ホーム ページの [ヘルプ] ボタンをクリックします。

3 検索フィールドにキーワードを入力して、関連するトピックを検索します。

[ヘルプ] ボタンをクリックすると、現在のページに関連するドキュメント リンクがリストに表示されます。たとえば、プール ページで [ヘルプ] ボタンをクリックすると、プールに関連するすべての関連ドキュメント リンクがヘルプ パネルに表示されます。

4 [ドキュメントでさらに表示] をクリックして、[ドキュメント] ページに移動します。

5 [サポート リクエストを作成します] タイルをクリックして [Customer Connect] に移動し、サポート チケットを発行します。

6 [すべてのサポート リクエストの表示] をクリックして、すべてのサポート リクエストのリストを表示します。

7 [サポート エクスペリエンスに関するフィードバックの提供] をクリックして、フィードバックを提供します。

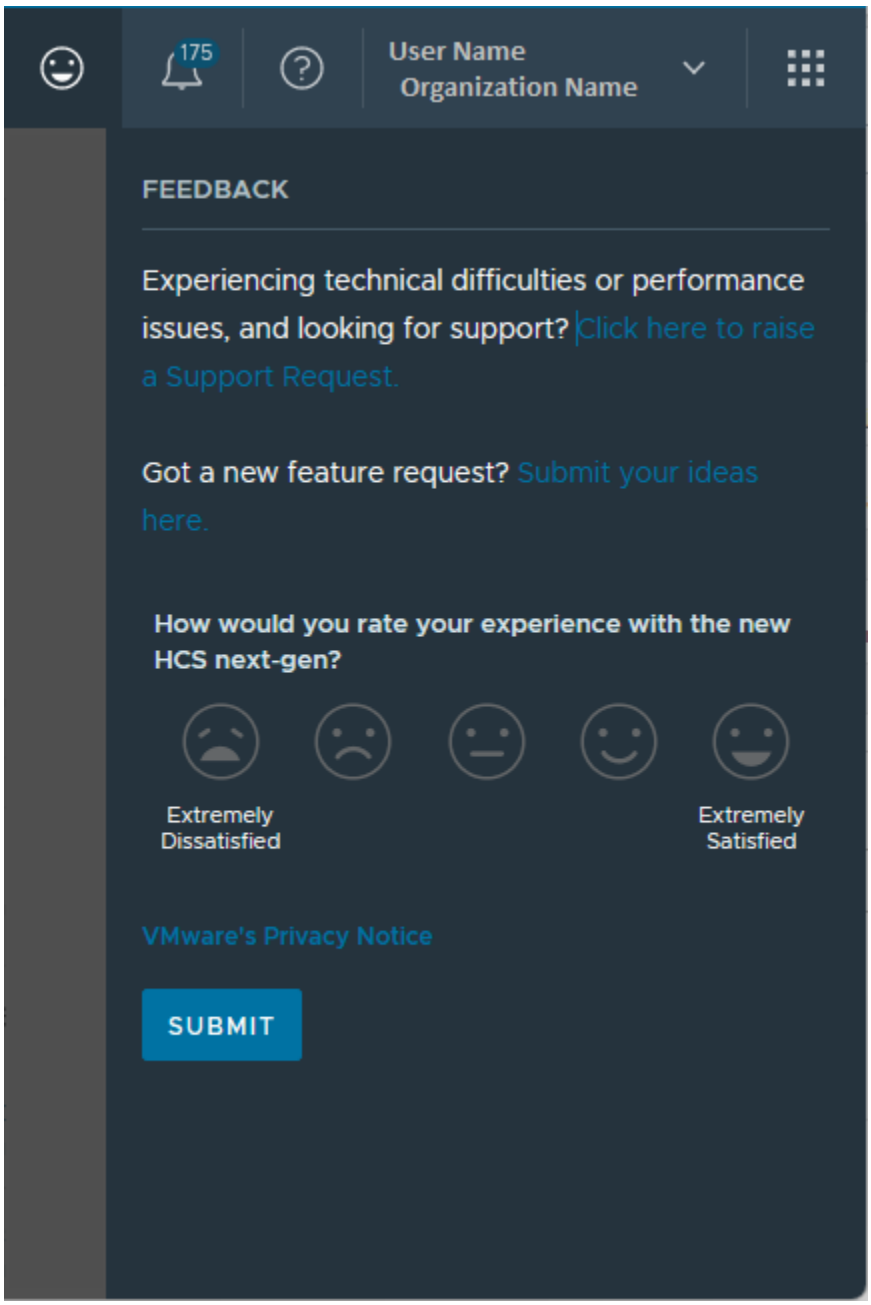
製品フィードバックの共有

製品内フィードバックは、フィードバックを共有できる機能です。この機能は、ご使用の製品の品質向上に役立ちます。

フィードバックを共有するには、次の 2 つの方法があります。

- コンソールの上部にあるフィードバック アイコン をクリックすると、コンソールの右側で [フィードバック] パネルが開きます。
- [フィードバック] パネルは、コンソールにログインした後に表示される場合があります。パネルがコンソールの中央に開きます。

次のスクリーンショットは、フィードバック アイコンをクリックしたときに表示される [フィードバック] パネルです。



[フィードバック] パネルが開くと、次のアクションを実行できます。

サポート リクエストを発行する。

リンクをクリックしてサポート リクエストを発行するときに、Customer Connect にログインしていない場合は、[Customer Connect] ページが表示されるので、ログインします。

ログインすると、[サポート] ページが表示され、さまざまなサポート オプションを選択できます。

アイデアを送信する。

リンクをクリックしてアイデアを共有するときに、Customer Connect にログインしていない場合は、Customer Connect に移動してログインするように促されます。

ログインすると、機能要求ポータルに移動し、[Horizon] などのワークスペースを選択して、そのワークスペースのアイデアを共有するように求められます。

製品を評価する。

[エクスペリエンスを評価] アイコンのいずれかを選択すると、パネルが展開され、特定のフィードバックを提供したり、フォローアップの会話に参加するかどうかを示したりできます。

Cookie の使用方法とサードパーティ分析ツール

Horizon Cloud は、カスタマー エクスペリエンスを観察して向上させるため、およびその他の目的のためにデータを収集します。

Horizon Cloud は、VMware のプライバシー通知に従ってデータを収集します。このデータの一部は、Pendo などの Cookie や同様のテクノロジーを使用して収集されます。

Pendo は、Horizon Cloud と統合されたサードパーティ ツールで、管理者がどのように機能を操作して使用しているかを追跡することによって、Cookie を収集し、製品機能がどのように使用されているかを判断します。

ページを離れる

Horizon Cloud Service - next-gen で、ワークフローを完了せずにページを離れようとすると、ページに残るようにという警告を受け取り、移動した場合は作業が失われる可能性があります。

手順

1. ページのすべての手順を完了する前に [戻る] または任意のリンクをクリックすると、ページを離れると変更が失われる可能性があることを示すダイアログ ボックスが表示されます。[キャンセル] をクリックしてページに残るか、[終了] をクリックしてページを終了します。
2. [更新] をクリックしてページのすべての手順を完了する前にページを更新すると、ページを離れると変更が失われる可能性があることを示すダイアログ ボックスが表示されます。[再ロード] をクリックしてページを更新するか、[キャンセル] をクリックしてページに残ります。
3. ページのすべての手順を完了する前にタブまたはウィンドウを閉じようとすると、ページを離れると変更が失われる可能性があることを示すダイアログ ボックスが表示されます。[離れる] をクリックしてページを離れるか、[キャンセル] をクリックしてページに残ります。

Horizon Plus のドキュメント

10

Horizon Plus のドキュメント ページには、サービスの使用を開始する方法が記載されています。

ウェルカム メール

VMware は、管理者アカウントにウェルカム メールを送信して、ライセンスの評価または購入を確認します。この E メールは、登録を確認するものであり、VMware Horizon Cloud へのアクセスと引き換える招待リンクが含まれています。

VMware Horizon® Cloud Service™ は、Anywhere Workspace ソリューション全体の一部です。

VMware Horizon® Cloud Service™ - next-gen の Horizon Cloud ライセンス サービスは、IT 管理者が購入したライセンス タイプに基づいて機能にアクセスして利用できるようにします。

Horizon サブスクリプションのライセンス機能の比較については、VMware Horizon サブスクリプション比較マトリックスを参照してください。これは、ライセンスを期間と SaaS に大別します。現在リストされているすべての機能が VMware Horizon® Cloud Service™ - next-gen に適用されるわけではありません。

注： ウェルカム メールには、購入したライセンスのタイプに関する情報は含まれません。このような情報は、自分の VMware Customer Connect™ アカウントから取得できます。Customer Connect ユーザーになるには、ナレッジベースの記事 KB2007005 を参照してください。

オンボーディング プロセスが完了したら、Horizon のライセンスを Horizon Universal Console から追跡できます。現時点で、次世代の Horizon 制御プレーンにのみアクセスできる場合は、VMware のサポートに問い合わせ、無期限キーの送付を依頼してください。詳細については、Horizon Universal Console を使用した Horizon ライセンスの追跡を参照してください。

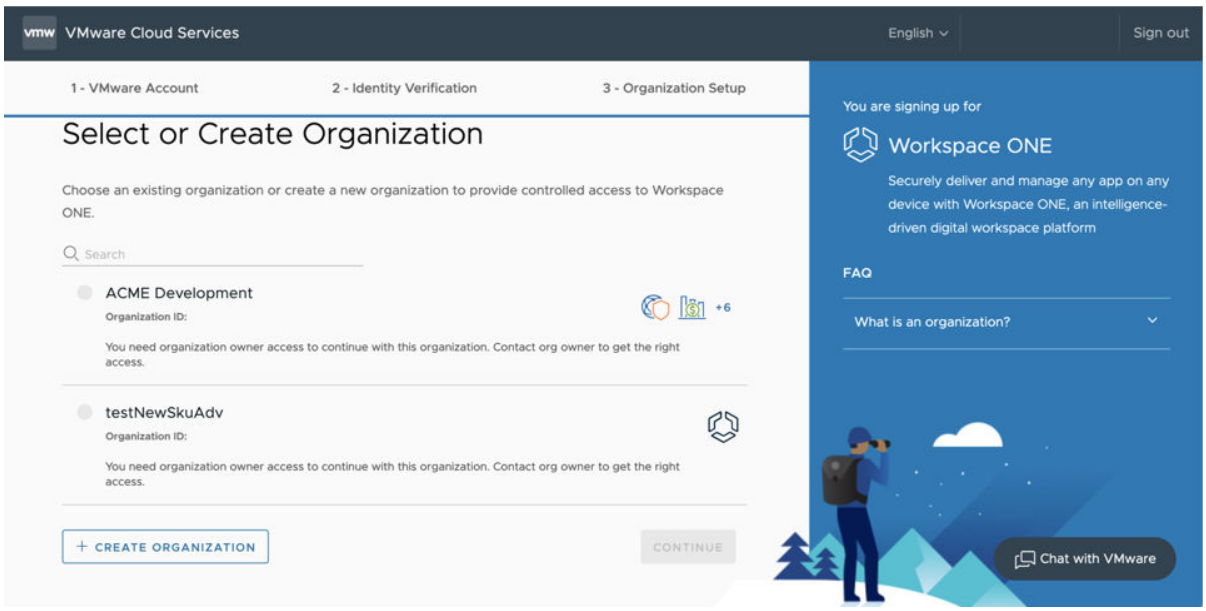
VMware Cloud Services コンソールへのログイン

注： VMware Cloud™ Services の詳細については、VMware Cloud Services 製品ドキュメントを参照してください。VMware 製品およびドキュメントでは、「VMware Cloud Services Platform」(CSP) や「VMware Cloud Services Engagement Platform」など、VMware Cloud services に他の名前が使用されることがあります。

1 新しい VMware Cloud services アカウントを作成します。

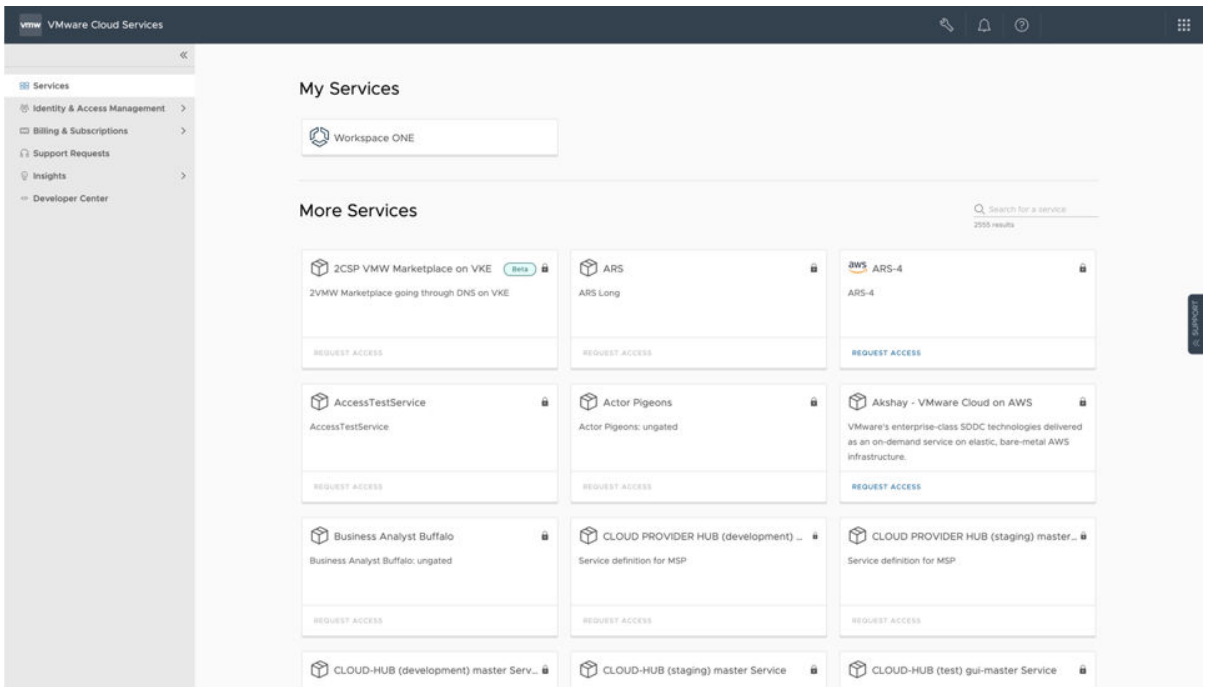
手順は、「ウェルカム メール」から始まります。E メール内のリンクをクリックし、VMware Cloud services アカウントを作成し、VMware ID を使用して VMware Cloud services にログインします。

VMware Cloud Services コンソール で [組織のセットアップ] ページが開きます。



2 選択した組織名を入力し、[組織を作成してサインアップを完了する] をクリックします。

VMware Cloud services コンソール ページが表示され、すべてのサービスが表示されます。



3 右上隅の名前をクリックし、[組織を表示] をクリックします。

VMware Cloud Services コンソール に戻り、必要なロールを割り当てることができます。

ユーザーの追加とロールの割り当ての概要

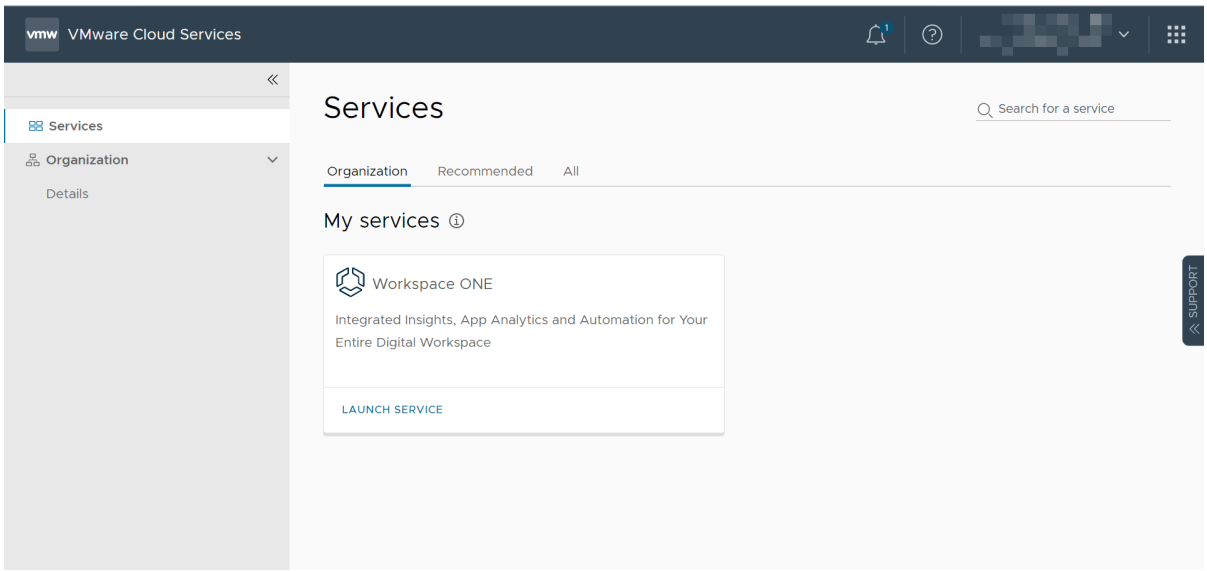
ウェルカム E メールのリンクを使用して招待を引き換えると、自動的に管理者ロールが割り当てられます。管理者ロールにより、オンボーディングする必要がある Horizon Universal Console のユーザー インターフェイスと API に対する完全な権限が付与されます。Horizon Universal Console へのアクセス権を他の管理者ユーザーに付与することができます。詳細については、Horizon Universal Console ユーザーへの管理ロールの割り当て

VMware Cloud Services コンソール を使用して Workspace ONE を起動する

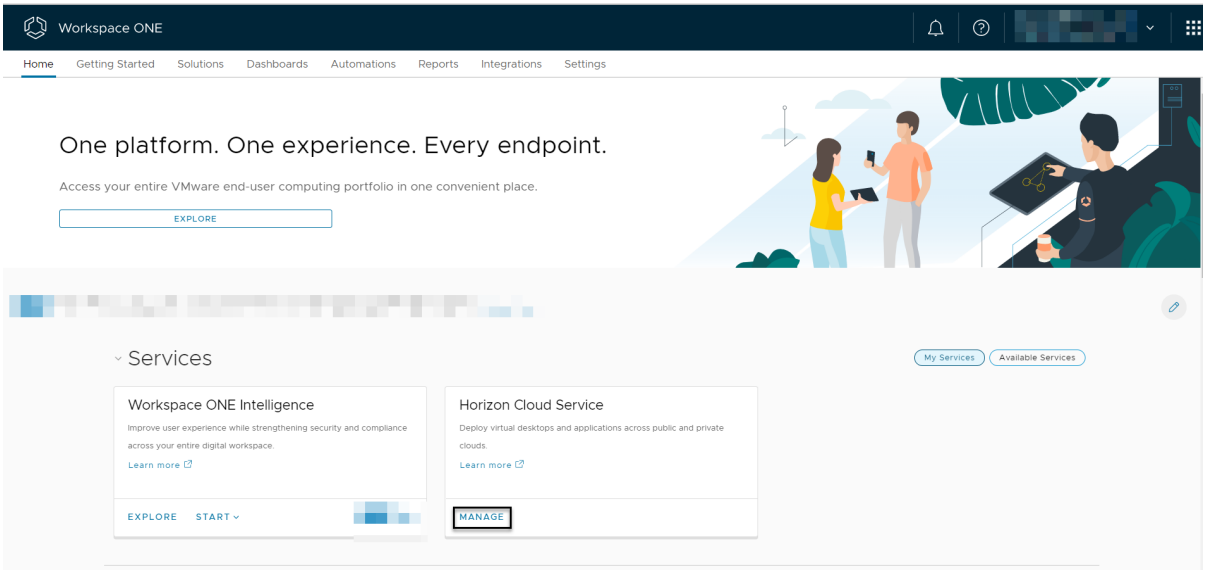
Horizon Cloud を起動するには、次の手順を実行します。

1 左側のペインで、[サービス] をクリックします。

2 Workspace ONE に対して [サービスの起動] をクリックします。

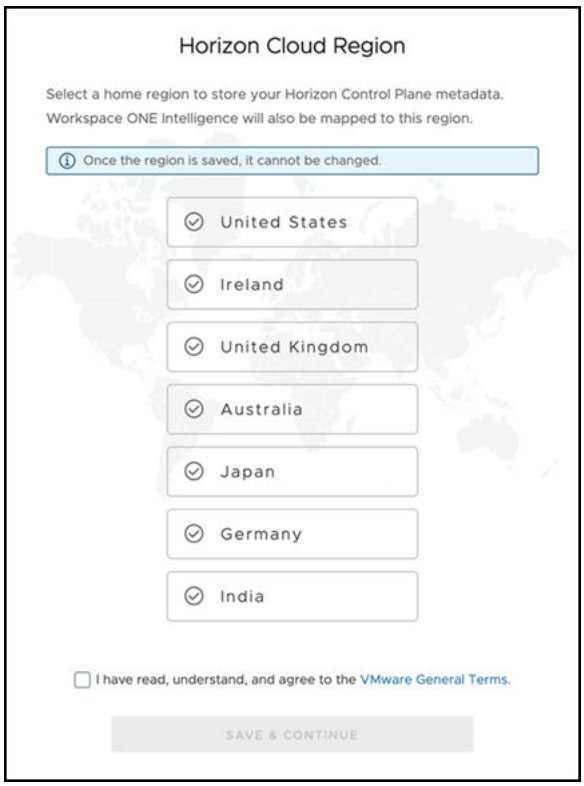


3 [Horizon Cloud Service] タイルで [管理] をクリックして、Horizon Universal Console を起動します。



Horizon Universal Console を使用して Horizon Cloud リージョンを選択する

コンソールを起動すると、リージョンを選択するように求められます。データ主権の原則に準拠するには、リソースとそのメタデータを配置するリージョンを選択する必要があります。一度選択したリージョンは変更できません。



1 Horizon Cloud リージョンを選択します。

2 サービスの利用条件に同意するチェックボックスを選択します。

3 [保存して続行] をクリックして、[Horizon Universal Console の使用開始] ページに移動します。

注： この時点で、Horizon Universal Console に、ライセンスの同期が進行中であることを示すバナーが画面の上部に表示されることがあります。この場合、同期が完了してブラウザを更新するまで、コンソールには特定のライセンスによって有効になるすべての機能が表示されません。同期が完了すると、ユーザーのライセンスに該当する要素が Horizon Universal Console に表示されます。

次のトピックを参照してください。

- Horizon Cloud Service - next-gen を使用した Horizon Plus の使用開始とデプロイ
- Horizon Edge リソースの可用性の監視 - Horizon Plus
- Splunk Enterprise を使用した Horizon 8 Edge の監視の構成

Horizon Cloud Service - next-gen を使用した Horizon Plus の使用開始とデプロイ

このドキュメント ページでは、Horizon Plus サブスクリプションを使用し、Horizon Universal Console にログインして Horizon Cloud リージョンを選択する手順をすでに完了しており、Horizon 8 ポッドを Horizon Cloud Service - next-gen 制御プレーンに接続する必要があるユースケースの Horizon Universal Console の [Horizon Edge を追加] ワークフローの手順について説明します。

概要

Horizon 8 Edge のデプロイには、Horizon Edge Gateway アプライアンスの目的の仮想化プラットフォームへのデプロイ、そのアプライアンスと next-gen 制御プレーンのペアリング、Horizon 8 Edge 用の Horizon 8 ポッドの Horizon Connection Server の詳細の構成が含まれます。

注： 各 Horizon 8 ポッドを個別の Horizon Edge としてオンボーディングします。

このエンドツーエンドのプロセスには、複数の手順があります。

1 このプロセスは、Horizon Universal Console で開始します。

2 その途中で、OVA アプライアンスを vSphere 環境（非フェデレーション）にデプロイします。OVA のデプロイ時に、プロセスの最初の部分で作成されるペアリング コード情報を OVF テンプレートのデプロイ ユーザー インターフェイス フィールドで使用する必要があります。

   注： Horizon Edge Gateway OVA/OVF デプロイは、オールイン SDDC アーキテクチャまたはキャパシティ タイプのプライベート データセンターを使用する Horizon 8 プロバイダのみが使用できます。フェデレーション アーキテクチャを使用する Horizon 8 プロバイダの場合は、「Horizon Cloud Service - next-gen を使用した Horizon 8 フェデレーション デプロイの構成」で説明されている特定のキャパシティ タイプの手順を参照してください。

3 次にアプライアンスをパワーオンしたら、Horizon Universal Console に戻り、ペアリング ステータスが成功したことを確認し、このコンソールの残りの手順を完了して Horizon 8 ポッドの詳細を追加します。

ご使用前の注意事項

次の VMware Tech Zone のビデオを参照してください。

VMware Tech Zone では、Horizon 8 Edge をデプロイするための主なベスト プラクティスを示す 4 つのビデオを作成しました。

- Horizon Edge Gateway アプライアンスのデプロイ - DNS 構成 (https://via.vmw.com/tchzmno5209)。
- Horizon Edge Gateway アプライアンスのデプロイ - URL チェッカー (https://via.vmw.com/tchzmno5210)。
- Horizon Edge Gateway アプライアンスのデプロイ - プロバイダとアプライアンスの構成 (https://via.vmw.com/tchzmno5211)。
- OVA からの Horizon Edge Gateway アプライアンスのデプロイ (https://via.vmw.com/tchzmno5212)。

タイトルは、ビデオの検索を支援するために上記で提供されています。

ユーザーまたは IT チームが次の項目を完了していることを確認します。

- Horizon 8 Edge をデプロイするための要件チェックリストを参照して、これらの要件が満たされていることを確認します。
- 「Horizon 8 Edge デプロイ」ページ内のリンクされたページで説明されている準備項目を参照し、これらの項目が完了していることを確認します。
- デプロイされた Horizon Edge Gateway アプライアンスに使用する完全修飾ドメイン名 (FQDN) を判断します。ユーザー インターフェイス ウィザードで、その FQDN を入力するように求められます。
- この Horizon Edge に含まれる Horizon Connection Server に自己署名証明書がある場合は、ウィザードの検証手順の証明書のフィンガープリントを確認してください。

[Horizon Edge を追加] ウィザードを開始する

Horizon Edge をデプロイする場合は、コンソールの [Horizon Edge を追加] ウィザードを使用します。

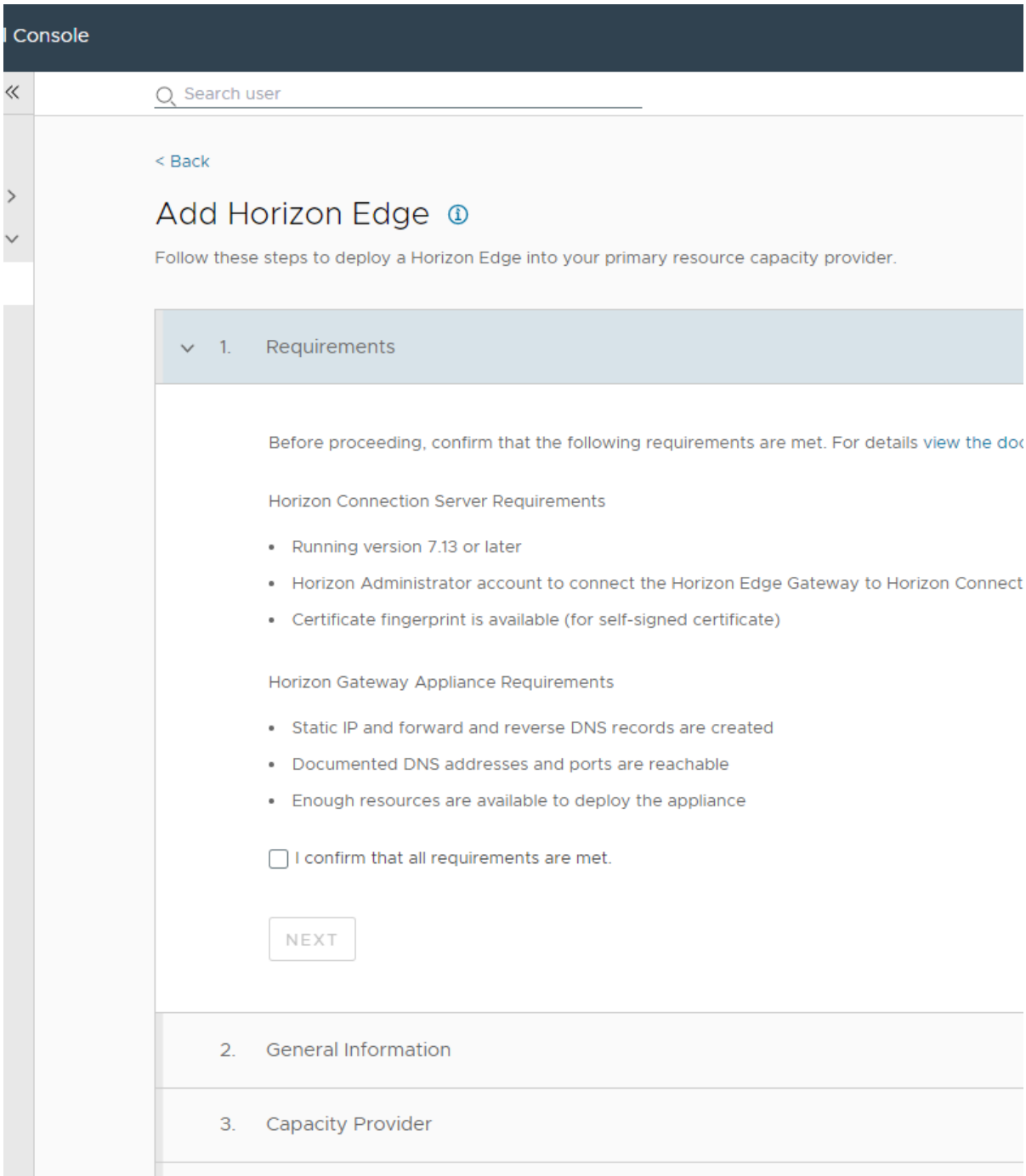
コンソールでは、[Horizon Edge を追加] ウィザードをさまざまなエントリ ポイントから使用できます。コンソールでのこの手順の開始点は通常、環境が新規であるか、既存の Horizon Edge が存在するかによって異なります。

- 「Horizon Plus のドキュメント」ページで説明されている手順を完了したばかりの場合、環境内に既存の Horizon Edge がなく、コンソールに [ようこそ] 画面が表示されます。この場合、[開始] をクリックして、コンソールの [Horizon Edge を追加] ウィザードを開始します。
- 環境に少なくとも 1 台の Horizon Edge がある場合、[キャパシティ] ページには既存の Horizon Edge を一覧表示するグリッドが表示されます。このシナリオでは、[リソース] - [キャパシティ] の順に移動し、そこから別の Horizon Edge の追加を開始します。

[Horizon Edge を追加] ウィザードを開始する

1 環境に既存の Horizon Edge がない場合は [ようこそ] 画面から、または既存の Horizon Edge がある場合は [キャパシティ] ページから、コンソールの [Horizon Edge を追加] ウィザードを起動します。

コンソールには、手順 1 から開始する [Horizon Edge を追加] ウィザードが表示されます。



この時点で、ウィザードの手順は、Horizon 8 Edge のデプロイページに記載されている手順と同じです。

2 Horizon 8 Edge のデプロイページで説明されている手順に従って手順を完了します。

vSphere 環境に OVA をデプロイする際の重要なポイント

[OVF テンプレートのデプロイ] ツールを使用して OVA を環境にデプロイする場合は、次の重要な点に注意してください。これらの項目は、エンドツーエンドのデプロイを成功させるために重要です。

注： Horizon Edge Gateway OVA/OVF デプロイは、オールイン SDDC アーキテクチャまたはキャパシティ タイプのプライベート データセンターを使用する Horizon 8 プロバイダのみが使用できます。フェデレーション アーキテクチャを使用する Horizon 8 プロバイダの場合は、「Horizon Cloud Service - next-gen を使用した Horizon 8 フェデレーション デプロイの構成」で説明されている特定のキャパシティ タイプの手順を参照してください。

重要：

- [Horizon Edge Gateway のデプロイとペアリング] 手順に、[ペアリング コード] というラベルの付いたフィールドが表示されます。このペアリング コードは、エンドツーエンドのプロセスを成功させるために非常に重要です。アプライアンスを vSphere 環境にデプロイする場合は、このペアリング コードを [OVF テンプレートのデプロイ] ユーザー インターフェイス内で使用する必要があります。
- また、[OVF テンプレートのデプロイ] ユーザー インターフェイスでは、このコードに異なるラベル（[OVF テンプレートのデプロイ] ユーザー インターフェイスの [接続文字列]）が使用されていることに注意してください。
- ウィザードの手順からペアリング コードをコピーする場合は、コンソールにペアリング コードの文字列全体が表示されないため、コピー アイコンを使用する必要があります。コード文字列はコンソールに表示される文字列よりも長いので、表示されているテキストを強調表示してコピーするだけでは、完全なコード文字列を取得できません。
- [OVF テンプレートのデプロイ] ユーザー インターフェイスの [テンプレートのカスタマイズ] 手順で、[接続文字列] フィールドに、前の手順で [Horizon Edge を追加] ウィザードからコピーした [ペアリング コード] 文字列を入力する必要があります。
- 本書の執筆時点では、画面上のテキストは [接続文字列] フィールドがオプションであることを示している場合がありますが、ペアリング コードの入力は、Horizon Edge Gateway アプライアンスをデプロイするための重要な鍵であることに注意してください。

[OVF テンプレートのデプロイ] ユーザー インターフェイスを使用して Horizon Edge Gateway アプライアンスをデプロイする手順については、Tech Zone のビデオ「OVA からの Horizon Edge アプライアンスのデプロイ」を参照してください。

これらの重要なポイントを示す [OVF テンプレートのデプロイ] ユーザー インターフェイスのスクリーンショットについては、Horizon 8 Edge のデプロイのページを参照してください。

結果

すべてが成功すると、コンソールはウィザードのユーザー インターフェイスを閉じ、この新しく追加された Horizon Edge の詳細ページを表示します。

注： ネットワーク トラフィックによっては、詳細ページの接続ステータス インジケータの更新が完了するまでに 1 分かかる場合があります。

詳細ページの図については、Horizon Edge の詳細または Horizon 8 Edge のデプロイページの下部を参照してください。

後でこの Horizon Edge の詳細を編集または削除する場合は、[キャパシティ] ページに移動し、リストから Horizon Edge を選択して、適切なアクション（[編集] または [削除]）を使用します。

Horizon Edge リソースの可用性の監視 - Horizon Plus

Horizon Plus ライセンスをお持ちの場合、VMware® Horizon Availability Monitoring™ は、Horizon Edge リソースの健全性をテストするためにインストールおよび使用できるクライアントを提供します。このテストは、問題がより深刻になる前に迅速に検出して分離するのに役立ちます。たとえば、Horizon Availability Monitoring クライアントを使用して接続をテストし、VMware Horizon® Connection Server™、Active Directory、Horizon Gateway アプライアンス、デスクトップ、公開アプリケーションなどのさまざまなコンポーネントに対して、他のアクションを実行できます。

Horizon Availability Monitoring クライアントを構成したら、Horizon Universal Console を使用して、Horizon Edge 環境で健全性チェックを実行するテストを構成します。

注： Horizon Availability Monitoring 機能は、テナント内にある Horizon Edge にのみ適用されます。

Horizon Availability Monitoring プロセスの手順の概要は次のとおりです。

1 クライアント タイプを選択します。

- [インストール可能] クライアント タイプを選択して、クライアントの Horizon Universal Console へのペアリングを含む、独自の Windows システムで Horizon Availability Monitoring クライアントをダウンロード、インストール、および構成します。
- [クラウド] クライアント タイプを選択して、クラウドで Horizon Availability Monitoring クライアントを構成します。

2 Horizon Universal Console を使用して、Horizon Availability Monitoring クライアントから次のいずれかのタイプのテストを作成して実行します。

次のリストでは、各テストで Horizon Edge 環境へのアクセスを段階的に高める必要があります。そのため、より多くのアクセス関連情報を提供する必要があります。

注意： Horizon Availability Monitoring テストを含む一般的なテストのベスト プラクティスとして、認証情報（ユーザー名とパスワード）の入力を求められたら、通常のユーザー アカウントではなくテスト アカウントを使用します。

接続テスト

接続テストでクライアントと Unified Access Gateway アプライアンス間のネットワーク パスが検証されると、結果は正常になります。

接続テストは、Horizon Availability Monitoring クライアントから Unified Access Gateway アプライアンスに対して実行されます。

このテストの前提条件は次のとおりです。

- 接続テストのターゲットである Horizon Edge の URL があること。

  Horizon の場合、これは Horizon Client で使用される Horizon Connection Server URL です。

認証テスト

認証テストで Active Directory に対して認証を行い、Horizon Connection Server が実行状態であることを検証すると、結果は正常になります。

認証テストは、Horizon Availability Monitoring クライアントから、Horizon Edge 環境、Horizon Gateway アプライアンス(Unified Access Gateway および Horizon Edge Gateway)、および Horizon Connection Server に対して実行されます。

このテストの前提条件は次のとおりです。

- 接続テストのターゲットである Horizon Edge の URL があること。

  Horizon の場合、これは Horizon Client で使用される Horizon Connection Server URL です。

- この Horizon Availability Monitoring テストに使用するテスト アカウントの認証情報があること。

リソースの起動テスト

リソースの起動テストで選択したデスクトップまたは公開アプリケーションが起動されると、結果は正常になります。

リソースの起動テストは、Horizon Availability Monitoring クライアントから、Horizon Edge 環境、デスクトップまで実行されます。

このテストの前提条件は次のとおりです。

- 接続テストのターゲットである Horizon Edge の URL があること。

  Horizon の場合、これは Horizon Client で使用される Horizon Connection Server URL です。

- この Horizon Availability Monitoring テストに使用するテスト アカウントの認証情報があること。
- テストの一部として起動するデスクトップまたは公開アプリケーションの名前があること。

シミュレートされた起動

シミュレートされた起動では、Horizon Edge Gateway をターゲットとして使用し、実際のデスクトップやアプリケーションを使用せずにセッションの起動をシミュレートします。Edge のデプロイに組み込まれたシミュレートされたエージェント モジュールを使用して、デスクトップ接続パスをテストおよび監視できます。

シミュレートされた起動では、シミュレートされたクライアント、接続サービス、UAG、Edge モジュールを含むデスクトップ接続フローを検証します。

このテストの前提条件は次のとおりです。

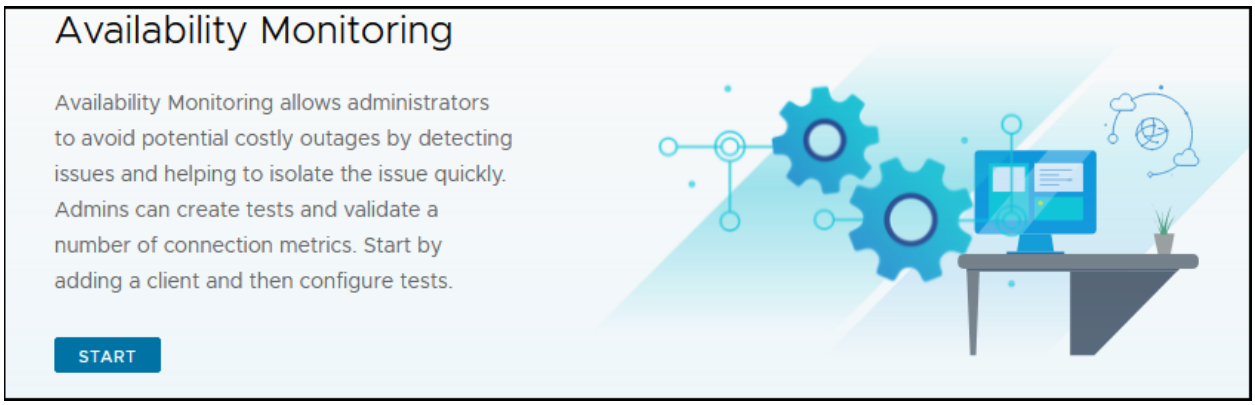
- Edge のキャパシティと UAG がデプロイされていること。

最初の Horizon Availability Monitoring テストの構成

Horizon Availability Monitoring のテストは、Horizon Universal Console の Horizon Availability Monitoring ページで構成します。最初の構成後、Horizon Availability Monitoring ページの外観が変わります。このトピックでは、最初のテストの構成を通じて、Horizon Availability Monitoring クライアントの初期構成について説明します。以降の構成では、手順は似ていますが、インターフェイスの外観が若干異なります。

注： Horizon Availability Monitoring 機能は、テナント内にある Horizon Edge にのみ適用されます。

Horizon Availability Monitoring ページにアクセスするには、[監視] - [可用性] を選択します。最初の Horizon Availability Monitoring テストを構成する前に、[可用性監視] ページが次のように表示されます。



次のタスクは、最初のテストを構成するために必要な手順を示しています。[可用性監視] ページは前の図のようになります。

前提条件

実行するテスト タイプに必要な情報を用意します。前述の [接続]、[認証]、[リソースの起動]、[シミュレートされた起動] の各テスト タイプの説明を参照してください。

手順

1 Horizon Universal Console を使用して、左側のメニューで [監視] - [可用性] を選択します。

2 [開始] をクリックします。

Horizon Availability Monitoring ウィザードが開きます。最初の手順は、Horizon Availability Monitoring クライアントを追加することです。

Horizon Availability Monitoring テストを初めて作成するには、1 つのクライアントと 1 つのテストを作成します。ウィザードを終了したら、追加のクライアントとテストを作成できます。

3 クライアント タイプ（[インストール可能] クライアント タイプまたは [クラウド] クライアント タイプ）のいずれかを選択して構成します。

インストール可能なクライアント タイプ

Windows システムのネットワーク上の場所にダウンロードしてインストールする必要があるクライアント。このタイプのクライアントは、デスクトップ ユーザーが配置されているのと同じネットワーク上の場所からテストをシミュレートする場合に最適です。

クラウド クライアント タイプ

クラウドで VMware によってホストされるクライアント。このタイプのクライアントは、デスクトップ ユーザーがインターネットからデスクトップにアクセスする場合に最適です。管理者は、エージェントをホストするマシンを維持する必要はありません。

- Windows システムで Horizon Availability Monitoring クライアントをダウンロード、インストール、および構成するには、次の手順を実行します。
  a [タイプの選択] オプションで [インストール可能] を選択します。
  b ブラウザでクライアント バンドル（Windows インストーラ パッケージの `.msi` ファイル）をダウンロードできるようにするには、[ダウンロード] をクリックします。
  c ペアリング コードの横にあるコピー アイコンをクリックして、コードをコピーします。
  d Windows インストーラ パッケージを、Horizon Availability Monitoring クライアントを実行する Windows システム上のフォルダに移動します。
  e Windows システムで、Windows インストーラ パッケージのインストールを開始して完了します。
    - よりわかりやすいクライアント名が必要な場合は、クライアントの名前を変更します。
    - プロンプトが表示されたら、適切なテキスト ボックスにペアリング コードを入力します。

      [可用性監視の開始] ページに、「ペアリングが完了しました」など、更新されたペアリング プロセスのステータスが表示されます。
  f [次へ] をクリックします。
- クラウドで Horizon Availability Monitoring クライアントを構成するには、次の手順を実行します。
  a [タイプの選択] オプションで [クラウド] を選択します。
  b [名前] テキスト ボックスにクライアントの名前を入力します。
  c [リージョン] ドロップダウン メニューからリージョンを選択します。

    [リージョン] ドロップダウン メニューには、環境内の利用可能なリージョンがすべて含まれます。

4 テスト タイプを選択して保存します。

前述の [接続]、[認証]、[リソースの起動]、[シミュレートされた起動] の各テスト タイプの説明を参照してください。

5 要求された情報を入力し、テストを保存します。

ページで要求される情報の量は構成するテスト タイプごとに異なり、[接続] テスト、[認証] テスト、[リソースの起動] テスト、[シミュレートされた起動] テストの順に多くなります。

すべてのテスト タイプに適用可能なプロンプト	説明
タイプ	実行するテスト タイプを選択します。
名前	テストの名前を作成します。
クライアント	テストを実行するクライアントを選択します。 最初のテストでは、このクライアントは Horizon Availability Monitoring ウィザードの最初の手順で追加したクライアントです。 今後クライアントを作成する場合は、クライアントを別のクライアントに変更するか、クライアントを追加して、このテストを構成できます。 **注：** 複数のクライアントが同じテストを使用できます。
間隔	テストを実行する頻度を選択します。 テストは、間隔を変更するか、テストを削除するまで、選択した間隔で継続的に実行されます。
URL	テスト ターゲットに使用される Horizon Edge の URL。

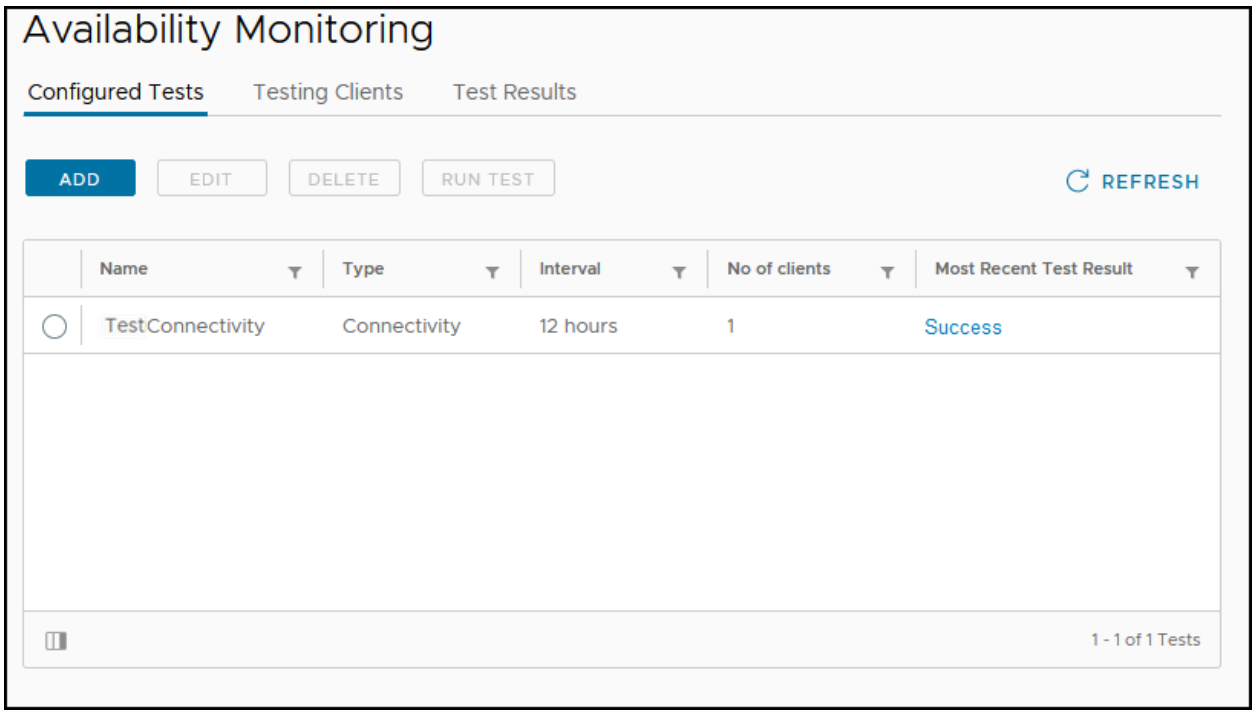
[認証] および [リソースの起動] テスト タイプに適用可能な追加プロンプト	説明
ユーザー名	この Horizon Availability Monitoring テストのテスト アカウントのユーザー名を入力します。
パスワード	この Horizon Availability Monitoring テストのテスト アカウントのパスワードを入力します。
ドメイン（オプション）	テスト ターゲットに使用される Horizon Edge のドメイン。

[リソースの起動] テスト タイプに適用可能な追加プロンプト	説明
プール名	起動するデスクトップまたはアプリケーションの名前を指定します。

[シミュレートされた起動] テスト タイプに適用可能な追加プロンプト	説明
Horizon Edge	HST テストのターゲットとして機能する Edge を選択します。
Unified Access Gateway のアドレス	Unified Access Gateway のアドレス。
SSL の検証	[SSL の検証] を切り替えます。このオプションをオンに切り替えると、テストはサーバ ID 証明書の有無と信頼性を検証します。

結果

[可用性監視] ページが更新された外観で再表示され、構成されたテスト、クライアント、および結果に関する情報が表示されます。この更新された外観が、今後のページで永続的に表示されます。



実行できる Horizon Availability Monitoring アクション

最初の Horizon Availability Monitoring テストを作成したら、[可用性監視] ページからいくつかの異なるアクションを実行できます。これにより、最終的に Horizon Availability Monitoring 機能を使用して、Horizon Edge 環境の健全性をテストできます。

次のアクションを実行できます。その多くは、最初の Horizon Availability Monitoring テストを構成する手順と同じか、似ています。最初の Horizon Availability Monitoring テストの構成を参照してください。

注： Horizon Availability Monitoring テストが失敗すると、[通知] ページに通知が表示されます。このページは、任意のページの右上隅にあるベル ( ) アイコンからアクセスできます。

アクション	説明
[可用性監視] ページで情報をフィルタリングする。	[可用性監視] ページの各タブから、列フィルタを使用して、ニーズに最適な方法で情報を表示できます。
構成済みのテストを追加、編集、削除、または実行する。	[可用性] - [構成済みのテスト] を選択して、次のいずれかのアクションを実行します。 ■ 別の Horizon Availability Monitoring テストを追加します。 ■ 既存の構成済みのテストを編集します。たとえば、クライアントの追加や変更、テスト間隔の変更を行います。テスト タイプに応じて、テスト アカウントの認証情報を変更したり、プール名を変更したりすることもできます。 ■ 既存の構成済みのテストを削除します。たとえば、テストが役に立たなくなった場合などです。 ■ 既存の構成済みのテストを手動で実行します。たとえば、次にスケジュール設定されたテストの実行を待つのではなく、今すぐテストを実行する場合などです。

アクション	説明
テスト用クライアントを追加、編集、または削除する。	[可用性] - [クライアントのテスト] を選択して、次のいずれかのアクションを実行します。 ■ 新しいテスト用クライアントを追加します。 「インストール可能」クライアント タイプの場合、新しいテスト用クライアントを別の Windows システムにのみ追加できます。 **注：** 特定のオペレーティング システムで、一度に 1 つの Horizon Availability Monitoring クライアントがサポートされます。 ■ 既存のテスト用クライアントを編集します。 「インストール可能」クライアント タイプで、クライアントをホストする Windows システムで障害が発生し、再インストールが必要な場合は、新しいクライアントをインストールして元のクライアント レコードと再ペアリングできます。 ■ 既存のテスト用クライアントを削除します。たとえば、クライアントが役に立たなくなった場合などです。
テスト結果を表示する。	[可用性] - [テスト結果] を選択して、テスト結果のリストを表示します。 このリストには、30 日間のテスト結果が含まれています。 ページでは、テスト結果のリストを表示できます。たとえば、成功したテストと失敗したテスト（ある場合）を表示できます。失敗したテスト タイプと失敗したタイミングを考慮して、失敗したテストのトラブルシューティングを行います。詳細については、前述のテスト タイプの情報を参照してください。

Splunk Enterprise を使用した Horizon 8 Edge の監視の構成

Horizon Plus ライセンスを持っている場合は、Splunk Enterprise 構成を 1 つ以上の Horizon 8 Edge と統合できます。その後、Splunk Enterprise を使用して、Horizon 8 Edge を監視できます。

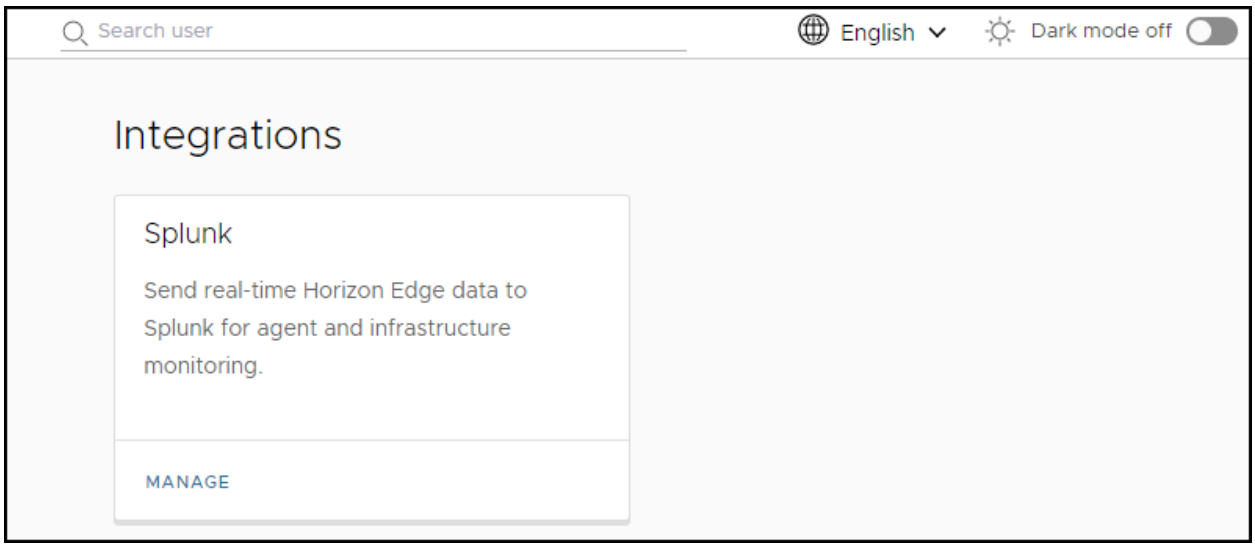
注目： この Horizon Cloud Service - next-gen 機能は、Horizon Plus ライセンスの Horizon 8 Edge Gateway のみを対象とします。

Horizon Plus ライセンスは、Workspace ONE Intelligence 監視オプションの代わりに Horizon 8 Edge の Splunk Enterprise 監視オプションをサポートします。

複数の Splunk Enterprise インスタンスを Horizon 8 Edge と統合できますが、Splunk Enterprise インスタンスは相互に通信する必要はありません。各 Splunk Enterprise インスタンスはハブとして機能しますが、同様に Horizon 8 Edge はスポークとして機能します。

したがって、単一の Splunk Enterprise インスタンスに複数の Horizon 8 Edge を割り当て、その Splunk インスタンスにデータを供給することができます。Horizon Edge と Splunk Enterprise インスタンス間の通信は、Horizon 8 Edge から Splunk Enterprise インスタンスへの一方向です。

Horizon Universal Console を使用して Splunk Enterprise 構成を追加、割り当て、または削除するには、ナビゲーション バーで [統合] をクリックして Splunk ページにアクセスし、[[Splunk] 統合] タイルで [管理] をクリックします。



Splunk Enterprise インスタンスの構成の追加

Splunk 構成を追加するには、Horizon Universal Console を使用します。

前提条件

Horizon Edge と統合する Splunk Enterprise インスタンスから次の情報を使用できるようにします。

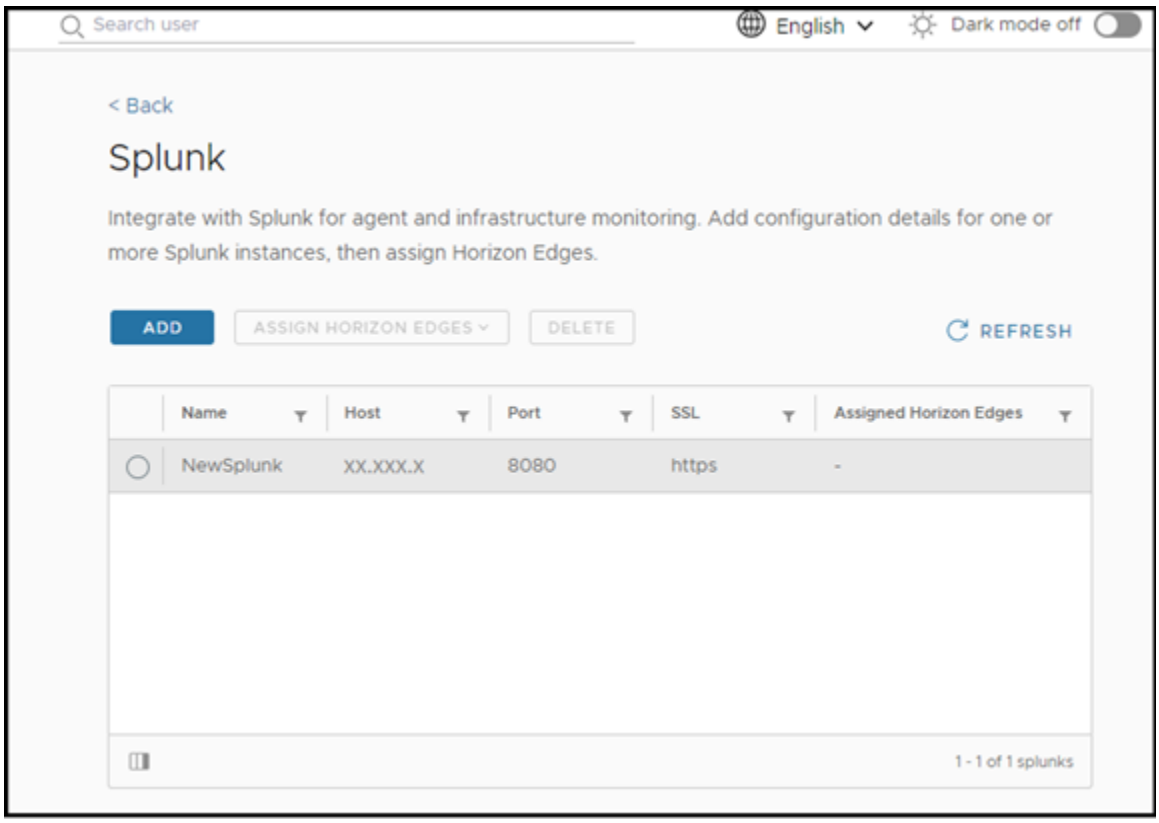
- Splunk Enterprise ホストの IP アドレス。
- Splunk Enterprise インスタンスのポート番号。
- Splunk Enterprise インスタンスからのシークレット トークン。

  統合の準備ができたら、Splunk Enterprise インスタンスからこのトークンをコピーできます。
- 自己署名証明書を使用することはお勧めしませんが、最終的に自己署名証明書として使用することを決定した場合は、その証明書をアップロードできるようにします。

手順

1 Splunk 統合タイルで [管理] をクリックします。

  [Splunk] ページが開きます。



2 既存の Splunk Enterprise インスタンスの構成情報を追加するには、[追加] をクリックします。

3 このタスクの前提条件として収集した情報を入力し、[保存] をクリックします。

Splunk Enterprise 構成への Horizon Edge の割り当て

Horizon Universal Console を使用して 1 つ以上の Splunk Enterprise 構成を追加したら、次の手順を実行して、Splunk Enterprise 構成に Horizon Edge を割り当てます。

手順

1 [Splunk] ページで、Splunk Enterprise 構成を選択します。

2 [Horizon Edge を割り当てる] - [追加] を選択します。

3 Splunk 構成に割り当てる 1 つ以上の Horizon Edge を選択し、[追加] をクリックします。

結果

これで、割り当てられた Horizon Edge が Splunk と統合されました。Splunk を使用して、割り当てられた Horizon Edge を監視できます。

割り当てられた Horizon Edge の [サマリ] ページで、同じ詳細の多くを見つけることができます。

Splunk Enterprise 構成からの Horizon Edge の割り当て解除

Splunk Enterprise 構成に Horizon Edge を割り当てると、その Horizon Edge の割り当てをいつでも解除できます。

手順

1 [Splunk] ページで、Splunk Enterprise 構成を選択します。

2 [Horizon Edge を割り当てる] - [削除] を選択します。

3 Splunk 構成から割り当てを解除する 1 つ以上の Horizon Edge を選択し、[削除] をクリックします。

Splunk Enterprise 構成の編集

Splunk Enterprise インスタンスからのシークレット トークン、SSL 証明書、ホスト IP アドレスなどの、Splunk Enterpirse インスタンスの構成情報を編集できます。

1 つ以上の Horizon Edge に割り当てられている Splunk Enterprise 構成を編集すると、その更新された構成は割り当てられた Horizon Edge およびデータベースに適用されます。

Horizon Edge に割り当てられていない Splunk Enterprise 構成を編集すると、Splunk Enterprise 構成はデータベースに対してのみ更新されます。

前提条件

次の 1 つまたは複数の、変更する情報を準備しておきます。

- Splunk Enterprise ホストの新しい IP アドレス。
- Splunk Enterprise インスタンスの新しいポート番号。
- Splunk Enterprise インスタンスからの新しいシークレット トークン。
- 新しい自己署名証明書のホスト上の場所。

手順

1 [統合] - [Splunk] ページで、編集する Splunk Enterprise 構成を選択します。

2 [編集] をクリックします。

3 更新する構成情報を変更し、[保存] をクリックします。

Splunk Enterprise 構成の削除

Splunk Enterprise 構成からすべての Horizon Edge の割り当てを解除した後、構成を削除できます。

手順

1 [Splunk] ページで、削除する Splunk Enterprise 構成を選択します。

2 [削除] をクリックします。

[削除の確認] ダイアログ ボックスが表示されます。

3 [削除] をクリックします。