

第1世代テナント - Horizon Cloud デプロイ ガイド

コンテンツは、2023年11月以降のサービスを反映しています。
VMware Horizon Cloud Service

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

Copyright © 2017-2024 Broadcom. All Rights Reserved. 「Broadcom」という語表現は、Broadcom Inc. およびその子会社のいずれかまたは両方を指します。詳細については、<https://www.broadcom.com> を参照してください。本書に記載されるすべての商標、製品名、サービス マークおよびロゴは、各社に帰属します。 [著作権および商標情報](#)。

目次

- 第 1 世代テナント - Horizon Cloud のポッドのデプロイとオンボーディング 6
- 1 第 1 世代テナント - Horizon Cloud および Horizon 制御プレーン サービスに関する情報 13**
 - 第 1 世代テナント - Horizon Cloud - 使用可能な環境、オペレーティング システムのサポート、VMware エコシステム内の緊密な連携、互換性情報、TLS プロトコルと暗号スイートのサポート 17
 - 第 1 世代テナント - Horizon Cloud - Windows 11 ゲスト OS のサポート - 考慮事項、既知の制限、および既知の問題 22
 - 第 1 世代テナント - 既存のクラウド接続ポッドを使用している現在のユーザー向け - Horizon Cloud Service リリースについて 23
 - 第 1 世代テナント - VMware Horizon Cloud Service on Microsoft Azure サービスの制限 52
 - 第 1 世代テナント - Horizon Cloud - Active Directory ドメイン構成 54
 - 第 1 世代 Horizon Cloud - 既知の制限事項 55
 - 第 1 世代テナント - Horizon Cloud - 既知の問題 61
- 2 第 1 世代テナント - Horizon テナントの基本的な概念 - クラウド サービス、制御プレーン、Horizon Universal Console、およびクラウド接続されたポッド 77**
- 3 第 1 世代テナント - 2023 年 11 月 2 日のサービス更新以降の新しいポッド デプロイに対する VMware Horizon Cloud Service on Microsoft Azure 要件チェックリスト 81**
- 4 第 1 世代の Horizon Cloud 制御プレーンを使用する VMware Horizon 8 ポッド - 要件チェックリスト - 2023 年 11 月 2 日のサービス更新に合わせて適切に更新されました 99**
- 5 第 1 世代テナント - Horizon ポッドをオンボーディングしてそのポッドで第 1 世代の Horizon 制御プレーン サービスを使用する 105**
 - 第 1 世代テナント - 第 1 世代 Horizon Cloud を使用した Horizon ポッドのデプロイ アーキテクチャ 107
 - 第 1 世代テナント - Horizon ポッドの第 1 世代の Horizon Cloud 制御プレーンへのオンボーディング 111
 - 第 1 世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件 115
 - 第 1 世代テナント - Horizon ポッドと Horizon Cloud Connector - 第 1 世代の制御プレーン サービスにオンボーディングする準備 122
 - Horizon Cloud Connector の既知の考慮事項 124
 - 第 1 世代テナント - 第 1 世代 Horizon Cloud Service を既存の Horizon ポッドに接続してクラウド ホスト型サービスを使用する 125
 - 第 1 世代テナント - Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイする 131
 - 第 1 世代テナント - Horizon ポッドと仮想アプライアンスの第 1 世代 Horizon 制御プレーンとのペアリングの準備ができていることを確認する 167
 - 第 1 世代テナント - Horizon Cloud Connector 構成ポータルを使用して Horizon ポッドと第 1 世代 Horizon Cloud のペアリングを完了する 168
 - Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector クラスタへのワーカー ノードの追加 178

6 第1世代 Horizon Cloud on Microsoft Azure のデプロイ - 主な特性 181

- 第1世代テナント - 事前検証のための簡素化された Horizon Cloud Service on Microsoft Azure ポッド環境の使用開始 187
- 第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - 概要レベルの手順 270
- 第1世代テナント - 第1世代 Horizon Cloud ポッドを Microsoft Azure にデプロイする前の準備 274
 - 第1世代テナント - Microsoft Azure の Horizon Cloud ポッドに対する Microsoft Azure 仮想マシンの要件 279
 - 第1世代 Horizon Cloud - Microsoft Azure での必要な仮想ネットワークの構成 288
 - 第1世代テナント - ポッドのデプロイの前に、Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成する 292
 - 第1世代テナント - Microsoft Azure で Horizon Cloud ポッド用に既存のサブネットを使用する場合 295
 - 第1世代テナント - Microsoft Azure の Horizon Cloud ポッドに使用する VNet トポロジに必要な DNS サーバの設定 297
 - 第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名 299
 - 第1世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件 329
 - 第1世代テナント - ポッドのサブスクリプションでの Horizon Cloud アプリケーション登録の作成 346
 - 第1世代テナント - 組織が第1世代 Horizon Cloud のアプリケーション登録にカスタム ロールを使用することを希望する場合 353
 - 第1世代テナント - Horizon Cloud ポッドのデプロイ ウィザードのためのサブスクリプション関連情報 369
 - 第1世代テナント - 第1世代 Horizon Cloud で Microsoft Azure サブスクリプションにおける状態が登録済みになっている必要があるリソース プロバイダ 370
 - 第1世代テナント - 第1世代 Horizon Cloud ポッドのデプロイに必要な PEM 形式への証明書ファイルの変換 371
- 第1世代テナント - Microsoft Azure へのポッドの自動デプロイを実行するための第1世代 Horizon Universal Console の使用 374
 - 第1世代テナント - 第1世代のポッド デプロイ ウィザードを実行するための前提条件 377
 - 第1世代テナント - ポッド マネージャ ベースのポッドをデプロイするためのポッド デプロイ ウィザードの起動 382
 - 第1世代テナント - 新しい Horizon Cloud ポッドの Microsoft Azure サブスクリプション情報の指定 385
 - 第1世代テナント - デプロイ ウィザードを使用して Microsoft Azure にデプロイする Horizon Cloud ポッドのポッド構成情報の指定 389
 - 第1世代テナント - Horizon Cloud ポッドのゲートウェイ構成の指定 395
 - 第1世代テナント - 検証と続行、およびポッドのデプロイ プロセスの開始 409
- 第1世代テナント - 第1世代 Horizon Cloud ポッドのデプロイまたは初めてのドメイン バインドで問題が発生した場合のトラブルシューティング 413
 - Horizon Cloud ポッドのデプロイのトラブルシューティング - SSH キー ペアを作成する 416
 - Microsoft Azure サブスクリプションにテスト用仮想マシンを作成する 419
 - SSH を使用してテスト用仮想マシンに接続する 421
 - Microsoft Azure 環境でネットワークを確認するためのテストを実行する 424
 - テストの完了後にテスト用仮想マシンを削除する 428

- 7 第1世代テナント - 最初のポッドのデプロイが完了し、第1世代 Horizon Cloud に接続されました 430
- 8 リビジョン履歴 - 変更ログ - Microsoft Azure および Horizon ポッドの Horizon Cloud へのオンボーディング 431

第 1 世代テナント - Horizon Cloud のポッドのデプロイとオンボーディング

このドキュメント ページとその内容は、VMware ナレッジベースの記事 KB92424 で説明する承認された例外がある場合にのみ適用されます。

重要： [KB92424](#) で説明されているように、第 1 世代の制御プレーンへのアクセスは提供終了 (EOA) となりました。

[KB92424](#) で説明するように、第 1 世代の制御プレーンにオンボーディングする承認された例外を受け取った場合にのみ、このドキュメント ページと「ポッドのデプロイとオンボーディング」のページ コレクションを使用します。

それ以外の場合は、Horizon Cloud Service - next-gen ドキュメントの[次世代のオンボーディング ドキュメント ページ](#)を使用する必要があります。

Horizon Plus サブスクリバ

このページも、「ポッドのデプロイとオンボーディング」のページ セットも使用しないでください。Horizon Plus サブスクリバの場合、Horizon Plus サブスクリプションでライセンス供与された機能を使用するには、これらの Horizon デプロイを次世代の制御プレーンにオンボーディングする必要があります。次世代の制御プレーンにオンボーディングして Horizon Edge のデプロイを開始する最初の手順について、このページの [Horizon Plus](#) に関する情報を参照してください。

第一世代のデプロイとポッドのオンボーディングの概要

ポッドのデプロイとオンボーディングのページ コレクションでは、最初のポッドを第 1 世代テナントにデプロイする前の Day-0 タスクと、最初のポッドをその第 1 世代テナントにオンボーディングする Day-1 タスクについて説明します。この特定のページは、このコレクションのエントリ ページとして機能します。

ヒント： 第 1 世代のテナントのポッド フリートにすでに少なくとも 1 つのクラウド接続されたポッドがある場合は、Day-2 操作に関する情報について、このオンボーディングのトピック セットの代わりに、関連する第 1 世代の [管理の一連のページ](#)を使用してください。

第 1 世代のクラウド プレーン ユーザー インターフェイスへの初期アクセス

重要： 次の内容は、オンボーディング ワークフローの一部として第 1 世代 Horizon Cloud 制御プレーンにアクセスする承認された例外がある場合にのみ適用されます。

新しい第1世代のテナント環境は、単一の Horizon Universal Console 画面とその画面内のクラウドホスト型ワークフロー アクションの小さなサブセットへのアクセスを提供します。次のスクリーンショットは、グリーンフィールド環境としてコンソールにアクセスした時点のコンソールを示しています。

ヒント: ログイン後、[全般的なセットアップ] バーをクリックして、次に示す主要なアクションを確認します。



第1世代ポッドをオンボーディングする前に、これらの主要なアクションは、この画面の行から使用できます。

[容量] セクション

第1世代のテナントとログインがライセンスとロールの要件を満たしている場合は、コンソールの [はじめに] ページで [無期限キーの表示] リンクを確認できます。



このリンクをクリックすると、テナントに関連付けられている基本的な VMware 製品の無期限キーを表示、コピー、および生成できるユーザー インターフェイス画面が表示されます。

Horizon Universal Console を使用したライセンス情報の取得では、テナントに関連付けられている可能性のある VMware 基本製品のキーを表示、コピー、および生成するための要件を確認できます。

[VMware SDDC] 行

[追加] をクリックして、Horizon Cloud Connector をダウンロードし、Horizon ポッドを第1世代の Horizon Cloud テナントに接続する方法を確認します。このタイプのポッドは、クラウドプレーン テナントに接続する前にデプロイしておく必要がある Connection Server ソフトウェアをベースとしています。この行から [追加] をクリックした後、画面に表示されている [ダウンロード] リンクに従ってください。これらの手順

は、[Horizon ポッドをオンボーディングする場合のワークフローの概要](#)に記載されています。これらの手順により、前提条件、DNS およびポートの要件、および後続の手順に関する情報へのリンクが得られるため、現時点で最もスムーズに操作を進めることができます。

 VMware SDDC, 0 ポッド 完了していません	VMware SDDC ベースのプラットフォーム上の Horizon ポッドをパブリッククラウドまたはプライベート データセンターにデプロイまたは接続します。
--	---

[Microsoft Azure] 行

Microsoft Azure のサブスクリプションへの Horizon Cloud ポッドのデプロイを自動化する自動ウィザードを起動します。これらのポッドは VMware Horizon Cloud のポッドマネージャ テクノロジーをベースとしています。

 Microsoft Azure®, 0 ポッド 完了していません	<input type="button" value="管理"/>
---	-----------------------------------

[全般的なセットアップ] セクション - My VMware アカウント


Horizon Cloud Connector のオンボーディングおよび構成ポータル、および Horizon Universal Console (テナント環境へのポータル)にログインする権限を付与する管理者の最初のセットを追加します。最初のライセンス購入者のアカウントがデフォルトで事前入力されています。その結果、その行には緑色のチェック マークが付けられていることがわかります。ただしこれは、テナント環境の作成時にテナント アカウントに関連付けられた最初のアカウントが常に1つあるからのみです。

ヒント: ユーザーが会社や組織を離れる場合など、何らかの理由で最初の購入者のアカウントが非アクティブになったために第1世代のテナント環境、Horizon Cloud Connector オンボーディングおよび構成ポータルからロックアウトされるのを防ぐため、最初のポッドがオンボーディングされる前でも、[Horizon Service へようこそ] E メールを受信したらすぐに最初の管理者セットを追加することを推奨します。最初の購入者が組織の Horizon デプロイの管理者でない場合は、管理者となる少なくとも1人のユーザーは、VMware Customer Connect アカウントを新しいサービス テナント アカウントに対して許可するようサポートに要求する必要があります。許可されると、そのユーザーはログインし、この [My VMware アカウント] の行を使用してさらに管理者を追加できます。この要求を行うには、[ナレッジベースの記事 KB2006985](#)に記載されている手順を使用して、技術以外のサポート リクエストを発行します。

 My VMware アカウント	最初の MyVMware アカウントを作成し、より多くのユーザーにアクセスを許可します。	<input type="button" value="追加"/>
---	--	-----------------------------------

[全般的なセットアップ] セクション - Cloud Monitoring Service (CMS)

[全般的なセットアップ] セクションで、必要な Cloud Monitoring Service (CMS) の設定を確認します。CMS はデフォルトで有効になっているため、緑色のチェック マークが付いた行が表示されます。この時点で、ポッドをオンボーディングする前でも、その機能を無効にすることができます。



完了しました

Cloud Monitoring Service

監視とレポートの目的で、セッション、アプリケーション、およびデスクトップデータを収集して保存します。

ヒント: 上記の4つのアクションのほかに、ポータル以外のアクションとワークフローにアクセスするには、オンボーディングされたポッドがあり、そのポッドがオンラインで、クラウド管理プレーンと通信し、テナント環境に Active Directory ドメインが登録されている必要があります。コンソールは、Active Directory ドメイン登録ワークフローが完了するまで、他の管理アクションへのアクセスをブロックします。このワークフローの詳細については、[Horizon Cloud 環境での最初の Active Directory ドメイン登録の実行](#)を参照してください。

バナー - VMware Cloud Services のエンゲージメント プラットフォームへのオンボーディング

Horizon Cloud のテナント レコードが、VMware Cloud Services エンゲージメント プラットフォームにオンボーディングするオプションを使用して構成されていて、テナントが VMware Cloud Services の組織にまだ関連付けられていない場合、ウィンドウの上部に青いバナーが表示され、そのオンボーディング プロセスを有効にする方法を提供します。次のスクリーンショットは、テナント レコードがこれらの条件を満たしている場合の表示を示しています。

VMware Cloud Services プラットフォームをオンボーディングして、さらに多くの機能を利用可能にします。

このプロセスの詳細については、[Horizon Cloud テナントを VMware Cloud Services にオンボーディングする](#)を参照してください。Horizon Cloud タイルをクリックして Workspace ONE 環境からこのポータルにアクセスしている場合、青いバナーは表示されません。テナント レコードがプラットフォームにオンボーディングするオプションを使用して構成されていない場合、青いバナーは表示されません。

第1世代のオンボーディング要件チェックリスト

最初の第1世代ポッド オンボーディングが Horizon ポッド デプロイの場合に、第1世代のクラウドベースのサービスを使用する

4章 第1世代の Horizon Cloud 制御プレーンを使用する VMware Horizon 8 ポッド - 要件チェックリスト - 2023年11月2日のサービス更新に合わせて適切に更新されましたの項目を確認します。このページでは、第1世代の Horizon 8 を使用して Horizon Cloud Connector ポッドをクラウド プレーンに正常に接続するために必要なさまざまな前提条件の要素について説明します。

最初の第1世代ポッドのオンボーディングが第1世代の Horizon Cloud on Microsoft Azure デプロイである場合

3章 第1世代テナント - 2023年11月2日のサービス更新以降の新しいポッド デプロイに対する VMware Horizon Cloud Service on Microsoft Azure 要件チェックリストの項目を確認します。このページでは、第1世代の Horizon Cloud ポッド デプロイ ウィザードを開始する前に必要となるさまざまな前提条件の要素について説明します。

これらのオンボーディング トピックのリビジョン履歴

このドキュメントのトピック セットは、製品がリリースされるたびに、あるいは必要に応じて更新されます。これまでに行われた大幅な改訂のセットについては、[8 章 リビジョン履歴 - 変更ログ - Microsoft Azure](#) および [Horizon ポッドの Horizon Cloud へのオンボーディング](#)を参照してください。

対象読者

このドキュメントは、以下の領域の知識がある経験豊富なデータセンター管理者を対象としています。

- VMware Horizon および VMware Horizon Connection Server
- VMware Horizon Cloud Connector
- VMware Unified Access Gateway™
- VMware Workspace ONE® Access™
- 仮想化テクノロジー
- ネットワーク
- VMware Cloud™ on AWS および Amazon Web Services EC2 (AWS EC2)
- Microsoft Azure、およびその Marketplace
- Azure VMware Solution (AVS)
- Google Cloud Platform (GCP) および Google Cloud VMware Engine (GCVE)


Horizon Cloud コミュニティ

以下のコミュニティを使用して質問をしたり、その他のユーザーからの質問への回答を検索したり、役に立つ情報へのリンクにアクセスしたりすることができます。

- <https://communities.vmware.com/community/vmtn/horizon-cloud-service> にある VMware Horizon Cloud Service コミュニティ
- <https://communities.vmware.com/community/vmtn/horizon-cloud-service/horizon-cloud-on-azure> にある VMware Horizon Cloud on Microsoft Azure サブコミュニティ (VMware Horizon Cloud Service コミュニティのサブコミュニティ)。

VMware サポートへのお問い合わせ

第1世代の Horizon Cloud 環境でなにかお困りの場合は、VMware のサポートにお問い合わせください。

- VMware Customer Connect アカウントを使用して、オンラインで VMware サポートにサポート リクエストを発行するか、お電話でお問い合わせください。
- [KB 2144012](#) カスタマ サポートのガイドライン から、発生した問題に応じてサポートを受ける方法が参照できます。
- コンソールにおいて、 - [サポート] をクリックすると、[KB 2144012](#) へのリンクも表示されます。

これらの First-Gen デプロイ ガイド ページで使用される選択したポッド関連の用語

第1世代の Horizon Cloud のドキュメント ページ全体にわたり、以下の語句が見られます。これらの語句には、次のような意味があります。

Horizon ポッド

Horizon Connection Server ソフトウェアと関連ソフトウェア コンポーネントを使用して構築されたポッド。Horizon Connection Server コンポーネントは、VMware がこのようなポッドの使用をサポートするインフラストラクチャで動作しています。Horizon ポッドには、通常、VMware SDDC (Software-Defined Data Center) が必要です。VMware SDDC の例としては、オンプレミスの vSphere 環境、VMware Cloud on AWS、Google Cloud VMware Engine (GCVE)、Azure VMware Solution (AVS) などがあります。

Horizon Cloud ポッド、Microsoft Azure 上の Horizon Cloud ポッド

Microsoft Azure サブスクリプションへのデプロイを自動化する第1世代の Horizon Cloud のポッド デプロイ ウィザードを実行して構成されるポッド。このタイプのポッドは第1世代の VMware Horizon Cloud ポッド マネージャ テクノロジーをベースとしており、Microsoft Azure でのみ実行できます。

注： Microsoft Azure 上の Horizon ポッドは、Azure VMware Solution (AVS) 上の Horizon ポッドとは別個のエンティティです。これら 2 つは完全に異なるテクノロジーに基づいています。1 つは Horizon Connection Server テクノロジーに基づいており、もう 1 つは Horizon Cloud ポッド マネージャ テクノロジーに基づいています。

コネクション ブローカ

コネクション ブローカーは、エンドユーザー クライアントを仮想デスクトップ仮想マシンまたはファーム仮想マシンに接続し、各エンドユーザーのクライアントと、接続した仮想マシンで実行されているエージェント間で接続セッションを設定します。英語のブローカ (名詞) には、一般的に、取引について交渉する人という意味があるため、この「ブローカ」(名詞) という言葉を使用しています。

デスクトップ仮想化ソフトウェアのユースケースでは、コネクション ブローカがエンドユーザーのクライアント要求を受信し、仮想デスクトップ仮想マシンまたはファーム仮想マシンとの接続を確立します。次に、コネクション ブローカは要求を適切にルーティングし、いずれか 1 台の仮想マシンで実行されているエージェントとそのエンドユーザー クライアント間の接続セッションをネゴシエートします。このネゴシエーションでは、ポッドプロビジョニングされ、エンド ユーザーが接続資格を付与されているリソースのタイプが考慮されます。

第1世代の Horizon 制御プレーン サービスの 1 つが Universal Broker サービスです。Universal Broker はマルチテナントのクラウドベース サービスであり、複数のポッドにまたがるリソースの仲介を可能にし、ユーザーとポッドの地理的サイトに基づいて仲介の決定を行います。

Horizon ポッドの Connection Server または Horizon Cloud ポッドのポッド マネージャ仮想マシンは、エンドユーザー クライアントからクライアントの接続要求を満たすポッド内のリソースへのルーティングを容易にするコンポーネントです。

スクリーンショットについて

スクリーンショットは通常次のようになっています。

- ユーザー インターフェイス画面全体の一部のみを表示し、必ずしもユーザー インターフェイス全体を表示することはありません。表示されている部分は、通常、その部分を説明するドキュメント テキストに対応していません。
- データの匿名性を維持するため、適宜ぼかしを入れています。
- PDF 形式では、幅が 6 インチを超えるスクリーンショット イメージは自動的にサイズ変更されます。その結果、そのようなイメージは PDF 形式でぼやけて表示されることがあります。パラレル HTML ページで画像をフルサイズで表示するには、スクリーンショットをクリックしてみてください。

注：一部のスクリーンショットは高解像度で取得しています。このため、PDF を 100% で表示したときに、読みにくい場合があります。このような画像は、200% に拡大すると明瞭になり、読みやすくなります。

VMware の技術ドキュメントの用語集

VMware の技術ドキュメントには、専門的な用語などを集約した用語集があります。VMware の技術ドキュメントで使用されている用語の定義については、<http://www.vmware.com/support/pubs> をご覧ください。

第 1 世代テナント - Horizon Cloud および Horizon 制御プレーン サービス に関する情報

1

第 1 世代 Horizon Cloud または第 1 世代 Horizon 制御プレーン サービスを使用する準備をするとき、ポッドのオンボーディング中、および日常操作中は、次の情報とリンク先の記事を使用してください。

重要： この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。KB-92424 で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

セットアップの前提条件、ソフトウェアのダウンロード、ユーザー設定のパーシステンス、製品ドキュメント、追加の役立つリソース

セットアップの前提条件

Microsoft Azure 環境で、デプロイを開始する前にセットアップの前提条件を確認してください。

- [VMware Horizon Cloud Service on Microsoft Azure 要件チェックリスト](#)
- [第 1 世代テナント - 第 1 世代 Horizon Cloud ポッドを Microsoft Azure にデプロイする前の準備](#)

ライセンス サービスを含むクラウドプレーン サービスの Horizon ポッドをオンボーディングする場合は、ポッドが使用しているデプロイ アーキテクチャのタイプの説明とオンボーディングのガイダンスを確認します。次の場所にある情報を参照してください。

- [5 章 第 1 世代テナント - Horizon ポッドをオンボーディングしてそのポッドで第 1 世代の Horizon 制御プレーン サービスを使用する - Horizon ポッドをクラウド プレーンにオンボーディングします。](#)
- VMware Digital Workspace Tech Zone の「[Horizon Reference Architecture](#)」ページ。
techzone.vmware.com/search#browser にアクセスし、[Horizon] - [Reference Architecture] を選択します。次に、使用するデプロイ プラットフォームを選択します。
- ポッドの Connection Server ソフトウェア バージョンに従ったインストールおよびリリース ノートのドキュメント：
 - [バージョン 7.13 - Horizon 7 のドキュメント](#)で入手できます。
 - [VMware Horizon 8 バージョン - Horizon のドキュメント](#)で入手できます。

ソフトウェアのダウンロード

環境で使用するソフトウェアのダウンロードを VMware Customer Connect で確認します。これらのダウンロードは特定のデプロイを開始する前のオプションですが、ユースケース シナリオによっては、デプロイの前

に確認することができます。[VMware Horizon Cloud Service のダウンロード ページ](#)を参照し、最新のサービス リリース日を見つけて、そのダウンロード リンクに移動します。同じページ内に Horizon Cloud Connector の行が表示され、[ダウンロードに移動] をクリックすると、Horizon Cloud Connector と VMware Universal Broker プラグイン インストーラの両方の最新バージョンを入手できます。どのバージョンの VMware Universal Broker プラグイン インストーラがどの Horizon Connection Server に使用できるかについては、[Horizon ポッド - Connection Server への Universal Broker プラグインのインストール](#)ピックアップ内の表を参照してください。

ユーザー設定のパーシステンス

すべての Microsoft Azure のデプロイで、フォルダ リダイレクト機能を備えた VMware Dynamic Environment Manager™ を使用して、ユーザー プロファイルのパーシステンスを提供できます。「[VMware Horizon Cloud Service のダウンロード ページ](#)」を参照して、このリリースのダウンロード リンクに進み、このリリースでの使用がサポートされている Dynamic Environment Manager ソフトウェアをダウンロードできます。

製品ドキュメントと追加の役立つリソース

さまざまなデプロイ モデルについてのすべての製品ドキュメントにアクセスするには、[VMware Horizon Cloud Service のドキュメントの Web サイト](#)を参照してください。

役に立つヒントを参照したり質問をしたりする場合は[コミュニティ サイト](#)にアクセスしてください。[Horizon Cloud の製品ページのリソース セクション](#)でテクニカル ペーパーも入手できます。

Day-0 の役に立つ情報

デプロイ タイプを実行する前に

- Horizon Cloud 環境が Workspace ONE 環境と統合されていない場合、クラウドベースのコンソールへのログイン認証は VMware Cloud services プラットフォームでのアカウント認証情報の認証に依存します。そのサービスが必要な認証要求を完了できない場合、コンソールへのログインは失敗します。コンソールの最初のログイン画面でログインの問題が発生する場合は、VMware Workspace ONE ステータス ページ (<https://status.workspace.com>) で最新のシステム ステータスを確認してください。そのページでは、アップデートを定期受信にすることもできます。
- コンソールのポッド デプロイヤー ウィザードを使用してポッドをデプロイする場合、および Horizon Cloud Connector を使用して Horizon ポッドを接続する場合は、特定の DNS 名にアクセス可能で、特定のポートとプロトコルが許可されている必要があります。接続要件については、[第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件](#)、[第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件](#)、DNS 名、および[第1世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件](#)を参照してください。
- Horizon Cloud 制御プレーンにペアリングされ、同じユーザー アカウントに関連付けられている各ポッドは、それらのポッドに接続された Active Directory ドメインへの線を持っていて、その線に沿って一方向

または双方向の信頼関係を設定している必要があります。たとえば、3つのポッドがあり、そのうちの1つは Microsoft Azure 内に、1つはオンプレミスに、もう1つは VMware Cloud on AWS 内にある場合、これらのポッドのそれぞれが線を持ち、同じ Active Directory ドメインのセットに対して一方向または双方向の信頼関係を設定している必要があります。

Microsoft Azure のデプロイの前に

- サブスクリプションとポッドの数：Microsoft Azure サブスクリプションに展開するポッド数については、特に大規模に各ポッドを実行させる予定がある場合は、十分に考慮しておいてください。複数のポッドを1つの Microsoft Azure サブスクリプションにデプロイできますが、すべてを1つのリージョンにデプロイしても、複数のリージョンにわたりデプロイしても、Microsoft Azure では1つのサブスクリプション内で一定の制限がかかります。このような Microsoft Azure の制限が原因で、多数のポッドを1つのサブスクリプションにデプロイすると、それらの制限に到達する可能性が高くなります。それらの制限に関わるのは、ポッドの数、各ポッド内のファームと割り当ての数、各ポッド内のサーバの数、各割り当て内のデスクトップの数などの多くの変数、およびそれらの変数の組み合わせです。大規模にポッドを実行する予定がある場合は、複数のサブスクリプションを1つの Microsoft Azure アカウントで利用する方法を採用することを検討してください。Microsoft Azure のユーザーは、この方法を使用する方が、サブスクリプションの進行中の管理に対していくつかのメリットを得られるため、都合がよい可能性があります。この方法を使用すると、サブスクリプションあたり1つのポッドを展開し、それらのサブスクリプションを1つの「プライマリ アカウント」にロールアップして、1つのサブスクリプションに対して適用される Microsoft Azure の制限に達する可能性を排除します。
- デプロイのポッド マネージャ仮想マシンで使用される Microsoft Azure 仮想ネットワーク (VNet) では、アウトバウンド インターネット アクセスが必要です。プロキシベースの認証は、Horizon Cloud on Microsoft Azure デプロイでサポートされます。ポッドのデプロイ ウィザードでプロキシの詳細を指定する必要があります。ポッドのデプロイでは、特定の DNS 名にアクセス可能で、特定のポートとプロトコルが許可されている必要があります。接続要件については、[第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名を参照してください](#)。
- サブネットのサイズ：ポッドのデプロイ後に、ポッドのサブネットのサイズを拡張することは現在サポートされていません。このため、本番環境では、次の要件に十分対応できるサブネットサイズを使用する必要があります。
 - 管理サブネット：ポッドをデプロイする場合、2019年3月の時点では、ポッドの管理サブネットには最小で CIDR /27 が必要です。以前のリリースでは最小でこれより低い CIDR /28 が許可されていました。この変更は、サブネット内に使用可能な IP アドレスがないためにポッドのアップデート中に発生する可能性がある問題の発生を低減する目的で行われました。/27 の CIDR では、32 個の IP アドレスが提供されます。
 - 仮想マシン サブネット - プライマリ：予測される VDI デスクトップ、RDS イメージ、およびポッドの RDS ファーム内のすべての仮想マシンの接続に対応できる十分な範囲の CIDR を使用します。ポッド マネージャ仮想マシンと Unified Access Gateway 仮想マシンも、このサブネットからの IP アドレスを必要とします（合計 12 のアドレスを使用して、両方のタイプのゲートウェイを備えた HA 対応ポッドのブルー/グリーン更新に対応します）。一般的に、/24 ~ /21 の範囲は典型的なユースケースを提供します。注：この仮想マシン サブネットは、デスクトップ サブネットまたはテナント サブネットと呼ばれることもあります。

- 2020年7月のサービスリリースとポッド マニフェスト 2298.0以降、VDI デスクトップと RDS ファーム仮想マシンに追加のテナント サブネットを使用するための新機能が提供されます。これらの追加のサブネットは、ポッドと同じ VNet またはピアリングされた VNet に含めることができます。マニフェスト 2298.0 以降のポッドでは、ポッドの構成を編集して、追加のサブネットを含めることができます。その後、プライマリの仮想マシン サブネットを使用するのではなく、ファームおよび VDI デスクトップ割り当ての定義でこれらの追加のテナント サブネットを使用するように指定できます。ファーム仮想マシンおよび VDI デスクトップ仮想マシンにこれらのセカンダリ サブネットを使用すると、どのテナント サブネットおよび VNet にどのファームおよび VDI デスクトップを割り当てるかを指定できるため、管理が簡素化されます。
- 外部ゲートウェイを独自の VNet にデプロイする機能を使用するには、VNet をピアリングする必要があります。そのため、デプロイ ウィザードを実行する前に、サブネットを手動で作成する必要があります。外部ゲートウェイの VNet の場合、その管理サブネットとバックエンド サブネットはそれぞれ、同じ最低限の CIDR/27 に準拠する必要があります。

Horizon Cloud Connector を使用してポッドを接続する前に

- 新しいデプロイでは、VMware Customer Connect で入手可能で、ポッドの Horizon Connection Server ソフトウェア バージョンと互換性のある最新バージョンの Horizon Cloud Connector をダウンロードして使用する必要があります。最新バージョンを使用すると、最新の修正と改善が提供されます。Horizon Cloud Connector と Horizon Connection Server の互換性マトリックスについては、[VMware 製品の相互運用性マトリックス](#)にアクセスし、[VMware Horizon Cloud Connector] と [VMware Horizon] としてリストされている 2 つのソリューション名の相互運用性を確認してください。
- Horizon Cloud Connector でサービスのクラウド プレーンと通信するには、特にライセンスの詳細を受け取るために、アウトバウンド インターネット アクセスが必要です。特定の DNS 名にアクセス可能で、特定のポートとプロトコルが許可されている必要があります。接続要件については、[第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件](#)を参照してください。
- Horizon Cloud Connector のオンボーディング プロセスを使用して最初の Horizon ポッドを接続した後、第2の Horizon ポッドを Horizon Cloud に接続する前に、Horizon Cloud 管理コンソールにログインして Active Directory ドメイン登録プロセスを完了する必要があります。Active Directory ドメイン登録を完了する前に複数の Horizon ポッドを Horizon Cloud とペアリングすると、コンソールにログインしてドメイン登録プロセスを試みたときに予期しない結果が発生することがあります。
- 既知の問題により、オンプレミスの Active Directory ドメインを使用して VMware Cloud on AWS でポッドにサービスを実行している場合、オンプレミスの Active Directory ドメインと VMware Cloud on AWS のポッド間のネットワークの遅延またはネットワークの輻輳が原因でアクセス時間が遅くなり、ドメインの呼び出しがタイムアウトになることがあります。通常、この遅延には、Active Directory ログイン画面でタイムアウトになる前にログインを完了できない場合が含まれます。このような状況が発生した場合は、各クラウドのソフトウェア定義データセンター (SDDC) で書き込み可能ドメイン コントローラを構成すると役立つことがあります。

一部のサービスの運用 E メールについて

2021 年 4 月のサービス リリース以降、指定された VMware 顧客アカウントの担当者に関連付けられているすべての顧客レコードについて、システムの運用 E メールの一部には、デフォルトで、指定された VMware 顧客アカウントの担当者のメール アドレスが BCC フィールドに含まれます。これらの Eメールの BCC フィールドに VMware 顧客アカウントの担当者を含める目的は、オンボーディングとビジネス継続性を向上させることです。

BCC フィールドに VMware 顧客アカウントの担当者が含まれる運用 E メールは次のとおりです。

- サービスの顧客レコードの最初の作成時に、顧客名とメール アドレスは新しく作成された顧客レコードに所有者として指定されます。その所有者 顧客名に関連付けられているメール アドレスに「ようこそ」Eメールが送信されます。
- その所有者に関連する更新が発生すると（メール アドレスの更新など）、通知 Eメールが送信されます。
- 顧客レコードの Horizon ライセンスに関連する更新が発生すると、通知 Eメールが送信されます。

次のトピックを参照してください。

- [第 1 世代テナント - Horizon Cloud - 使用可能な環境、オペレーティング システムのサポート、VMware エコシステム内の緊密な連携、互換性情報、TLS プロトコルと暗号スイートのサポート](#)
- [第 1 世代テナント - Horizon Cloud - Windows 11 ゲスト OS のサポート - 考慮事項、既知の制限、および既知の問題](#)
- [第 1 世代テナント - 既存のクラウド接続ポッドを使用している現在のユーザー向け - Horizon Cloud Service リリースについて](#)
- [第 1 世代テナント - VMware Horizon Cloud Service on Microsoft Azure サービスの制限](#)
- [第 1 世代テナント - Horizon Cloud - Active Directory ドメイン構成](#)
- [第 1 世代 Horizon Cloud - 既知の制限事項](#)
- [第 1 世代テナント - Horizon Cloud - 既知の問題](#)

第 1 世代テナント - Horizon Cloud - 使用可能な環境、オペレーティング システムのサポート、VMware エコシステム内の緊密な連携、互換性情報、TLS プロトコルと暗号スイートのサポート

このドキュメントのトピックでは、第 1 世代 Horizon Cloud と一緒に使用できる環境とオペレーティング システムについて説明します。また、このトピックでは、Horizon Cloud と VMware エコシステムとの緊密な連携についても説明し、VMware の相互運用性マトリックスへの便利なポイントについても取り上げます。

重要： この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

Microsoft Azure クラウド環境

Microsoft Azure デプロイに対して、このサービスは現在、次の Microsoft Azure クラウド環境で利用できます。

- Microsoft Azure (商用)
- Microsoft Azure (中国)
- Microsoft Azure Germany (公開)
- Microsoft Azure Government (バージニア州政府、アリゾナ州政府、テキサス州政府)

サポートされる Microsoft Windows オペレーティング システム

サービスの Microsoft Azure 環境では、Azure Marketplace における次の Microsoft Windows オペレーティング システムのエディションおよびバージョンは、本リリースでのイメージのデプロイ方法が自動か手動にかかわらず、本リリースでの使用がサポートされています。

- サポートされている Windows 10 または 11 以外のオペレーティング システムについては、[VMware ナレッジベースの記事 KB78170](#) を参照してください。
- サポートされている Windows 10 または Windows 11 オペレーティング システムについては、[VMware ナレッジベースの記事 KB70965](#) を参照してください。

サービスの Windows 11 のサポートには、現在既知の考慮事項、制限事項、および問題があります。これらの詳細については、[Windows 11 ゲスト OS のサポート - 考慮事項、既知の制限、および既知の問題](#)を参照してください。

VMware エコシステム内の緊密な連携

幅広い VMware エコシステムから入手可能な次の製品とともに、Horizon Cloud を使用することができます。

VMware Carbon Black

VMware Carbon Black Cloud 間の統合と、Horizon Cloud ポッドによってプロビジョニングされたファームおよび VDI デスクトップでの VMware Carbon Black センサーの使用については、[VMware Carbon Black と Horizon Cloud Service on Microsoft Azure の相互運用性 \(KB81253\)](#) を参照してください。

VMware Workspace ONE® Hub サービスと VMware Workspace ONE® Access™ クラウド

この統合によって、VMware Horizon® Service Universal Broker™ を使用して仲介されたデスクトップとリモート アプリケーションの割り当ては、VMware Workspace ONE® Intelligent Hub カタログに自動的に同期して、エンド ユーザーが表示および起動するために Hub を介して使用できるようになります。現在のリリースでは、この統合はブラウザベースの Hub カタログ、Workspace ONE Intelligent Hub for Windows、および Workspace ONE Intelligent Hub for macOS のクライアントを使用したエンドユーザー アクセスをサポートします。このサポートに必要な Windows および macOS デスクトップ アプリケーションの最小バージョンは 21.05 です。

VMware Workspace ONE® UEM

Workspace ONE UEM を使用して、Horizon Cloud ポッドによってプロビジョニングされた Microsoft Windows 10 専用 VDI デスクトップを管理できます。詳細については、[VMware Workspace ONE UEM のドキュメント](#)を参照してください。

VMware Workspace ONE® Assist™ for Horizon®

Workspace ONE Assist for Horizon を使用すると、Horizon Cloud 管理者は、Horizon Universal Console にあるヘルプ デスク ツールから直接リモート サポート セッションを起動できます。この製品を使用すると、管理者はリモート表示および制御機能を活用して、仮想デスクトップについて従業員を支援できます。詳細については、[VMware Workspace ONE Assist のドキュメント](#)を参照してください。

注： Workspace ONE Assist for Horizon との統合には、関連する VDI デスクトップからのアウトバウンド通信のための追加の DNS、ポート、およびプロトコル要件が含まれます。詳細については、[VMware Workspace ONE Assist のドキュメント](#)を参照してください。

VMware NSX-T™ Data Center

Horizon Cloud on Microsoft Azure バージョンと NSX-T Data Center バージョン間の互換性は、最新バージョンの Horizon Cloud Service on Microsoft Azure の [VMware 製品の相互運用性マトリックス](#)で利用できます。Horizon Cloud ドキュメントは、マトリックスで互換性があると表示されているバージョンに従って、最新の構成手順を反映しています。

ポッドでバージョン 2010 より前の Horizon Cloud Service on Microsoft Azure バージョンのマニフェストが実行されている状態で、そのようなポッドで NSX-T Data Center 2.4 または 2.5 を使用するようすでに構成している場合、構成は引き続き動作します。ただし、Horizon Cloud システムがこれらのポッドを更新する必要があるとコンソールに表示する場合は、これらのポッドを更新する必要があります。

VMware NSX® Advanced Load Balancer™

Horizon Cloud は、Microsoft Azure の Horizon Cloud ポッドのゲートウェイ構成で NSX Advanced Load Balancer の使用をサポートします。NSX Advanced Load Balancer は、VMware の一部となった、Avi Networks の Avi Vantage ロード バランシング機能を提供します。リファレンス設計、一連の手順、および適用可能な構成情報は、[Azure 環境での Horizon Cloud の UAG のロード バランシング](#)というタイトルの Avi Networks の記事に記載されています。

注： Horizon Cloud ポッドとのこの統合のいくつかの側面では、全体的な構成を完了するために VMware Horizon Cloud Service チームの支援が必要になる可能性があります。この統合を開始する前に最新情報を取得するには、[Customer Connect でサポート リクエストを発行する方法 \(VMware KB 2006985\)](#)の説明に従って、Horizon Cloud Service チームにサービス リクエスト (SR) を発行してください。

VMware Horizon® Client™ 製品ライン

クラウド接続されたポッド フリート内のポッドによって仲介されるデスクトップおよびリモート アプリケーションと互換性のある Horizon Client 製品ラインの特定のバージョンを確認するには、[VMware 製品の相互運用性マトリックス](#)を参照してください。ポッドのタイプに応じて、ドロップダウン メニューで Horizon Cloud Service on Microsoft Azure または VMware Horizon を選択し、VMware Horizon Client を選択します。

一般的に、さまざまな種類の Horizon Client と VMware Horizon HTML Access クライアントで、使用事例ごとに同じ機能やプロトコルのセットが必ずしもサポートされているとは限りません。このドキュメントが執筆されている時点では、次のようなバリエーションがあります。

- VMware Horizon HTML Access クライアントは、モバイル ブラウザで使用すると、一部の機能がサポートされなくなります。また、出荷状態の Horizon Client がクライアントのローカル システムと仮想マシンの間でテキストのコピー アンド ペーストをサポートしていても、Web クライアントの場合は、エンドユーザーがこの機能を使用するために、機能の構成が必要になります。
- VMware Horizon Client for Mac には、RDP プロトコルを使用するメニュー オプションはありません。
- Horizon Client は、RDSH アプリケーションでの RDP プロトコルの使用をサポートしていません。

Horizon Client と Horizon Cloud Service on Microsoft Azure の間でサポートされる機能のマトリックスをダウンロードするには、[VMware ナレッジベースの記事: Horizon Cloud on Azure の Horizon Client 機能のマトリックス \(80386\)](#)を参照してください。現時点では、マトリックスの情報は、最善の努力で最新の状態に保持されています。

注：

- VDI セッションのゲスト OS 内でディスプレイの解像度などのディスプレイ設定を変更することは、公式にはサポートされていません。VMware のベスト プラクティスは、Horizon Client の機能を使用して、リモート デスクトップのディスプレイの解像度とスケーリングをカスタマイズすることです。たとえば、Horizon Windows クライアントの場合、このページでは[クライアントを使用してディスプレイの解像度とスケーリングをカスタマイズする方法](#)について説明します。
- Microsoft Azure の Horizon Cloud ポッドでのゼロ クライアントの使用はサポートされていません。
- Universal Broker でのゼロ クライアントの使用はサポートされていません。

オペレーティング システム固有の Horizon Client を使用して、Universal Broker によって仲介されたりリモート リソースにアクセスする場合、次のクライアント バージョンがサポートされます。クライアントで使用するための Universal Broker の接続 FQDN をエンド ユーザーに提供する必要があります。その接続 FQDN を構成する方法については、[Universal Broker 設定の構成](#)を参照してください。

- オペレーティング システムの場合は Horizon Client 5.4 以降。
- Windows ユーザーは、Horizon Client for Windows 5.3 以降を実行できます。

エンド ユーザーは、Horizon HTML Access を使用して Web ブラウザから Universal Broker サービスに接続することもできます。次の場合、Web ベースのクライアントを使用している場合、エンド ユーザーが仲介されたデスクトップを起動すると、標準ブラウザの「安全でない」というメッセージが表示されます。

- ポッドの Unified Access Gateway セットアップのロード バランサが、ロード バランサの名前と正確に一致する共通名を持たないか、既知の認証局 (CA) によって署名されていない SSL 証明書で構成されている場合。
- ポッドに外部 Unified Access Gateway があるが、内部 Unified Access Gateway セットアップがなく、エンド ユーザーのアクセスが内部ネットワークを介している場合。
- ポッドに Unified Access Gateway セットアップがまったくない場合。

(証明書の共通名と、証明書のインストール先のホスト名との関係の詳細については、<https://support.dnsimple.com/articles/what-is-common-name/> を参照してください)。

VMware Horizon® ポッド

Horizon ポッドは、Horizon Connection Server ソフトウェアに基づいて構築されたポッド タイプです。Horizon Cloud Connector を使用して、これらのポッドを Horizon Cloud に接続します。Horizon Cloud Connector の新しいデプロイは、バージョン N、N-1、N-2 を使用してサポートされます。N は、一般公開された最新の Horizon Cloud Connector バージョンです。一般公開された最新の Horizon Cloud Connector バージョンのバージョン番号は、[Horizon Cloud Service リリース ノート ドキュメント](#)の上部に表示されます。

Horizon Cloud Connector の N、N-1、N-2 バージョンに対応する Horizon ポッド ソフトウェアのマトリックスについては、[VMware 製品の相互運用性マトリックス](#)を参照してください。クラウドに接続された Horizon ポッドでのみ使用可能な高度な機能のメリットを活用するには、デプロイで Horizon Cloud Connector および Horizon ポッド ソフトウェアの最新バージョンを使用する必要があります。[VMware Horizon Cloud Service ダウンロード ページ](#)内にある Horizon Cloud Connector セクションに移動して、最新の Horizon Cloud Connector アプライアンスと VMware Universal Broker プラグイン インストーラをダウンロードできます。

注： 2021年1月以降、1.6.x より前のバージョンの Horizon Cloud Connector はクラウド制御プレーンに接続できなくなります。2020年の後半に、以前のバージョンに基づいてデプロイされた既存のすべてのテナントにはコネクタを更新するように通知が送信されました。

他の VMware 製品との互換性

この製品と他の VMware 製品との互換性に関する最新情報については、[VMware 製品の相互運用性マトリックス](#)を参照してください。

IPv6 の使用について

Horizon Cloud は IPv6 の使用をサポートしていません。

TLS プロトコルと暗号スイート

Horizon Cloud Service は、次の TLS プロトコルと暗号スイートをサポートします。

- TLS 1.3 128 ビット TLS_AES_128_GCM_SHA256
- TLS 1.3 256 ビット TLS_AES_256_GCM_SHA384
- TLS 1.2 128 ビット TLS_ECDHE_RSA_AES128_GCM_SHA256
- TLS 1.2 256 ビット TLS_ECDHE_RSA_AES256_GCM_SHA384

Horizon Cloud Service on Microsoft Azure のデプロイに固有

- Microsoft Azure 上の Horizon Cloud ポッドのデプロイでは、TLS 1.2 は、ポッドのストレージ アカウントとサービスの提供の一部としてデプロイされる Azure PostgreSQL サービスの両方の最小 TLS バ

ーションとして設定されます。これらのストレージ アカウントと Azure PostgreSQL サービスは、ポッド マネージャ インスタンスなどのサービス コンポーネントでのみ使用されます。このため、ポッドによる TLS 1.2 の使用が、Microsoft Azure サブスクリプションの顧客管理のアーティファクトに影響することはありません。

- デフォルトでは、Horizon Cloud ポッドの Unified Access Gateway アプライアンスをデプロイするためのウィザード ユーザー インターフェイスは、それらのアプライアンスに次の TLS プロトコルと暗号スイートを構成します。
 - TLS v1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS v1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

デプロイ ウィザードのユーザー インターフェイスの詳細については、「[Horizon Cloud ポッドのゲートウェイ構成の指定](#)」を参照してください。デプロイ ウィザードのユーザー インターフェイスまたは Horizon Universal Console を使用して、ポッドの Unified Access Gateway アプライアンスで他の TLS プロトコルと暗号スイートを構成する機能は、現在使用できません。

対応ブラウザ

クラウドベースの管理コンソールは、Google Chrome、Mozilla Firefox、Microsoft Edge の最新バージョンに対応しています。Microsoft Internet Explorer 11 でのコンソールの使用は非推奨であり、最適なエクスペリエンスは提供されません。Apple Safari でのコンソールの使用はサポートされていません。ただし、Apple Safari で使用してみることはできます。Microsoft Internet Explorer 11 などの最新でないブラウザを使用してコンソールにアクセスしようとすると、最新のブラウザの使用を求める情報メッセージがコンソールに表示されます。最高のユーザー エクスペリエンスを実現するには、Google Chrome、Mozilla Firefox、および Microsoft Edge の最新バージョンを使用してください。

第1世代テナント - Horizon Cloud - Windows 11 ゲスト OS のサポート - 考慮事項、既知の制限、および既知の問題

第1世代 Horizon Cloud Service で Windows 11 ゲスト OS を使用する場合は、次の考慮事項、制限事項、および問題が確認されています。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

考慮事項

- ポッドは v2204 リリース以降のマニフェストを実行している必要があります。
- ゴールド イメージは、Horizon Agents Installer v22.1.0 以降を実行している必要があります。

- Gen 1/Gen 2 および Windows 10/Windows 11 のサポート マトリックス。

Azure 仮想マシン モデル	Windows 10	Windows 11
Gen 1 仮想マシン	サポートされています	サポート対象外
Gen 2 仮想マシン	サポート対象外	サポートされています

制限事項

- コンソールベースの App Volumes アプリケーション キャプチャ ワークフローは現在サポートされていません。Windows 11 VDI デスクトップで Azure の App Volumes を使用するには、Windows 10 ゴールド イメージを使用してコンソールベースのキャプチャ ワークフローを実行し、アプリケーションをキャプチャします。次に、それらのアプリケーションをユーザーに割り当てて、Windows 11 ベースのデスクトップで使用します。
- Windows 11 イメージを手動でインポートするには、直接ソースとして Azure Marketplace からインポートする必要があります。共有イメージ ギャラリー (SIG)、Azure 管理対象イメージ、Azure 仮想マシン スナップショットなど、その他のソースからのインポートは現在サポートされていません。
- vTPM は現在サポートされていません。
- AMD ドライバを実行している仮想マシンで Windows 11 を使用することは、現在サポートされていません。

既知の問題

- GPO を使用してタイム ゾーン リダイレクトを有効にすると、デスクトップのちらつきと、エクスプローラ プロセスのクラッシュが発生します。詳細は、[KB88086](#) を参照してください。

既知の問題を回避するには、Windows 11 マルチセッション仮想マシンのタイム ゾーン同期 GPO を有効にしないようにします。

第1世代テナント - 既存のクラウド接続ポッドを使用している現在のユーザー向け - Horizon Cloud Service リリースについて

このページの情報は、第1世代 Horizon Cloud Service のリリース ノートの「新機能」と併せて使用してください。

注意: ナレッジベースの記事 [KB92424](#) で説明されているように、第1世代の Horizon Cloud 制御プレーンの提供終了が発表されました。この発表に合わせて、第1世代の Horizon Cloud 製品ドキュメントが更新されました。

この内容の紹介

注目: この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

2022 年 8 月の時点で、Horizon Cloud Service - next-gen は一般公開され、独自の『Horizon 制御プレーン next-gen の使用』ガイドを入手できます。

次世代と第 1 世代のどちらの環境を使用しているかは、環境にログインし、Horizon Universal Console ラベルに表示されるブラウザの URL フィールドのパターンで確認することができます。次世代環境の場合、コンソールの URL アドレスには /hcsadmin/ のような部分が含まれます。第 1 世代コンソールの URL の場合は、異なるセクション (/horizonadmin/) があります。

リリース ノート ドキュメントにリストされている項目に加えて、このページは、直近のサービス更新日以前にすでにクラウドに接続された既存のポッドを環境にオンボーディングしているか、以前に Horizon Cloud の機能およびワークフローを使用した経験がある方を対象としています。このページでは、ユーザーおよびそれらのポッドにとって今回の新機能と変更点を持つ重要性について説明します。機能とワークフローの重要な変更のみが記載されています。管理コンソールの新しいレイアウトや配色などの軽微な変更はワークフローに大幅な変更をもたらすことはないため、ここでは詳しく説明しません。

第 1 世代サービスの直近のサービス更新日は、サービスの [リリース ノート ドキュメント](#) に記載されています。Horizon Cloud テナント環境で実行されるさまざまなワークフローに関する最新情報を表示するには、[Horizon Cloud Service ドキュメント ページ](#) からリンクされている個々のガイドに記載されているドキュメントのトピックを参照してください。

次のセクションは 2019 年 9 月に戻ります。以前のリリースについて、同様の情報を公開することはできません。

重要: このページで使用されている用語を理解するうえで重要な情報については、このページの情報を読む前に、[リリース ノートのドキュメント](#) に記載されている情報を参照してください。リリース ノート ドキュメントには、Microsoft Azure にデプロイされるポッドの最新のポッド マニフェスト番号など、重要な関連情報が含まれています。また、次のセクションで説明する重要な事実はすべての Horizon Cloud リリースに当てはまることに注意してください。

すべての Horizon Cloud リリースに関する重要な事実

- ポッドのマニフェスト バージョン レベル、Horizon Cloud Connector のバージョン レベル、Horizon ポッドのバージョン レベル、または制御プレーンの地域の違いに依存しない、クラウド プレーン ベースのすべての新しい機能は、既存ユーザーと新規ユーザーの両方に自動的に提供されます。一例として、以下に特に記載されていない、または製品ガイドに記載されていない限り、クラウド プレーンからポッドへの API 呼び出し用の新しい API に依存しない、または Horizon Cloud Connector に関連する新しいユーザー インターフェイス機能は、既存のユーザーに表示され、利用できます。
- VMware Horizon Cloud Service チームは、継続的かつ定期的に、そして暦年の任意の週に、ポッドのマニフェスト バージョン レベルや Horizon Cloud Connector バージョン レベル、または Horizon ポッド バージョン レベルに依存しない、新しいクラウド プレーン ベースの機能を公開します。[リリース ノートのドキュメント](#) には、これらの機能の公開日が含まれています。

- そのマニフェスト バージョンがクラウド制御プレーンで初めて使用された日から、ポッドを Microsoft Azure にデプロイするためのポッド デプロイヤは、常に最新のポッド マニフェスト バージョンでポッドをデプロイします。
- 新しいポッド マニフェスト バージョンがクラウド プレーンで初めて使用される前にサービス テナントに存在するデプロイ済みのポッドは、リリースの新しいマニフェストに更新されるまで、既存のマニフェスト バージョンで実行され続けます。次の事実が当てはまります。
 - 最新のマニフェスト レベルを必要とする API への依存度がゼロの新しいサービス機能は、これらの既存のポッドで利用できます。
 - 最新のマニフェスト レベルの API に依存する新しいサービス機能は、それらのポッドが更新されるまで既存のポッドでは利用できません。
 - 一部の新しいサービス機能は、テナント アカウントが配置されているクラウド プレーンのリージョンに依存する場合があります。これらの機能については、該当するドキュメントに記載されています。制御プレーンの地域は、ユーザー アカウントが作成されたときに送信される「Horizon Service へようこそ」E メールに記載されています。[Microsoft Azure および Horizon ポッドの Horizon Cloud へのデプロイとオンボーディング](#)を参照してください。
- コンソールの [Marketplace からの仮想マシンのインポート] ウィザードは、ポッド マニフェストに組み込まれている Horizon Agents Installer (HAI) を使用します。その結果、最新のマニフェスト バージョンでデプロイされたポッドには最新の HAI が組み込まれ、[仮想マシンのインポート] ウィザードを実行して最新レベルでポッドを選択すると、その最新の HAI からエージェントがインストールされます。最新のマニフェスト レベルにまだ更新されていないポッドの場合、[Marketplace からの仮想マシンのインポート] ウィザードは、それぞれのポッド マニフェストがビルトされたときに提供されていた HAI バージョンを使用します。
- 当該ポッドでのサブスクリプション ライセンスの使用のアクティベーションと、Horizon Cloud が Horizon ポッドに提供するクラウドホスト型サービスの使用の有効化という 2 つの主なユースケースでは、Horizon ポッドが Horizon Cloud にオンボーディングされています。各ポッドは Horizon Cloud Connector を使用してオンボーディングされます。これらのユースケースは、Horizon ポッドでのサブスクリプション ライセンスのアクティベーションのために、Horizon 7 バージョン 7.6 環境と Horizon Cloud Connector 1.0 で初登場しました。その後、新しいバージョンの Horizon Connection Server をそれぞれ新しいバージョンの Horizon Cloud Connector と組み合わせることにより、Horizon Connection Server の最新バージョンを Horizon Cloud Connector の最新バージョンと組み合わせて実行しているクラウド接続された Horizon ポッドで追加のクラウドホスト型サービスを利用できるようになります。Horizon Cloud Connector の新しいデプロイは、バージョン N、N-1、N-2 を使用してサポートされます。N は、Horizon Cloud Connector の最新バージョンです。N-2 バージョンよりも前のバージョンの Horizon Cloud Connector を使用しているデプロイでは、新機能およびセキュリティと回復性の修正を活用するために、最新バージョンに更新することをお勧めします。Horizon Cloud Connector の最新の N バージョンについては、[リリース ノート ドキュメント](#)の上部を参照してください。また、Horizon Cloud Connector で現在サポートされているバージョンの Horizon ポッド ソフトウェアについては、[VMware 製品の相互運用性マトリックス](#)を参照してください。マトリックスに一致しなくなった Horizon Connection Server と Horizon Cloud Connector のバージョンの組み合わせを実行している場合は、サポートされている組み合わせに更新してください。

2023年11月 - v2310

2023年4月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、v2310 リリースのリリースノートに記載されている機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

次のキー バイナリの新しいバージョンが 2023 年 11 月に初登場しました。

Horizon Cloud on Microsoft Azure デプロイの修正とセキュリティ アップデートを含む新しいポッド マニフェスト バージョンと、更新されたエージェントを含む新しいバージョンの Horizon Agents Installer (HAI)。

2023年11月2日

- [VMware ナレッジベースの記事 KB92424](#) で説明されているように、第1世代 Horizon Cloud 制御プレーンの提供終了 (EOA) が発表されました。第1世代 Horizon Cloud Service のドキュメントのポッド デプロイ コンテンツは、そのナレッジベースの記事に合わせて更新されています。
- [VMware ナレッジベースの記事 KB93762](#) で説明されているように、Horizon インフラストラクチャの監視機能は廃止されました。この廃止およびナレッジベースの記事の情報に合わせて、この機能に関連するコンテンツは第1世代 Horizon Cloud Service のドキュメントから削除されました。

2023年7月3日

「[VMware ナレッジベースの記事 KB91183](#)」で説明されているように、VMware Workspace ONE Intelligence for Horizon は、サブスクリプション ライセンス VMware Horizon Universal、Horizon Apps Universal、Horizon Apps Standard を持つ第1世代の Horizon Cloud テナントで使用できます。この可用性により、ナレッジベースの記事には次の情報が記載されています。

- 第1世代コンソールが提供していた履歴ダッシュボードとレポートは、Workspace ONE Intelligence を通じて利用できるようになります。
- 2023年6月30日時点で、これらの履歴ダッシュボードとレポートは第1世代コンソールでは使用できなくなりました。
- これらの変更により、コンソールの更新に合わせて、『管理ガイド』の「[Horizon Universal Console の \[レポート\] ページ](#)」、「[Horizon Cloud ダッシュボード - ポッド フリートおよびテナント環境の健全性の可視性および洞察](#)」、「[Horizon Cloud - ユーザー カード機能 \(別称: ヘルプ デスク\) について](#)」、「[Horizon Universal Console で提供される Cloud Monitoring Service の統合された可視性および洞察、健全性監視、およびヘルプ デスク機能の紹介](#)」の各ページが更新されています。
- 第1世代テナントでユーザー セッション データの監視が無効になっている場合、使用率、傾向、および履歴の分析に関連するレポートは無効になり、Workspace ONE Intelligence では使用できなくなりました。監視が無効になっている場合、システムはリアルタイムの管理を可能にするためにそのようなユーザー セッション情報を限られた期間で収集し、ユーザー名をハッシュします。その間、そのユーザー情報の履歴および集計の表示は無効になります。その結果、セッション レポートなど、そのデータの履歴および集計を表示するレポートは利用できなくなりました。テナントでこの監視が無効になっているかどうかを確認するには、[設定] - [全般設定] - [監視] のコンソール設定に移動します。

詳細については、「[Digital Employee Experience for Horizon](#)」、[「Horizon Cloud First-Gen の統合」](#)、および「[Intelligence レポートの Horizon Cloud データへのアクセス](#)」を参照してください。

2023 年 5 月

2023 年 5 月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2023 年 5 月のリリース ノートに記載されている機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

要求別有効化の機能の有効化を要求するには、[VMware ナレッジベースの記事 KB2006985](#)に記載されているように、サポート リクエストを発行します。

次のキー バイナリの新しいバージョンが 2023 年 5 月に初登場しました。

Horizon Cloud Connector の新しいバージョン。

Horizon Cloud Connector v2.4 の新機能

- Horizon Cloud Connector で構成された Horizon Connection Server 認証情報を変更できるようになりました。[登録済みの Active Directory 認証情報を更新する](#)を参照してください。
- SSL オフロードが送信トラフィック用に構成されている場合に、Horizon Cloud Connector で証明書を構成して、制御プレーンへの接続を許可できるようになりました。[カスタムの CA 署名証明書の構成](#)を参照してください。
- アプライアンスは、証明書の有効期限に達する前に、Kubernetes クラスタ証明書を自動的に更新します。また、有効期限までの残り日数もユーザー インターフェイスに表示されます。[Kubernetes クラスタ証明書の警告とシステムの自動更新への対応](#)を参照してください。

2023 年 4 月 - v2303

2023 年 4 月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2023 年 4 月および v2303 リリースのリリース ノートに記載されている機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

要求別有効化の機能の有効化を要求するには、[VMware ナレッジベースの記事 KB2006985](#)に記載されているように、サポート リクエストを発行します。

次のキー バイナリの新しいバージョンが 2023 年 4 月に初登場しました。

Horizon Cloud on Microsoft Azure 環境用の新しいポッド マニフェスト バージョン、および Horizon Agents Installer (HAI) の新しいバージョン。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- マニフェスト バージョン 4136 以降のポッドでは、[インポートされた仮想マシン] ページの [インポート] ウィザードを使用する場合、および [イメージ - マルチポッド] ページを使用してマルチポッド イメージを

公開する場合、エージェント オプションで Skype for Business のオプションが提供されなくなりました。[Horizon Agent for Windows v2303 の新機能](#)で説明されているように、VMware Virtualization Pack for Skype for Business と呼ばれる機能は、v2303 Horizon Agent 以降ではサポートされなくなりました。

イメージに関連する新しい項目

サポートが追加された Windows ゲスト OS は次のとおりです。

- Windows 10 Enterprise 22H2
- Windows 10 Enterprise マルチセッション 22H2
- Windows 11 Enterprise 22H2
- Windows 11 Enterprise マルチセッション 22H2
- Windows Server 2022 データセンター

2022 年 10 月 - v2210

2022 年 10 月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2022 年 10 月および v2210 リリースの[リリース ノート](#)に記載されている機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

要求別有効化の機能の有効化を要求するには、[VMware ナレッジベースの記事 KB2006985](#)に記載されているように、サポート リクエストを発行します。

次のキー バイナリの新しいバージョンが 2022 年 10 月に初登場しました。

Horizon Cloud on Microsoft Azure 環境用の新しいポッド マニフェスト バージョン、Horizon Cloud Connector の新しいバージョン、および Horizon Agents Installer (HAI) の新しいバージョン。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- 管理者は、ゲートウェイ デプロイの Unified Access Gateway インスタンスで NTP 設定を構成して、ポッド マネージャ インスタンスで使用される NTP 設定を継承できるようになりました。このリリースより前にテナントに存在していたゲートウェイ構成を持つポッドの場合、[ポッドを編集] ワークフローを使用してこの機能を使用し、Unified Access Gateway インスタンスがポッド マネージャ インスタンスで使用される NTP 設定を継承するようにすることができます。
- API の問題により、Horizon Cloud Service on Microsoft Azure デプロイの Unified Access Gateway インスタンスに Syslog サーバを構成する v2201 コンソールの機能は、API の問題が解決されるまでオフになっています。Horizon Universal Console でこの機能がオフにされていると同時に、機能がコンソールに戻るまで、この機能への参照も Horizon Cloud Service のドキュメントから削除されています。

イメージ管理サービス (IMS) に関連する新しい項目

Horizon 8 2209 以降の Horizon ポッドのデプロイの場合、ゴールド イメージの管理方法に応じて、プールとファーム内のゴールド イメージとスナップショット ソースを vCenter Server からイメージ カタログへ、またはその逆に変更できます。この新機能を利用するには、VMware Horizon Console の操作を使用して既

存のプールとファームの編集およびインスタント クローンのメンテナンスを行い、関連するソース エンティティを変更します。

- [自動化されたフル クローン デスクトップ プールの作成と管理](#)
- [インスタント クローン ファームのメンテナンス](#)
- [インスタント クローン デスクトップ プールのメンテナンス](#)

Universal Broker および Horizon ポッドに関連する新しい項目

- Unified Access Gateway バージョン 2209 で Unified Access Gateway 管理コンソールが機能強化されたため、Horizon 環境でそのバージョンを使用するときに、JWT 設定のユーザー インターフェイス ラベルがわずかに変更されます。関連するドキュメント ページ [Horizon ポッド - Universal Broker で使用するための Unified Access Gateway の構成](#)が更新され、デプロイに Unified Access Gateway バージョン 2209 以降が含まれる場合の適切な要素についての説明が追加されました。

2022 年 8 月 - v2207

2022 年 8 月および v2207 リリースよりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2022 年 8 月のリリース ノートに記載されている機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

要求別有効化の機能の有効化を要求するには、[VMware ナレッジベースの記事 KB2006985](#)に記載されているように、サポート リクエストを発行します。

次のキー バイナリの新しいバージョンが v2207 で初登場しました。

Horizon Cloud on Microsoft Azure 環境および Horizon Agents Installer (HAI) 用の新しいポッド マニフェスト バージョン。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- 管理者は、クライアントが Unified Access Gateway マシンに接続したときに受け入れられる暗号スイートを構成できるようになりました。このリリースより前にテナントに存在していたゲートウェイ構成のポッドの場合は、ポッドの詳細ページを使用して、これらのゲートウェイ構成で構成された暗号スイートを確認します。[ポッドの編集] ワークフローを使用して、構成された暗号スイートを変更できます。
- アップグレードのメンテナンス中は、Unified Access Gateway セッション数を使用してタイミングを最適化し、エンドユーザー セッションの中断を減らします。
- ジャンプ ボックスとも呼ばれる一時的なポッド デプロイ エンジン、新しい Horizon Cloud on Microsoft Azure 環境と更新のアーキテクチャから削除されました。一時的なジャンプ ボックスのキャパシティが必要になるのは、ユーザーがサポート リクエストを開いて、VMware のサポートでそのリクエストに対応する方法がサポート関連のジャンプ ボックス仮想マシンをその監督下でデプロイすることであると判断した場合のみです。
- Microsoft Azure Cloud による今後の一部の仮想マシン モデルの廃止による影響を回避し、GPU 対応の仮想マシンのインポートにより適切に対応し、シングルポッドおよびマルチポッド イメージのインポートのための仮想マシン モデルを標準化するために、v2207 リリース以降、サービスの自動化された [Marketplace からの仮想マシンのインポート] ウィザードでデフォルトで使用される仮想マシン モデルが変更されました。

ウィザードは、シングルポッド イメージとマルチポッド イメージの両方に示されている次のモデルを使用するようになりました。ポッドの Azure サブスクリプションで仮想マシン ファミリの割り当てを確認し、ウィザードを使用して作成する予定のイメージに対して使用可能な割り当てがあることを確認することをお勧めします。

[Marketplace からの仮想マシンのインポート] ウィザードで以下が作成されます。

- 非 GPU、Windows 11 以外、Standard_DS2_v2 仮想マシン
- 非 GPU、Windows 11 使用、Standard_D4s_v3 仮想マシン
- GPU 対応、Standard_NV12s_v3 仮想マシン

その他の注意事項

- すべてのサブスクリプションには、Horizon Universal Console を使用して追加できる Workspace ONE Access テナントが含まれているため、Horizon Universal Console 内から新しい Workspace ONE Access テナントを作成できます。この変更は、VMware のビジネス運用に対応しています。

2022 年 5 月 - v2204

2022 年 5 月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2022 年 5 月のリリース ノートに記載されている機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

要求別有効化の機能の有効化を要求するには、[VMware ナレッジベースの記事 KB2006985](#)に記載されているように、サポート リクエストを発行します。

次のキー バイナリの新しいバージョンが v2204 で初登場しました。

Horizon Cloud on Microsoft Azure 環境用の新しいポッド マニフェスト バージョン、Horizon Cloud Connector、Universal Broker プラグイン インストーラ、および Horizon Agents Installer (HAI) の新しいバージョン。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- Windows 11 は、Horizon Cloud on Microsoft Azure 環境で使用するゲスト OS としてサポートされるようになりました。サービスで Windows 11 を使用する場合の既知の考慮事項、制限事項、および問題については、[Windows 11 ゲスト OS のサポート - 考慮事項、既知の制限、および既知の問題](#)ページを参照してください。この機能を使用するには、ポッドがこのリリースのマニフェスト以降を実行している必要があります。

この Windows 11 のサポートに関連するいくつかの追加ポイント：

- 手動のインポート方法を使用して Windows 11 の仮想マシンをインポートする場合は、エージェントのインストールに Horizon Agents Installer (HAI) バージョン 22.1 以降が使用されていることを確認する必要があります。Windows 11 のサポートには、HAI v22.1 によって提供される最小エージェント バージョンが必要です。

- Windows 11 ゴールド イメージを使用したコンソールの App Volumes キャプチャ ワークフローの使用は、現在サポートされていません。回避策として、Windows 10 ゴールド イメージを使用してパッケージをキャプチャし、それらのパッケージをエンド ユーザーに割り当てて、割り当てられた Windows 11 単一セッションまたはマルチセッション デスクトップで使用することができます。
- 新しい Horizon Cloud on Microsoft Azure ポッドは、常に高可用性が有効な状態でデプロイされます。
- マルチポッド イメージは、ユーザー ネットワークからインターネットに送信されるイメージ操作（自動化された [Marketplace からの仮想マシンのインポート] ウィザードを使用する場合など）に対して構成されたプロキシ設定を利用するようになりました。
- Azure Marketplace から AMD GPU およびグラフィックス ドライバを使用する仮想マシンを手動でインポートし、それらのインポートされた仮想マシンをゴールド イメージに使用するためのサポート。このサポートでは、Azure 仮想マシン モデル Standard_NV4as_v4 と、このリリースのマニフェスト以降を実行しているポッドを使用する必要があります。
- 既存の専用割り当てでは、個々のユーザーのニーズに基づいて、プロビジョニングされた仮想マシンのワークロード CPU、メモリ、またはディスクを調整できるようになりました。これを行うと、プール タイプが混合タイプに変更されます。この機能の使用は、このリリースのマニフェスト以降を実行するポッドでサポートされています。
- 推奨される Horizon Agents Installer バージョンがコンソールの [キャパシティ] 画面に表示されるようになりました。エージェントを最新の状態に保つためのリマインダとして定期的な通知が生成されます。この機能は、このリリースのマニフェスト以降を実行しているポッドで提供されます。
- ゲスト OS のシャットダウンによって [停止] 状態になった、サービスによって作成された Microsoft Azure 仮想マシンは、請求が継続されるのを防ぐために自動的に [割り当て解除] 状態に移行します。この機能の使用は、このリリースのマニフェスト以降を実行するポッドでサポートされています。
- Horizon Cloud ポッドの App Volumes 領域に関する機能強化。この機能を使用するには、ポッドでこのリリースのマニフェスト レベル以降が実行されている必要があります。
 - ユーザーがデスクトップと [スタート] メニューからアプリケーションをクリックして起動すると、アプリケーションをオンデマンドで配信できるようになりました。この動作は、アプリケーションがすでに Windows マシンにネイティブでインストールされている場合と同じです。この設定は、新しく作成したパッケージで使用できます。
- Microsoft Azure の問題による影響を軽減するため、v2204 サービス リリース以降、サービスの自動化された [Marketplace からの仮想マシンのインポート] ウィザードで、デフォルトで非 GPU Windows 10 OS イメージに使用される仮想マシン モデルが変更されました。報告された問題の詳細については、VMware ナレッジベースの記事 [KB88343](#) を参照してください。

このウィザードでは、この v2204 リリースで新たに追加された Windows 11 サポートに対して特定のモデルも使用します。

ウィザードは次のモデルを使用するようになりました。ポッドの Azure サブスクリプションで仮想マシンファミリーの割り当てを確認し、ウィザードを使用して作成する予定のイメージに対して使用可能な割り当てがあることを確認することをお勧めします。

シングルポッド イメージ - [Marketplace からの仮想マシンのインポート] ウィザードでは、以下が作成されます。

- 非 GPU Windows 10 OS または Windows 10 Enterprise マルチセッション OS シングルポッド イメージ、Standard_DS2_v2 仮想マシン
- 非 GPU Windows Server OS 仮想マシン シングルポッド イメージ、Standard_D2_v3 仮想マシン
- GPU 対応の Windows 10 OS、Windows 10 Enterprise マルチセッション OS、または Windows Server OS シングルポッド イメージ、Standard_NV6 仮想マシン
- 非 GPU Windows 11 OS または Windows 11 Enterprise マルチセッション OS シングルポッド イメージ、Standard_D4s_v3 仮想マシン
- GPU 対応の Windows 11 OS または Windows 11 Enterprise マルチセッション OS シングルポッド イメージ、Standard_NC6s_v3 仮想マシン
- 非 GPU Windows 7 OS シングルポッド イメージ、Standard_DS2_v2 仮想マシン (Windows 7 では GPU がサポートされない)

マルチポッド イメージ - [Marketplace からの仮想マシンのインポート] ウィザードでは、以下が作成されます。

- 非 GPU Windows 10 OS、Windows 10 Enterprise マルチセッション OS、または Windows Server OS マルチポッド イメージ、Standard_DS2_v2 仮想マシン
- GPU 対応の Windows 10 OS、Windows 10 Enterprise マルチセッション OS、または Windows Server OS マルチポッド イメージ、Standard_NV6 仮想マシン
- 非 GPU Windows 11 OS または Windows 11 Enterprise マルチセッション OS マルチポッド イメージ、Standard_D4s_v3 仮想マシン
- GPU 対応の Windows 11 OS または Windows 11 Enterprise マルチセッション OS マルチポッド イメージ、Standard_NC6s_v3 仮想マシン
- 非 GPU Windows 7 OS マルチポッド イメージ、Standard_DS2_v2 仮想マシン (Windows 7 では GPU がサポートされない)

その他の注意事項

- Horizon オンプレミス ポッドの IMS サポートでは：
 - イメージ コピーのターゲット ポッドの vCenter Server でデータストアとネットワークを選択するオプションが提供されます。
 - マルチクラスタ化された vCenter Server での IMS の使用がサポートされるようになりました。
 - このポッド タイプでは、公開が失敗したときに公開を再試行する [再公開] オプションが提供されるようになりました。

2022年3月 - v2203

2022年3月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2022年3月のリリースノートに記載されている機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

要求別有効化の機能の有効化を要求するには、[VMware ナレッジベースの記事 KB2006985](#)に記載されているように、サポート リクエストを発行します。

注： Horizon Agents Installer、Horizon Cloud Connector、および Universal Broker プラグイン インストーラの一般公開されたバージョンは、この v2203 リリースでは変更されていません。

次のキー バイナリの新しいバージョンが v2203 で初登場しました。

サービスのデプロイ ウィザードによって Microsoft Azure にデプロイされた Horizon Cloud ポッドの新しいポッド マニフェスト バージョン。このマニフェストには、ポッド マネージャが初めて実装された機能の一部に必要とするバックエンド サポートの提供に加えて、信頼性のためのプラットフォーム コードの改善が含まれています。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- VDI デスクトップ割り当ての [サマリ] タブにある新しい [編集] ボタンを使用すると、割り当ての詳細を簡単に編集できます。
- ファームの [サマリ] タブには、ファームの作成日時、Azure リソース グループ名、そのファーム ID など、追加の有用な情報が表示されます。
- ポッド デプロイヤーでは、ポッドのデプロイ中に Azure Key Vault を作成する必要がなくなりました。[ポッドの追加] ウィザードは、ファームと VDI デスクトップ割り当てのディスク暗号化機能の使用をサポートするために、サブスクリプションの Microsoft.KeyVault リソース プロバイダが Registered 状態であることを引き続き検証することに注意してください。この機能では、ディスク暗号化機能の使用を選択するときに、ポッド マネージャのリソース グループに Key Vault を作成する必要があります。

重要： 既存のユーザーは、VMware のサポートの指示がない限り、Horizon Cloud on Microsoft Azure デプロイに存在する Key Vault を削除しないでください。Key Vault を手動で削除すると、デプロイがサポート対象外の状態になります。

- RSA SecurID は、ポッドのゲートウェイ構成での 2 要素認証構成のオプションです。デプロイ済みのゲートウェイ構成でこの機能を使用するには、ポッドがマニフェスト 3139 以降を実行している必要があります。この機能は、2022年3月中旬までに [ポッドの追加] ウィザードと [ポッドの編集] ウィザードに導入される予定です。オプションは、その時点でこれらのウィザードに表示されるようになります。

その他の注意事項

- Horizon ポッドでの Horizon インフラストラクチャの監視機能の使用はサポートされなくなりました。その結果、これらの機能を Horizon ポッドで使用することに関するすべての参照がドキュメントから削除されます。(Horizon ポッドは、Connection Server を実行するポッドです。)

2022 年 2 月 - v2201

2022 年 2 月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2022 年 2 月のリリース ノートに記載されている機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

注： Horizon Agents Installer、Horizon Cloud Connector、および Universal Broker プラグイン インストーラの一般公開されたバージョンは、この v2201 リリースでは変更されていません。

次のキー バイナリの新しいバージョンが v2201 で初登場しました。

サービスのデプロイ ウィザードによって Microsoft Azure にデプロイされた Horizon Cloud ポッドの新しいポッド マニフェスト バージョン。このマニフェストには、ポッド マネージャが初めて実装された機能の一部に必要とするバックエンド サポートの提供に加えて、パフォーマンスと信頼性のためのプラットフォーム コードの改善が含まれています。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- Active Directory 環境をテナントに登録するときに、プロトコルとして LDAPS を選択できるようになりました。この機能は、テナントが明示的に有効になっていて、すべてのポッドがこのリリースのマニフェスト レベルを実行している場合に使用できます。有効化を要求するには、VMware のナレッジベースの記事 [KB2006985](#) の説明に従ってサポート リクエストを発行する必要があります。
- ポッドのアップグレードがスケジュールされている間、コンソールのポッドの詳細ページにバナーが表示されます。これは、ポッドとその Unified Access Gateway インスタンスのアップグレード後に、Unified Access Gateway インスタンスの NIC からの許可されたクライアント接続として RADIUS サーバで構成されている IP アドレスの更新が必要になる場合があることを示します。ポッドにゲートウェイ構成がある場合、そのポッドが新しいマニフェスト バージョンに更新されると、Unified Access Gateway インスタンスも更新されます。この機能を使用すると、アップグレードがスケジュールされている期間に、コンソールのポッドの詳細ページで、ゲートウェイ構成で RADIUS 設定が構成されている場合に、ゲートウェイ NIC がアップグレード後に使用する IP アドレスからのクライアント接続を許可するために RADIUS サーバ設定が更新されていることを確認する追加のアクションが必要になる場合があることを警告します。

イメージ管理サービス (IMS) に関連する新しい項目

- マルチポッド イメージをコピーするポッドを選択できるようになりました。以前は、デフォルトでイメージがすべてのポッドにコピーされていました。

Universal Broker に関連する新しい項目

- ヘルプ デスク ツールでは、Universal Broker を介して接続しているユーザーのセッション データにロギン セグメントの内訳が表示されます。
- Universal Broker と Dynamic Environment Manager を使用する場合、スマート ポリシーを適用するために、Dynamic Environment Manager で内部ユーザーと外部ユーザーを区別できるようになりました。
- Horizon ポッドで、VDI マルチクラウド割り当てワークフローが Windows Server 2019 を実行しているプールをサポートするようになりました。

2021年11月 - v2111

2021年10月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、この月のリリースでサービスに初めて登場した機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

次のキー バイナリの新バージョンは、2021年11月に初めて登場しました：サービスがデプロイしたポッドの新しいポッド マニフェスト バージョン、新しいバージョンの Horizon Cloud Connector、Universal Broker プラグイン インストーラ、および Horizon Agents Installer (HAI)。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- 既存の VDI デスクトップ割り当ての仮想マシン モデル タイプを編集できるようになりました。ポッドは、このリリースのマニフェスト レベルを実行している必要があります。
- マルチポッド イメージ管理で、マルチセッション オペレーティング システムがサポートされるようになりました。このようなマルチポッド イメージからファームを作成できるようになりました。ポッドはマニフェスト 2915.x 以降を実行している必要があります。
- シングルポッド プロセッサが有効になっているテナントでは、同じ Horizon Cloud ポッドによってプロビジョニングされた VDI デスクトップ割り当て間で個々の仮想マシンを移動できるようになりました。この機能を使用するには、テナントがこれに対し明示的に有効になっており、ポッドがこのリリースのマニフェスト レベルを実行している必要があります。テナントでのこの機能の有効化を要求するには、[VMware ナレッジベース記事 KB2006985](#) に記載されているように、サポート リクエストを発行します。
- エージェントの自動更新の領域では、エージェントが仮想マシンで停止し、実行されていない場合に、不完全または失敗したエージェントの更新を修正できるようになりました。ポッドは、このリリースのマニフェスト レベルを実行している必要があります。
- Horizon Cloud ポッドの App Volumes 領域に関する機能強化。ポッドは、このリリースのマニフェスト レベルを実行している必要があります。
 - アプリケーション パッケージは、そのアプリケーションの最後に割り当てられたユーザーが Windows 10 Enterprise マルチセッション システムからログオフすると、自動的に接続解除されるようになりました。以前は、パッケージを接続解除するためには仮想マシンのシャットダウンが必要でした。
 - App Volumes は、Windows 10 Enterprise マルチセッション オペレーティング システムでの VMware Dynamic Environment Manager をサポートするようになりました。
 - App Volumes バッチ ファイルを使用して、App Volumes ワークフローを構成できます。この機能は、『App Volumes 管理ガイド』の [App Volumes ワークフロー用のバッチ スクリプト](#) というタイトルのページで説明しています。
 - RunAsUser.exe ユーティリティが App Volumes Agent に含まれるようになり、App Volumes 詳細構成バッチ ファイルから実行可能ファイルを実行できるようになりました。通常、これらのバッチ ファイルのコードはシステムの範囲で実行され、このユーティリティを使用して、現在ログインしているユーザーのコンテキストでコードを実行できます。この機能は、『App Volumes 管理ガイド』の [App Volumes バッチ スクリプト用に RunAsUser を使用する](#) というタイトルのページで説明しています。

- Windows 10 Enterprise マルチセッション オペレーティング システムでの印刷スプーラ再起動動作の改善。

Universal Broker に関連する新しい項目

このリリース以降、Horizon Cloud on Microsoft Azure のグリーンフィールド デプロイでは、Universal Broker がデフォルトで有効なブローカーになります。

現在のユーザーに対する追加の注意事項

- テナントからアラートと通知を受信するメール アドレスを指定できるようになりました。これらのアドレスをテナント管理者ロールに関連付ける必要はありません。この機能の前は、テナント管理者のみが E メールでアラートと通知を受信できました。
- テナントの Horizon ユニバーサル ライセンスに VMware vCenter、vSAN、vSphere などの VMware SDDC コンポーネントのライセンスが含まれている場合は、Horizon Universal Console を使用してこれらのキーを取得できます。コンソールで、取得するキーのバージョンを選択し、それらのキーをいつでも表示できます。コンソールを使用してキーを生成するには、テナントでスーパー管理者ロールを持ち、このテナントに関連付けられている EA の Customer Connect ユーザーである必要があります。
- Workspace ONE リダイレクトがテナント レベルで有効になっている場合、エンド ユーザー クライアントがポッドの Unified Access Gateway 構成の FQDN に直接接続している場合でも、エンド ユーザーは適切に Workspace ONE Hub にリダイレクトされます。以前は、このようなエンド ユーザー接続はデスクトップを直接取得していました。

2021 年 10 月 - v2110

2021 年 10 月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、この月のリリースでサービスに初めて登場した機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

注： Horizon Agents Installer、Horizon Cloud Connector、および Universal Broker プラグイン インストーラの一般公開されたバージョンは、この v2110 リリースでは変更されていません。

また、サービスのデプロイ ウィザードによって Microsoft Azure にデプロイされた Horizon Cloud ポッドのポッド マニフェスト バージョンは 3000.x のままです。重要な修正が必要な場合、3000.1、3000.2 などのパッチが利用可能になります。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- Horizon Universal Console では、組み込みの事前定義済みロールのデスクトップ割り当てとファームに対する狭い範囲の権限がサポートされるようになりました。この機能を使用するには、テナントがこれに対し明示的に有効になっており、すべての Horizon Cloud ポッドがマニフェスト 2915.x 以降を実行している必要があります。テナントでのこの機能の有効化を要求するには、[VMware ナレッジベース記事 KB2006985](#) に記載されているように、サポート リクエストを発行します。
- [新規ポッド] ワークフローと [ポッドの編集] ワークフローで、管理者はポッドの Unified Access Gateway インスタンス上の Blast Extreme の TCP ポートとして 8443 を選択できるようになりました。この機能より前は、Blast Extreme TCP ポートはデフォルトで 443 に設定され、これを変更するためのウィザード オプションはありませんでした。ポート 8443 は、クライアントからゲートウェイへのト

ラフィックのパフォーマンスが向上し、Unified Access Gateway インスタンス上のリソース使用率が低くなるため、強く推奨されます。Blast Extreme TCP ポートに 8443 を使用すると、インスタンスでの CPU 輻輳によりクライアントからのトラフィック遅延が発生する可能性が低くなります。[ポッドの編集] ワークフローを使用して、既存のゲートウェイ構成の Blast Extreme TCP ポートを変更できます。

- マルチセッション デスクトップを使用する App Volumes アプリケーションの場合、アプリケーション パッケージの分離は、そのパッケージを最後に割り当てたユーザーがログオフした後に実行されるようになりました。ボリュームを接続解除するために基盤となるファーム仮想マシンをシャットダウンする必要はなくなりました。以前は、仮想マシンのシャットダウン時にアプリケーション パッケージの分離が実行されていました。

Universal Broker に関連する新しい項目

- Universal Broker およびマルチクラウド割り当てでは、Google Cloud VMware Engine (GCVE) を使用するポッドのデスクトップとアプリケーションの仲介がサポートされるようになりました。
- Universal Broker では、仮想デスクトップ、公開デスクトップ、公開アプリケーションの起動を特定のクライアントおよびバージョンに制限し、警告メッセージをクライアントに提供する機能がサポートされるようになりました。
- Universal Broker では、エンド ユーザーが、Windows ベースのデスクトップで使用するためのオプションとして RDP プロトコルを提供する Horizon Clients 内からの RDP プロトコルを使用して VDI デスクトップおよび公開デスクトップに接続する機能がサポートされるようになりました。

Horizon Cloud Connector およびクラウド接続された Horizon ポッドに関連する新しい項目

- Google Cloud Platform 用 Horizon Cloud Connector バージョン 2.0 ネイティブ バイナリの登場により、フェデレーション アーキテクチャでデプロイされた Horizon ポッドに対してクラウド プレーンが提供するすべてのクラウドプレーン サービスが、このようなポッドでサポートされるようになりました。このようなポッドでは、管理コンポーネントに Google Cloud Platform、デスクトップ コンポーネントに Google Cloud VMware Engine (GCVE) がそれぞれ使用されます。この完全なサポートを取得するには、Horizon Cloud Connector バージョン 2.0 を使用します。現在、イメージ管理サービス (IMS) はオンプレミスの Horizon ポッドでのみサポートされ、クラウドベースの Horizon ポッド デプロイではサポートされていません。
- Amazon EC2 用 Horizon Cloud Connector バージョン 2.0 ネイティブ バイナリの登場により、フェデレーション アーキテクチャでデプロイされた Horizon ポッドに対してクラウド プレーンが提供するすべてのクラウドプレーン サービスが、このようなポッドでサポートされるようになりました。このようなポッドでは、管理コンポーネントに Amazon EC2、デスクトップ コンポーネントに VMware Cloud on AWS がそれぞれ使用されます。この機能を使用するには、バージョン 2.0 以上の Horizon Cloud Connector が必要です。新しいデプロイでは、最新バージョンを使用する必要があります。現在、イメージ管理サービス (IMS) はオンプレミスの Horizon ポッドでのみサポートされ、クラウドベースの Horizon ポッド デプロイではサポートされていません。
- Horizon Cloud Connector バージョン 2.0 OVA が、Horizon on VMware Cloud on Dell EMC での使用ができるようになりました。これらのポッドは、オールイン SDDC デプロイです。Cloud Monitoring Service (CMS) およびイメージ管理サービス (IMS) を除き、クラウド プレーンがオールイン SDDC デプロイの Horizon ポッドに対して提供するクラウドプレーン サービスは、このデプロイ タイプでサポートされます。

2021年9月 - v2109

2021年9月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2021年9月のリリースノートに記載されている機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

注： Horizon Agents Installer、Horizon Cloud Connector、および Universal Broker プラグイン インストーラの一般公開されたバージョンは、この v2109 リリースでは変更されていません。

次のキー バイナリの新しいバージョンが v2109 で初登場しました。

サービスのデプロイ ウィザードによって Microsoft Azure にデプロイされた Horizon Cloud ポッドの新しいポッド マニフェスト バージョン。このマニフェストには、ポッド マネージャが初めて実装された機能の一部に必要とするバックエンド サポートの提供に加えて、パフォーマンスと信頼性のためのプラットフォーム コードの改善が含まれています。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- Horizon Agent 更新では、割り当て内の個々のデスクトップでエージェントの更新をターゲットにできるようになりました。この機能を使用するには、このリリースのマニフェスト レベルで実行されているポッドが必要です。
- テナントの Universal Broker 設定に 2 要素認証が含まれていない限り、ポッド デプロイ ウィザードとポッドの編集ウィザードで Unified Access Gateway 構成が必須ではなくなりました。以前は、ウィザードはポッドで少なくとも 1 つの Unified Access Gateway を使用する必要がありました。
- テナントがシングルポッド仲介を使用するように構成されている場合、RDP プロトコルを使用した VDI デスクトップまたはファームベースのセッション デスクトップへの接続がサポートされるようになりました。この機能は、マニフェスト 3000.x 以降を実行するポッドでサポートされています。
- シングルポッド ブローカ テナントを Universal Broker に移行するためのシステム要件には、次のシナリオを除いて、すべてのポッドに少なくとも 1 つの内部または外部の Unified Access Gateway 構成が含まれるという要件がなくなりました。
 - 移行のスケジュール設定ウィザードの Universal Broker 設定で 2 要素認証を有効にすることを選択した場合。ウィザードの Universal Broker で 2 要素認証が有効になっている場合、移行ではテナントのフリート内のすべてのポッドに外部 Unified Access Gateway が必要です。
 - テナントのフリートに Horizon ポッドも含まれていて、コンソールの [ブローカ] 画面に Universal Broker 構成で 2 要素認証がすでに有効であることが示されている場合。この場合も、移行では、テナントのフリート内のすべてのポッドに外部 Unified Access Gateway が必要です。
- マルチセッション デスクトップを使用する App Volumes アプリケーションの場合、アプリケーションパッケージの分離は、そのパッケージを最後に割り当てたユーザーがログオフした後に実行されるようになりました。ボリュームを接続解除するために基盤となるファーム仮想マシンをシャットダウンする必要はなくなりました。以前は、仮想マシンのシャットダウン時にアプリケーション パッケージの分離が実行されていました。

Horizon Cloud Connector およびクラウド接続された Horizon ポッドに関連する新しい項目

- Horizon Cloud Connector アプライアンスで vSphere の高可用性機能を使用するための文書化された手順が利用できるようになりました。この機能は、vSphere 高可用性機能に依存するため、オンプレミスおよびオールイン SDDC ポッドアーキテクチャに固有です。これらのデプロイアーキテクチャでは、Horizon Cloud Connector は vSphere インフラストラクチャにデプロイされます。
- Google Cloud Platform と Google Cloud VMware Engine (GCVE) を使用するフェデレーションデプロイ設計でデプロイされた Cloud Monitoring Service およびポッドの使用がサポートされるようになりました。
- 管理対象状態への変更ウィザードでは、テナントの Universal Broker 設定に 2 要素認証が含まれていない限り、Unified Access Gateway 構成が必須ではなくなりました。以前は、ウィザードはポッドで少なくとも 1 つの Unified Access Gateway を使用する必要がありました。

Universal Broker に関連する新しい項目

内部ネットワーク上のエンド ユーザーの場合、Universal Broker はクライアント、仮想デスクトップおよびリモート アプリケーション (VDI および RDSH) 間の直接接続をサポートするようになりました。このサポートにより、これらの内部接続用に仮想デスクトップとリモート アプリケーションを起動するために内部 Unified Access Gateway は不要になりました。これらの内部クライアントによる仮想デスクトップとリモート アプリケーションの起動をサポートするには、コンソールの [ブローカ] - [ネットワーク範囲] を使用して出力方向 NAT アドレスの範囲を指定し、Universal Broker が指定された範囲を内部ネットワークからの発信範囲として認識できるようにする必要があります。

2021 年 8 月 - v2108

2021 年 8 月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2021 年 8 月のリリースノートに記載されている機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

注： Horizon Agents Installer、Horizon Cloud Connector、および Universal Broker プラグイン インストーラの一般公開されたバージョンは、この v2108 リリースでは変更されていません。

次のキー バイナリの新しいバージョンが v2108 で初登場しました。

サービスのデプロイ ウィザードによって Microsoft Azure にデプロイされた Horizon Cloud ポッドの新しいポッド マニフェスト バージョン。このマニフェストには、パフォーマンスと信頼性に関するプラットフォーム コードの改善が含まれています。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- [第1世代テナント - 組織が第1世代 Horizon Cloud のアプリケーション登録にカスタム ロールを使用することを希望する場合](#)で説明するように、サービス プリンシパルがサブスクリプションで使用する必要のある一連の操作に 2 つの追加操作が追加されました。これらの 2 つの追加操作は、Microsoft Azure Marketplace で事前構成されたイメージを使用して、サービスが新しいポッドのデプロイとポッドのアップグレードにかかる時間を短縮できるようにする今後の機能をサポートするためのものです。サービス プリンシパルがカスタム ロールを使用する場合、そのロールにはこれらの 2 つの追加操作を実行する権限が必要です。

- App Volumes 割り当てを作成するときに、ウィザードには [OS ファミリ] 選択メニューが表示されなくなります。1つのタイプの Windows オペレーティングシステムを実行している仮想マシンでキャプチャされたパッケージは、これらのポッドで使用できるタイプの Windows オペレーティングシステムを実行しているデスクトップと互換性があるため、割り当てのために OS ファミリーを指定する必要はなくなったと判断されました。そのため、機能を保持したまま、メニューをウィザードから削除できます。この変更は、このリリースより前に作成された App Volumes 割り当てにも適用されます。このような既存の App Volumes 割り当てを編集するときに、割り当ての作成時に [OS ファミリ] が選択されていた場合でも、[OS ファミリ] の選択がシステムで不要になったため、編集ウィンドウにはそのフィールドが表示されなくなります。
- エージェントの自動更新中に発生する障害に関するレポート機能の領域における追加の改善。ポッドがこのリリースの新しいマニフェスト バージョンを実行している場合、ダウンロード可能な CSV レポートには、エージェントの更新プロセスが失敗したデスクトップ仮想マシンに加えて、プロセスが成功またはスキップされたデスクトップ仮想マシンの名前も表示されるようになりました。

現在のユーザーに対する追加の注意事項

新しい VMware 製品である VMware Workspace ONE Assist for Horizon との連携により、Horizon Cloud 管理者は、Horizon Universal Console にあるヘルプ デスク ツールから直接リモート サポート セッションを起動できます。管理者は、仮想デスクトップ セッションに関連するタスクや問題についてエンド ユーザーを支援できます。VMware Workspace ONE Assist for Horizon は、VMware Workspace ONE UEM 製品ラインの一部です。この新しい製品で提供される機能を使用するためのすべての要件については、[Workspace ONE for Horizon と Horizon Cloud ドキュメント](#)の「Workspace ONE Assist を使用した Horizon Cloud の要件」トピックを参照してください。

Horizon Universal Console の [全般設定] ページの [連絡先情報] セクションは削除されました。これは、そのフィールドがどのワークフロー、ユースケース、またはシステム操作にも必要ないためです。

2021 年 7 月 - v2106

2021 年 7 月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2021 年 7 月のリリース ノートに記載されている機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

次のキー バイナリの新バージョンは、2021 年 7 月に初めて登場しました：サービスがデプロイしたポッドの新しいポッド マニフェスト バージョン、新しいバージョンの Horizon Cloud Connector、Universal Broker プラグイン インストーラ、および Horizon Agents Installer (HAI)。

Horizon Cloud Connector および Horizon ポッドでの使用に関連する新しい項目

- Horizon Cloud Connector のバージョン 2.0 では、ライセンス サービスにサービス レベルのフォルトトレランスが追加されています。この機能に関するドキュメントについては、『管理ガイド』のトピック [Horizon Cloud Connector 2.0 - クラスタとサービス レベルのフォルトトレランス](#)およびそのサブトピックを参照してください。
- Horizon Cloud Connector のバージョン 2.0 では、SNMP を使用したアプライアンスの監視がサポートされます。管理者は、この標準ベースの監視機能を使用して、Horizon Universal Console にログイン

していない場合でも、ライセンス、アップグレード、コネクタのライフサイクルなど、コネクタ関連の重要なサービスをプロアクティブに監視して関連するアラートを受信できます。この機能に関するドキュメントについては、『管理ガイド』のトピック [Horizon Cloud Connector 2.0 - SNMP を使用したアプライアンスの監視](#) を参照してください。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- マルチポッド イメージ管理は、単一セッションの VDI イメージを Microsoft Azure の 2 つ以上の Horizon Cloud ポッドに公開して複製し、1 回の操作で複数の VDI マルチクラウド割り当てを更新するための簡単な方法を提供します。Horizon Cloud ポッドを使用したマルチポッド イメージ管理の機能は、VDI マルチクラウド割り当てを使用するように構成されたテナントと、マニフェスト 2632.x 以降を実行する Horizon Cloud ポッドでのみ使用できます。この機能に関するドキュメントについては、[クラウドからの Horizon イメージの管理](#) およびそのサブトピックを参照してください。
- エージェントの自動更新に関する機能強化：
 - スケジュール設定されたエージェントの更新に先立ち、システムはデフォルトでエージェントの更新プロセス用に選択された仮想マシンを自動的に再起動するようになりました。この自動再起動により、エージェントの更新操作を実行する前に、仮想マシンとそのオペレーティング システム内で実行されているソフトウェアおよびサービスが既知の状態であることを確認できます。
 - エージェントの自動更新中に発生する障害に関するレポート機能が向上しました。割り当てでエージェントの更新プロセスが進行中のときでも、エージェントの更新プロセスが失敗したデスクトップ仮想マシンの名前の CSV レポートをダウンロードできます。CSV レポートは、ポッドがこのリリースの新しいマニフェスト バージョンを実行しているときにダウンロードして入手できます。

2021 年 5 月 - v2105

2021 年 5 月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2021 年 5 月のリリースが操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

注： Horizon Agents Installer、Horizon Cloud Connector、および Universal Broker プラグイン インストーラの一般公開されたバージョンは、この v2105 リリースでは変更されていません。

次のキー バイナリの新しいバージョンが v2105 で初登場しました。

サービスのデプロイ ウィザードによって Microsoft Azure にデプロイされた Horizon Cloud ポッドの新しいポッド マニフェスト バージョン。このマニフェストには、パフォーマンスと信頼性に関するプラットフォーム コードの改善が含まれています。

Horizon Cloud Connector および Horizon ポッドでの使用に関連する新しい項目

Universal Broker は、VMware SDDC 上の Horizon ポッド用に公開されたデスクトップとアプリケーションをサポートするようになりました。このサポートを使用するには、ポッドで VMware Horizon 8 ソフトウェア バージョン 2103 以降および Universal Broker プラグイン インストーラ バージョン 21.03 以降が実行されている必要があります。

2021年4月 - v2104

2021年4月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、2021年4月のリリースが操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

注： Horizon Cloud Connector および Universal Broker プラグイン インストーラのバージョンは、この v2104 リリースでは変更されていません。テナント環境では、これらのコンポーネントの 2021年3月バージョンを引き続き使用できます。

次のキー バイナリの新しいバージョンが v2104 で初登場しました。

- サービスのデプロイ ウィザードによって Microsoft Azure にデプロイされた Horizon Cloud ポッドの新しいポッド マニフェスト バージョン。このマニフェストには、パフォーマンスと信頼性に関するプラットフォーム コードの改善が含まれています。
- 新しい HAI バージョンには、Horizon Agent からデータを受信する Cloud Monitoring Service に関連する断続的な問題を解決するための修正が含まれています（問題レポート 2742816）。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

コンソールを使用して App Volumes アプリケーション間で App Volumes パッケージを移動するためのサポート。新しくインポートされたパッケージを適切なアプリケーションに移動するためのサポートが含まれています。

現在のユーザーに対する追加の注意事項

一部の機能は、制限付き機能として初登場しています。このような機能は、テナントごとに、通常は、要求ベースで有効になります。

2021年3月 - v2103

2021年3月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、新しい機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

次のキー バイナリの新バージョンは、2021年3月に初めて登場しました。サービスがデプロイしたポッドの新しいポッド マニフェスト バージョン、新しいバージョンの Horizon Cloud Connector、Universal Broker プラグイン インストーラ、および Horizon Agents Installer (HAI)。

Horizon Cloud Connector および Horizon ポッドでの使用に関連する新しい項目

バージョン 1.10 の Horizon Cloud Connector で修正とセキュリティ アップデートが提供されます。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

- Microsoft Azure 上の Horizon Cloud ポッドの既存のデプロイで Universal Broker およびマルチクラウド割り当てを使用できるようになりました。
- コンソールのポッドの詳細ページに、優先メンテナンス ウィンドウを指定するために使用される新しいメンテナンス機能が追加されています。この機能を使用して、ポッドのメンテナンス アクティビティが行われるのに必要な時間と曜日をシステムに通知します。

- このリリースのポッド マニフェストから、Microsoft Azure 上の Horizon Cloud ポッドの App Volumes は Microsoft Windows 10 Enterprise マルチセッションをサポートするようになり、複数のユーザーがそれぞれのアプリケーション割り当てを使用して個々のセッションにログインできます。以前は、Horizon Cloud ポッドの App Volumes による Microsoft Windows 10 Enterprise マルチセッションの使用は Tech Preview でした。この機能は、このリリースのポッド マニフェストのバージョン以降と、このリリースの App Volumes Agent バージョン以降の環境でサポートされていることに注意してください。
- Microsoft Azure 上の Horizon Cloud ポッドの App Volumes を使用し、App Volumes コマンドライン キャプチャ プログラムを使用して Horizon Cloud アプリケーション インベントリにインポートするためのアプリケーションをキャプチャするユーザー向けに、App Volumes 4 バージョン 2103 で新しいオプションが導入されました。このオプションは、App Volumes Manager コンソールを必要とせずにアプリケーションをパッケージングできるだけでなく、VHD 形式や MSIX アプリケーション接続形式のパッケージで動作するその他のツールも提供します。詳細については、[App Volumes 4 バージョン 2103 リリース ノートの「新機能」](#)を参照してください。

現在のユーザーに対する追加の注意事項

一部のクラウドプレーン ベースの機能は、v2103 リリースの前の週に初登場しました。

Universal Broker およびマルチクラウド割り当てが Azure VMware Solutions (AVS) 上の Horizon ポッドをサポートするようになりました。ハイブリッドおよびマルチクラウドのデプロイ全体でマルチクラウド割り当ての統合仲介が可能になり、Horizon ポッドと Microsoft Azure 上の Horizon Cloud ポッドの両方がサポートされます。

新しい名前 Horizon Universal Console を反映するようにコンソールが拡張されました。

一部の機能は、制限付き機能として初登場しています。このような機能は、テナントごとに、通常は、要求ベースで有効になります。

このリリースでは、Horizon ポッドの管理コンソール (Horizon Console と呼ぶ) で、[クラウド ブローカ] オプションが動作しません。このオプションは、VMware Horizon 8 バージョン 2103 (8.2) を実行しているクラウド管理 Horizon ポッドの RDS デスクトップ プール設定およびアプリケーション プール設定に表示されます。[クラウド ブローカ] オプションを有効にしても、この Horizon Cloud リリースには影響はありません。

2021 年 1 月 - v2101

2021 年 1 月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、新しい機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

次のキー バイナリの新バージョンは、2021 年 1 月に初めて登場しました：サービスがデプロイしたポッドの新しいポッド マニフェスト バージョン、新しいバージョンの Horizon Cloud Connector、Universal Broker プラグイン インストーラ、および Horizon Agents Installer (HAI)。

Horizon Cloud Connector および Horizon ポッドでの使用に関連する新しい項目

- Horizon Cloud Connector 1.9 では、自動更新機能によってネットワークの詳細をより簡単に構成できるようになりました。アップグレードのために、新しいアプライアンスに対して未割り当ての固定 IP アドレスを指定することのみが必要です。

- Horizon Cloud Connector 1.9 は、Horizon Cloud Connector アプライアンスのトラブルシューティングを行う際に、よりセキュアなアクセス方法を提供します。アプライアンスの root ユーザーの SSH アクセスが無効になり、新しいカスタム ユーザー (ccadmin) を SSH アクセスで使用できるようになりました。これには、パスワード認証情報ではなく SSH パブリック キーを使用することのサポートが含まれています。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

ポッドで、エージェントの更新に失敗した場合に専用デスクトップを以前の使用可能な状態にロールバックする機能をサポートするようになりました。また、更新プロセスを停止して残りのデスクトップをスキップするフェイルファースト メカニズムを提供する、構成可能な障害しきい値もサポートします。以前から存在しているポッドでこの機能を使用するには、まずそのポッドをマニフェスト 2632.0 以降に更新する必要があります。

現在のユーザーに対する追加の注意事項

一部のクラウドプレーン ベースの機能は、v2101 リリースの前の週に初登場しました。

2474.0 以降のポッド マニフェストの場合、ドメイン参加アカウントの Active Directory 権限のセットが少なくなり、テナントの柔軟性が向上しています。ただし、システムが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操作のために同じドメイン参加アカウントを使用するため、2474.0 以前のマニフェストのポッドが含まれている場合は、そのポッドに必要な以前の権限セットがドメイン参加アカウントに含まれていることを確認する必要があります。Microsoft Azure のすべての Horizon ポッドがポッド マニフェスト 2474.0 以降にアップデートされると、ドメイン参加アカウントに対して、より新しい Active Directory 権限セットを採用できます。ドメイン参加アカウントの権限については、[Horizon Cloud の運用に必要なサービスアカウント](#)と、更新されたセクションを参照してください。

新しい用語を反映するためにコンソールが拡張されました。以前は、オンプレミスの vSphere インストールまたは VMware Cloud on AWS SDDC (Software-Defined Data Center) にインストールされているクラウド接続された Horizon ポッドを参照するときに、[オンプレミス] または [VMware Cloud on AWS] などのラベルがコンソールで表示されていました。これらは Horizon Connection Server ソフトウェアに基づいたポッドです。[Azure VMware Solution \(AVS\) 上の Horizon ポッド](#)および [Google Cloud VMware Engine \(GCVE\) 上の Horizon ポッド](#)など、追加のクラウドホスト型 VMware SDDC での Horizon ポッドのデプロイが利用可能であることにより、テナントのポッド フリートに含まれる該当メンバーを参照する際に、コンソールは [VMware SDDC] というラベルを使用するようになりました。

Microsoft Windows Server 2019 で登録サーバを実行するためのサポートが追加されました。登録サーバは、True SSO 機能のために使用されます。Microsoft Windows Server 2008 への登録サーバのインストールはサポートされなくなりました。

2020 年 10 月 - v2010

2020 年 10 月よりも前からクラウド接続されたポッドを使用している既存のユーザーであり、新しい機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

次のキー バイナリの新バージョンは、2020 年 10 月に初めて登場しました：サービスがデプロイしたポッドの新しいポッド マニフェスト バージョン、新しいバージョンの Horizon Cloud Connector、Universal Broker プラグイン インストーラ、および Horizon Agents Installer (HAI)。

Horizon Cloud Connector および Horizon ポッドでの使用に関連する新しい項目

- Horizon Cloud Connector バージョン 1.8 は、OVA と VHD の両方の形式でリリースされます。
- Horizon Cloud Connector 1.8 では、デプロイ プロファイルを選択して、サブスクリプション ライセンス サポートのみで有効にするか、Horizon Cloud 機能を使用して有効にするかを選択できます。この選択は、アプライアンスのデプロイ時に行われます。
- Horizon Cloud Connector は [Azure VMware Solution \(AVS\)](#) にデプロイされた Horizon ポッドをサポートするようになりました。現在このサポートは、これらのデプロイでのサブスクリプション ライセンスの使用に限定されています。クラウドホスト型サービスの完全なセットは、これらのデプロイ タイプにはまだ提供されていません。

Microsoft Azure のサービスがデプロイしたポッドに関連する新しい項目

Horizon Cloud on Microsoft Azure ポッドは、ポッドのデプロイまたはゲートウェイのデプロイ中にカスタムの Azure リソース タグを指定する機能をサポートするようになりました。ポッド デプロイヤーは、指定されたタグをポッド デプロイヤーが作成するリソース グループに適用します。ポッド デプロイヤーが作成するリソース グループの説明については、[Microsoft Azure にデプロイされたポッド用に作成されたリソース グループ](#)を参照してください。この新機能は、ポッドのマニフェスト バージョンに依存しません。

2020 年 7 月 - v3.1

2020 年 7 月よりも前からクラウド接続されたポッドを使用していて、新しい機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

既存のクラウド接続された Horizon ポッドの場合

Horizon Cloud Connector 1.7 の登場。

Microsoft Azure の既存のポッドの場合

以下の新機能を既存のポッドで使用するには、そのポッドを最初にマニフェスト 2298.0 以降に更新して機能を利用する必要があります。

- ファームおよび VDI デスクトップ割り当てで使用される複数のテナント サブネット。この機能は、Universal Broker で構成されたテナントで使用されているマルチクラウド デスクトップ割り当てではまだ使用できません。
- RDSH ファームでの高度なセッション ロード バランシングの使用。
- デスクトップの自動割り当てとファームのサイズ変更のサポートにより、キューに登録済みまたは実行中の状態にあるデスクトップとファームの拡張タスクの両方をキャンセルできるようになりました。この機能は、Universal Broker で構成されたテナントで使用されているマルチクラウド デスクトップ割り当てではまだ使用できません。

- エンド ユーザーのログイン時間を向上させるために、パワーオフ状態にあって、エンド ユーザーのデスクトップへの要求を満たすためにパワーオンにする必要があるポッド プロビジョニングされたデスクトップ 仮想マシンに対して、仮想マシンがエージェント準備完了状態になるまでにかかる時間が短縮されました。
- App Volumes 機能の使用 - ポッドをこのリリースのマニフェスト バージョンに更新する必要があります。またお使いのユーザー アカウントが、次の Horizon Cloud 制御プレーン リージョンのいずれかにある必要があります : USA-2 (PROD1_NORTHCENTRALUS2_CP1)、Europe-2 (PROD1_NORTHEUROPE_CP1)、または Australia-2 (PROD1_AUSTRALIAEAST_CP1)。制御プレーンの地域は、「Horizon Cloud Service へようこそ」という件名の E メールに記載されています。

ポッドにゲートウェイ構成をデプロイする場合、以前のリリースの Standard_A4_v2 仮想マシン サイズに加えて、各 Unified Access Gateway インスタンスにより多くの vCPU を提供する Standard_F8s_v2 仮想マシン サイズを使用することもできるようになりました。既存のポッドの場合、ポッドを編集してそのポッドに新しいゲートウェイ構成を追加すると、この新しい機能を使用できます。

現在のユーザーに対する追加の注意事項

既存のすべてのユーザーに対して、コンソールのヘッダー バーで製品フィードバックを送信する拡張機能を利用できるようになりました。

高可用性 (HA) 機能を備えたポッドが、Microsoft Azure Government (米国バージニア州政府、米国アリゾナ州政府、米国テキサス州政府) でサポートされるようになりました。この機能が必要な既存のポッドが Microsoft Azure Government にある場合は、有効化について VMware の担当者にお問い合わせください。

2020 年 3 月 - v3

2020 年 3 月よりも前からクラウド接続されたポッドを使用していて、新しい機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

既存のクラウド接続された Horizon ポッドの場合

Horizon Cloud Connector 1.6.x の登場によって、Horizon Cloud Connector がポッドを Horizon Cloud と正常にペアリングするために必要な Horizon ポッドのシステム コンポーネントとサービスの健全性を確認するためのコマンドライン診断ツールが提供されます。Web ベースの構成ポータルにログインしてポッドの構成ウィザードを実行する前に、この診断ツールを実行して、正常な結果を妨げる可能性のある項目を確認できます。問題が発見された場合、ツールはコンポーネント名、詳細、および推奨される修復手順をレポートします。

Microsoft Azure の既存のポッドの場合

以下の新機能を既存のポッドで使用するには、特に記載されていない限り、そのポッドを最初にマニフェスト 1976.0 以降に更新して機能を利用する必要があります。

- 外部 Unified Access Gateway 構成用に個別のサブスクリプションを使用する場合に高度なデプロイ構成をサポートするには、ポッド デプロイヤーによって作成されたデフォルトのリソース グループではなく、ユーザーが作成した既存のリソース グループに Unified Access Gateway リソースをデプロイすることを選択できます。既存のポッドでこの機能を利用するには、まずポッドを少なくともマニフェスト バージョン 1763 以降 (2019 年 12 月のマニフェスト) に更新する必要があります。次に、外部ゲートウェイ構成に個別のサブスクリプション、VNet、およびカスタム リソース グループを使用するには、文書化された要件をすべて満たす必要があります。その要件には、使用する VNet をポッドの VNet とピアリングし、使

用するサブスクリプションでリソース グループを作成することなどが含まれます。次に、コンソールのワークフローを使用して既存の外部ゲートウェイを削除し、ポッドの既存の外部 Unified Access Gateway 構成を削除する必要があります。削除が正常に完了したら、[ポッドの編集] ワークフローを実行して、新しいオプションを使用して外部ゲートウェイを追加し、外部 Unified Access Gateway を既存のリソースグループに配置できます。

- 管理者は、VDI デスクトップ仮想マシンがエンドユーザーに割り当てられると、デスクトップ仮想マシン名ではなく、専用 VDI デスクトップ割り当ての名前をエンドユーザー クライアントに表示するように指定できるようになりました。以前は、エンドユーザーが特定の VDI デスクトップ仮想マシンを要求すると、そのクライアントはデフォルトでデスクトップ仮想マシンの名前を表示し、それを変更することはできませんでした。このオプションによって、Workspace ONE Access を経由するエンドユーザー接続に対する表示内容が変更されることはありません。Workspace ONE Access は、常に専用 VDI デスクトップ割り当て名を表示し、エンドユーザーが Workspace ONE Access からデスクトップ仮想マシンを起動すると、デスクトップ名がエンドユーザー クライアントに表示されます。[全般設定] ページにこの機能のオプションが表示されますが、この機能を利用できるようにするには、ポッドで 1976.0 以降のマニフェストが実行されている必要があります。
- ポッド マニフェスト 1976.0 以降では、管理者が個々のファーム仮想マシンをメンテナンス モードに切り替えて、仮想マシンでメンテナンス アクションを実行できるようにすることができます。この機能を活用して仮想マシンごとのメンテナンス モードを設定する前に、ポッドでこのリリースのマニフェスト バージョンを実行する必要があります。また、コンソールの既知の問題により、この機能のオプションがコンソールのファームの [サーバ] タブに表示されますが、ファームの仮想マシンのエージェントがバージョン 20.1.0 以降を実行するまで、これらのユーザー インターフェイス オプションはモードを設定しません。

現在のユーザーに対する追加の注意事項

コンソールの [レポート] ページと [ダッシュボード] ページで利用可能なレポートの機能が拡張されました。これらのレポートのデータは、Cloud Monitoring Service によって提供されます。既存のポッドでこの機能を利用できます。

2019 年 12 月 - v2.2

2019 年 12 月よりも前からクラウド接続されたポッドを使用していて、新しい機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

既存のクラウド接続された Horizon ポッドの場合

このリリース以降：

- vCenter Server 環境のデータストア容量が不十分であるために更新に対応できないなどの、ユーザーが制御可能な条件によって、Cloud Connector の正常な自動更新が妨げられる可能性があります。このリリース以降、Horizon Cloud テナント アカウントで自動更新が有効になっている場合、そのようなアイテムはコンソールで識別されるため、それらのアイテムに対処してクリアできます。
- VMware Cloud on AWS にデプロイされた Horizon ポッドでは、Horizon Cloud Connector の自動アップグレードはサポートされていません。

- Horizon Cloud Connector のオンボーディング成功画面が強化されて、コネクタのコンポーネントの健全性ステータスが表示され、また Horizon Cloud Connector アプライアンスで SSH を有効/無効にするオプションが提供されます。

Microsoft Azure の既存のポッドの場合

以下の新機能を既存のポッドで使用するには、特に記載されていない限り、そのポッドを最初にマニフェスト 1763.0 以降に更新して機能を利用する必要があります。

- 高度なデプロイ構成をサポートするために、ポッド デプロイは次のオプションを提供します。
 - ポッドの VNet およびコア ポッド要素とは別に、外部ゲートウェイ構成の Unified Access Gateway インスタンスに個別の VNet を使用します。VNet をピア接続する必要があります。
 - コア ポッド要素に使用されるサブスクリプションとは別に、外部 Unified Access Gateway 構成に個別のサブスクリプションを使用します。VNet はサブスクリプションにスコープ指定されるため、個別のサブスクリプション デプロイ シナリオは、個別の VNet シナリオでもあります。VNet をピア接続する必要があります。
 - 既存のポッドでこの機能を利用するには、最初にポッドをマニフェスト 1763.0 以降に更新する必要があります。次に、その VNet をポッドの VNet とピアリングするなど、外部ゲートウェイ構成に個別の VNet を使用するには、文書化された要件をすべて満たす必要があります。次に、コンソールのワークフローを使用して既存の外部ゲートウェイを削除し、ポッドの既存の外部 Unified Access Gateway 構成を削除する必要があります。削除が正常に完了したら、[ポッドを編集]ワークフローを実行して、新しいオプションを使用して外部ゲートウェイを追加できます。
- このリリースのマニフェスト以降、VDI デスクトップ割り当ておよび RDSH ファームで SSD ディスクタイプを使用できます。
- このリリースのマニフェスト以降、VDI デスクトップ割り当ておよび RDSH ファームの OS ディスクサイズをカスタマイズできます。以前のポッド マニフェストで、OS のディスクサイズは公開された基本イメージと同じに設定されており、これはデフォルトで 127 GB であり変更できませんでした。
- このリリースの新機能として、[Marketplace から仮想マシンをインポート] ウィザードには、作成される仮想マシンを Active Directory ドメインに参加させないようにする設定が表示されます。以前は、このワークフローで仮想マシンがデフォルトでドメインに参加していたため、その動作を変更できませんでした。この新しいトグルは、このリリースのマニフェスト バージョンよりも前の既存のポッドで使用できます。
- このリリースでの [容量] ページの再設計により、[タイプ] ビューは削除されました。[容量] ページの [タイプ] ビューの削除により、そのビューから以前にアクセスしたアイテムについて注意すべき 2 つの変更があります。ポッドのサブスクリプションの Microsoft Azure 制限のうちのポッドの現在の使用量を表示するアクションがポッドの詳細ページに移動し、そのビュー内に存在していた [サブスクリプションを削除] アクションが完全に削除されました。

現在のユーザーに対する追加の注意事項

- 管理コンソールの [レポート] 画面で利用可能なレポートの機能が拡張されました。これらのレポートのデータは、Cloud Monitoring Service によって提供されます。
- Horizon Cloud 管理コンソールの [キャパシティ] 画面の機能強化。ポッドの詳細ページにドリルダウンしてポッドの構成可能な詳細を変更したり、テナント環境からポッドを削除したりするのではなく、[キャパ

シティ] 画面からポッドの編集とポッドの削除ワークフローを開始できるようになりました。この再設計の結果として、以前は [キャパシティ] 画面の [場所] ビューを使用して実行していた場所情報の変更ワークフローが、[ポッドを編集] ワークフローのオプションになりました。たとえば、新しい場所の名前を指定するには、ポッドで [編集] アクションを使用し、[ポッドの編集] ワークフローのオプションとして新しい場所の名前を指定できます。Microsoft Azure サブスクリプションに関連付けられたすべてのポッドが削除されたときに、保存されているサブスクリプション情報を削除するために以前の [場所] ビューのワークフローを使用することはできなくなりましたので注意してください。

- 以前の製品名 VMware Identity Manager は、VMware Workspace ONE™ Access という名前に変更されました。
- Horizon Agents Installer は、休止状態の DaaS Agent をインストールしません。以前のリリースでは、HAI によって DaaS Agent の MSI がゲスト OS にインストールされましたが、休止状態だったため使用されませんでした。今回のリリースでは、MSI はまったくインストールされません。

2019 年 9 月 - v2.1

2019 年 9 月よりも前からクラウド接続されたポッドを使用していて、新しい機能が操作性に与える影響について確認する必要がある場合は、次の情報を使用してください。

既存のクラウド接続された Horizon ポッドの場合

このリリース以降：

- Cloud Connector バージョン 1.3 および 1.4 で自動更新がサポートされるようになりました。この機能を利用するには、以前のバージョンの Cloud Connector を最新のバージョンに更新することをお勧めします。
- セッションの使用率が詳細にわかるクラウド監視サービス (CMS) 機能が Horizon Cloud Service に含まれています。

Microsoft Azure の既存のポッドの場合

以下の新機能を既存のポッドで使用するには、特に記載されていない限り、そのポッドを最初にマニフェスト 1600.0 以降に更新して機能を利用する必要があります。

- 今回のリリースでポッド アーキテクチャが変更されました。2019 年 9 月リリースのマニフェスト バージョンのすべてのポッドには、ポッドの Microsoft Azure ロード バランサと Microsoft Azure Database for PostgreSQL サーバ インスタンス (第 5 世代のメモリ最適化ティア) が含まれます。このため、既存のポッドをこのリリースのマニフェスト バージョンに更新する前に、既存のネットワーク構成が、ポッドの Microsoft Azure ロード バランサと Microsoft Azure Database for PostgreSQL サーバ インスタンスに対応するために必要な DNS、ポート、およびプロトコルを満たしていることを確認する必要があります。特定のポートおよびプロトコルをブロックするファイアウォールまたはネットワーク セキュリティ グループがある場合は、現在のネットワーク構成を次のトピックの情報と比較し、必要に応じてネットワーク構成を更新します。
 - [Microsoft Azure での Horizon Cloud ポッドの DNS の要件](#)
 - [2019 年 9 月のリリースのマニフェスト レベルでの Horizon Cloud ポッドのポートとプロトコルの要件](#)

- このリリースでは、解決のためにユーザーのアクションが必要なポッドの更新エラーのアラートが強化されています。ユーザーが完全に制御できるいくつかの要素により、ポッドの正常な更新が妨げられる可能性があります。たとえば、ポッドの更新を調整するジャンプ ボックス仮想マシンを作成するために、十分なコア数がポッドの関連付けられたサブスクリプションにない、というような状況が該当します。このリリース以降、このような問題はコンソールで特定されるため、これらの問題に対処して解消することができます。
- このリリース以降、すでにデプロイ済みのポッドで、2 要素認証設定を持たないゲートウェイにその設定を追加、ゲートウェイの 2 要素認証設定の編集、ゲートウェイのセッション仲介のタイムアウト設定の変更などの、ゲートウェイ関連設定の修正を行うことができます。以前のリリースでは、ポッドが最初にデプロイされたときに RADIUS 2 要素認証を構成する必要があり、後でそれらの設定を変更することができませんでした。また、このリリースでは、すでにデプロイされたポッドからゲートウェイを削除したり、Azure ロード バランサ上にパブリック IP アドレスではなく、代わりにプライベート IP アドレスを持つ外部ゲートウェイを使用するように新しいポッドをデプロイすることができます。
- Horizon Cloud on Microsoft Azure の新しい専用/フローティング VDI デスクトップ割り当てまたは新しいファームを作成するときの Microsoft Azure リソース タグの定義をサポートします。
- 高可用性が利用できるようになりました。Microsoft Azure でのポッドの高可用性をサポートするため、ポッド アーキテクチャは、Microsoft Azure Database for PostgreSQL サービス (更新された第 5 世代のメモリ最適化ティア)、Microsoft Azure ロード バランサ、および可用性セットを使用するように更新されています。このリリースで新しくデプロイされるポッドの場合、デプロイ時にそのポッドの高可用性を有効にするか、後で有効にするかを選択できます。このリリースより前に存在していたポッドについては、高可用性のためにこれらのポッドを有効にする前に、最初にそれらを 1600.0 マニフェスト以降に更新すること、およびポッドのイメージ、ファーム、および VDI デスクトップ割り当てのエージェントをこのリリースのレベルに更新することが必要となります。ポッドの更新とエージェントの更新が完了すると、管理コンソールのポッドの詳細画面からポッドを編集して、ポッドの高可用性を有効にすることができます。この新機能を使用する場合、ユーザー作成のサブネットをポッドが使用しているときにポッドの管理サブネットで Microsoft.SQL サービス エンドポイントを有効にするための要件、およびポート 5432 のアウトバウンド アクセスを許可するための要件が、追加で発生します。

2019 年 9 月の時点で、この Microsoft Azure のポッドの高可用性 (HA) 機能は、Microsoft Azure の商用リージョン (標準グローバル リージョン) にデプロイされたポッドでのみサポートされます。ポッド HA 機能は現在、中国の Microsoft Azure、ドイツの Microsoft Azure、および Microsoft Azure Government (米国バージニア州政府、米国アリゾナ州政府、米国テキサス州政府) に展開されているポッドではサポートされていません。VMware チームは、上記のクラウド環境のポッドに対する HA 機能のサポートの追加に取り組んでいます。Microsoft Azure in China、Microsoft Azure Germany、Microsoft Azure Government の既存のポッドを HA なしで今回のリリースのマニフェストバージョンに更新する場合は、VMware の担当者にお問い合わせの上サポートを受けてください。

標準の Microsoft Azure グローバル リージョンの 1 つで既存のポッドをマニフェスト 1600 以降に更新する前に、新しいポッド アーキテクチャでは Microsoft Azure Database for PostgreSQL サービスが使用されているため、次の項目を確認する必要があります。

- ポッドがカスタム管理サブネットを使用している場合は、ポッドの更新プロセスの前に、Microsoft.SQL サービス エンドポイントをその管理サブネットに追加する必要があります。
[Microsoft Azure で Horizon Cloud ポッド用の既存のサブネットを使用する場合の手順を参照してください。](#)

- ファイアウォール ルールとネットワーク セキュリティ グループが、管理サブネットを介した Microsoft Azure PostgreSQL データベース サーバとのポッド通信を許可していることを確認する必要があります。Microsoft Azure での Horizon Cloud ポッドの DNS の要件の TCP ポート 5432 のエントリを参照してください。
- ポッドに関連付けられたサブスクリプションに、アプリケーションの登録と必要なサービス プリンシパルの作成の手順 8 にリストされているリソース プロバイダが含まれていることを確認します。
- Horizon Agent ペアリング プロセスの回復性を高めるために、このリリースでは DaaS Agent 機能の Horizon Agent への移行がさらに進展しています。DaaS Agent は Horizon Agent に組み込まれるようになりました。以前のリリースと同様、自動化されたイメージのインポート ワークフローと Horizon Agents Installer の手動インストールはどちらも、ゲスト OS に DaaS Agent の MSI をインストールしますが、このリリース以降、DaaS Agent は休止状態となり使用されません。ただし、DaaS Agent のサービスは、Windows サービスのリストに引き続き表示されます。そのサービスは開始しないでください。予期しない結果が発生する可能性があります。
- Horizon View Agent への DaaS Agent 機能の移行によって、Azure Marketplace からのイメージの自動インポートのワークフローと、ベース仮想マシンを手動で構築する手順の両方が変更されました。以前は、自動ワークフローの結果として生成されたベース仮想マシンがワークフローの終わりでクラウドとペアリングされました。手動で作成した仮想マシンの場合は、手動でのブートストラップと仮想マシンのペアリングが必要でした。現在は、新規またはこのリリース バージョンに更新されたポッド内のベース仮想マシンでは、結果として作成されたベース仮想マシンが [ペアなし] のエージェント ステータスで [インポートされた仮想マシン] 画面に表示されるようになりました。仮想マシンをペアリングするには、次のいずれかを実行します。
 - カスタマイズの前にクラウドとペアリングする場合は、[インポートされた仮想マシン] 画面にリストされている仮想マシンで [[エージェント ペアリングをリセット]] アクションを実行します。
 - 仮想マシンに必要なすべてのカスタマイズがあり、それを公開する準備ができている場合、仮想マシンで [新しいイメージ] アクションを直接実行します。この場合、[新しいイメージ] ワークフローは最初にペアリング プロセスを実行してエージェントをアクティブにします。その後、残りのフィールドに入力し、[公開] をクリックしてイメージを公開できます。
- Horizon View Agent への DaaS Agent 機能の移行により、インポートされた仮想マシン、ファーム サーバ仮想マシン、および専用 VDI デスクトップ割り当てのデスクトップ仮想マシンで、エージェント ペアリングをリセットするワークフローが使用できるようになりました。ファームの詳細または専用 VDI デスクトップ割り当ての詳細で、ファーム サーバ仮想マシンまたはデスクトップ仮想マシンの [エージェントのステータス] 列にエラー状態が表示される場合、コンソールで [エージェント ペアリングをリセット] アクションを使用して、その仮想マシンのペアリング状態を修復できます。(フローティング VDI デスクトップ割り当てでは、このアクションは使用できません。) [インポートされた仮想マシン] 画面では、[エージェント ペアリングをリセット] アクションを使用して、ペアリングされていない仮想マシンを最初にペアリングするか、以前にペアリングされた仮想マシンのペアリング状態を修復できます。
- ディスク暗号化機能は新しい AzureDiskEncryption v2.2 を使用するようになりました。この新しいバージョンでは、インターネットと通信するように設定されたゲスト内プロキシを使用して、仮想マシンのディスク暗号化をサポートできます。この新しいサポートを利用するには、仮想マシンのエージェントをバージョン 19.3.0 以降に更新します。

- ファームと VDI デスクトップ割り当てに最低でも 2 個の CPU が搭載された仮想マシンのモデルを使用するようにガイダンスを更新しました。VMware のスケール テストでは、本番環境において最低 2 個の CPU を使用することによって、予期しないエンドユーザー接続の問題を回避していることが示されています。システムによって、単一の CPU を搭載した仮想マシン モデルの選択が妨げられることはありませんが、このような仮想マシン モデルはテスト用または事前検証用에만使用する必要があります。
- [仮想マシンのタイプとサイズ] 画面の操作性が向上しました。

現在のユーザーに対する追加の注意事項

- Unified Dashboard のインタラクティブ マップ ビューの使いやすさと最適化が向上し、たとえばポッドの位置とズーム機能がより正確に反映されるようになりました。
- 管理コンソールの [レポート] 画面で利用可能なレポートの機能が拡張されました。これらのレポートのデータは、Cloud Monitoring Service によって提供されます。
- クラウドに接続された Horizon 7 ポッドの場合は、ポッドの詳細画面に追加の詳細が表示されます。この機能を表示するには、ポッドと Cloud Connector が最新バージョンである必要があります。
- 以前の製品名 VMware User Environment Manager™ は、VMware Dynamic Environment Manager™ という名前に変更されました。

第 1 世代テナント - VMware Horizon Cloud Service on Microsoft Azure サービスの制限

このトピックでは、サポートされる最大値とも呼ばれる第 1 世代 VMware Horizon Cloud Service on Microsoft Azure のいくつかの一般的な制限について説明します。このトピックは現在、単一のサブスクリプションでデプロイ可能なデスクトップおよびファーム RDSH 仮想マシンの数と、第 1 世代 Horizon Cloud ポッドごとの同時実行される接続セッションの合計数の両方について、サポートされる最大値を記載しています。時間の経過とともにこのトピックは更新され、既知の制限が追加されます。

重要: この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

これらのサポートされている最大値は、これらの最大値までのサービスをテストした結果です。

サブスクリプションあたり最大 2,000 のデスクトップ仮想マシンとファーム RDSH 仮想マシン

この制限は、単一のサブスクリプションに対して適用される Microsoft Azure API の制限に基づいています。標準の操作でこれらの API 制限を守るため、Horizon Cloud はサブスクリプションあたり最大 2,000 のデスクトップ仮想マシンとファーム RDSH 仮想マシンをサポートします。

サブスクリプションあたり 2,000 という制限には、VDI デスクトップ仮想マシンとファーム RDSH 仮想マシンが含まれ、単一のサブスクリプションのすべてのポッドが対象です。たとえば、サブスクリプションに1つのポッドがある場合、そのポッドに最大 2,000 の VDI デスクトップを接続することも、1,950 の VDI デスクトップと 50 のファーム RDSH 仮想マシンを接続することもできます。サブスクリプションに複数のポッドがある場合でも、すべてのポッドに接続された VDI デスクトップとファーム RDSH 仮想マシンの数は合計で 2,000 を超えることはできません。

Horizon Cloud ポッドあたりの同時接続セッションの最大数

各 Horizon Cloud ポッドは最大 2,000 のアクティブな同時セッションをサポートできます。この数には、Windows クライアント タイプのオペレーティング システムを使用する VDI 単一セッション デスクトップ、Windows 10 または 11 Enterprise マルチセッションまたは Windows 11 Enterprise マルチセッションを使用するマルチセッション デスクトップ、Windows Server オペレーティング システムに基づくマルチセッション デスクトップ、およびポッドによって提供される RDS ベースのアプリケーションへの個々の接続が含まれます。

たとえば、ポッドに 400 台の VDI 単一セッション デスクトップへのアクティブなユーザー セッションが 400 あり、Windows 10 または 11 マルチセッション マシンへのアクティブなユーザー セッションが 1,500 あり、Windows Server 2016 マルチセッション マシンへのアクティブなユーザー セッションが 100 ある場合、ポッドの最大値の 2,000 ($400 + 1500 + 100 = 2,000$) に達します。

1つのポッドでは、2,000 を超えるアクティブ セッションはサポートされません。

また、ポッドが Unified Access Gateway 構成を使用するように設定されている場合、この 2,000 という数は、F8s_v2 仮想マシン モデルが Unified Access Gateway アプライアンスで使用される場合のみサポートされます。

- F8s_v2 仮想マシン モデルが Unified Access Gateway アプライアンスに使用されている場合、ポッドは最大 2,000 のセッションをサポートできます。環境内の使用量が、ポッドで 1,000 を超えるアクティブ セッションになると予測される場合は、ゲートウェイのデプロイ ウィザードで F8s_v2 仮想マシン モデルを指定する必要があります。
- A4_v2 仮想マシン モデルが Unified Access Gateway アプライアンスに使用されている場合、ポッドは最大 1,000 のアクティブ セッションのみをサポートできます。この選択が十分に機能するのは、ポッドでのアクティブ 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。

Unified Access Gateway アプライアンスのリソース使用率は、セッション内のユーザー アクティビティに依存し、ユーザー プロファイルやユーザーのタイプによって異なる場合があります。

VDI マルチクラウド割り当てあたりの Horizon Cloud ポッドの最大数

1つの VDI マルチクラウド割り当てでサポートされる Horizon Cloud ポッドの最大数は 5 です。5 つを超えると、VDI マルチクラウド割り当てで使用するためにテナント環境で構成される仲介テクノロジーである、Universal Broker の同時負荷が増大します。同時負荷が増大することによって、エンド ユーザーがクライアントで割り当ての表示タイルをクリックして、サービスがそのユーザーを仮想デスクトップにログインさせようとするときに、エラーが発生する可能性があります。

VDI マルチクラウド割り当てごとに 5 つのポッドの上限に従うだけでなく、VDI マルチクラウド割り当てに追加で 3% 分のデスクトップ キャパシティを含めるようにすることで、クライアントで割り当ての表示タイルをクリックした際にエンド ユーザーに障害が発生する可能性をさらに減らすことができます。たとえば、1,000 台の仮想デスクトップを 1,000 ユーザーにプロビジョニングするための VDI マルチクラウド割り当てを定義する場合は、割り当てのサイズを 1,030 台のデスクトップに設定します。

第1世代テナント - Horizon Cloud - Active Directory ドメイン構成

Horizon Cloud 環境では、少なくとも 1 つの Active Directory (AD) ドメインを Horizon Cloud ポッドに登録する必要があります。このトピックでは、Microsoft Azure の Horizon Cloud ポッドでの使用がサポートされている構成について説明します。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、[該当記事を参照してください](#)。

サポートされる構成は以下のとおりです。

- オンプレミスの Active Directory サーバと、VPN/MPLS または Microsoft Azure Express Route を使用したそのオンプレミス Active Directory と Microsoft Azure 環境との接続。
- Microsoft Azure 環境で実行する Active Directory サーバ。
- Microsoft Azure の Active Directory ドメイン サービスの使用。Microsoft Azure が提供するこれらのサービスの概要については、Microsoft のドキュメントでこの [Azure Active Directory ドメイン サービスの記事](#)を参照してください。

サポートされている各構成の技術的な詳細説明や、各構成のいくつかのオプション、および各構成のメリットとデメリットについては、VMware のテクニカル ペーパー『[VMware Horizon Cloud を使用した Microsoft Azure でのネットワークおよび Active Directory についての考慮事項](#)』を参照してください。

重要： クラウド接続されたポッドのフリートは、Microsoft Azure の Horizon Cloud ポッドと、VMware SDDC (Software-Defined Data Center) にインストールされている Horizon ポッドで構成できます。VMware SDDC はそのようなポッドでサポートされている必要があります。そのため、クラウド接続されたすべてのポッドは、同じ Active Directory ドメインのセットとの通信路を確立している必要があります。ポッドのフリートがすでにクラウド接続された Horizon ポッドで構成され、最初の Horizon Cloud ポッドを Microsoft Azure にデプロイしている場合は、そのポッドがすでに Horizon Cloud 環境に登録されている Active Directory ドメインを認識できることを確認する必要があります。詳細については、[Horizon Cloud 環境の使用を開始する](#)のトピックからリンクされたすべての Active Directory 関連のトピックを参照してください。

第1世代 Horizon Cloud - 既知の制限事項

第1世代 Horizon Cloud を使用して最高の結果を得ることができるよう、次の既知の制限に注意してください。

重要: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

すべてのデプロイ タイプ

- Horizon Cloud テナントに関連付けられ、Horizon Cloud に接続されているすべてのポッドは、同じ Active Directory ドメインのセットに対する見直しを持つ必要があります。テナントのポッド フリットにポッド タイプの組み合わせ (Horizon 8 タイプと Horizon Cloud タイプの両方など) がある場合は、この見直しの要件に加えて、同じ Horizon Cloud テナントに登録されているすべてのドメイン間で一方の信頼または双方の信頼が必要です。

注: この場合の見直しは、特定のポッドがステータス チェックのためにそのドメインにアクセスできるように、各ドメインへのネットワーク アクセスが必要であることを意味します。

- システムは、使用率、同時実行、セッション履歴、および上位アプリケーション レポートのデータを、1日に一度、指定の UTC 時間に取得します。使用率および同時実行レポートのデータは午前 2 時、セッション履歴レポートのデータは午前 2 時 10 分、上位アプリケーション レポートのデータは午前 2 時 30 分 (いずれも UTC) に取得されます。その結果、管理コンソールに表示されるレポート情報には、前回取得した時間からコンソールでレポートを表示している時間までの間に収集されたデータが反映されないことがあります。たとえば、同時実行レポートのユーザーおよびピーク時の同時実行データのロジックはデータの取得日単位で計算されるため、4月23日のユーザー アクティビティのデータは、4月24日 (翌日) の午前 2 時 (UTC) の時点で計算されます。その時点が過ぎた後、システムが収集されたデータを取得すると、レポートには 4月23日のデータが表示されます。エンド ユーザーの1人が4月23日の午前 2 時 (UTC) 以降にセッションを開始した場合、そのユーザーのセッションのデータは4月24日の午前 2 時 (UTC) が過ぎるまで画面のレポートに反映されません。

デプロイ - Microsoft Azure の Horizon Cloud ポッド

Horizon Cloud ポッドは、Horizon Cloud ポッド マネージャ テクノロジー上に構築されたタイプです。

- Microsoft Azure VNet では、同時にサブネットの作成および削除操作を処理する仕組みに制限があるため、同じ VNet を同時に変更する必要があるポッド関連の同時操作を実行すると、それらの操作を完了できなくなる場合があります。この問題が発生しないようにするには、サブネットが関与するポッドのデプロイ、ポッドの削除、またはポッドの編集操作をそれらのポッドが同じ VNet を使用しているときに同時に実行しないようにします。以下に、VNet の変更を伴うポッド関連の同時操作の例をいくつか示します。これらの操作では、VNet で同時サブネット アクションが発生する可能性があり、その結果、操作を完了できません。
 - 事前にサブネットを作成せずに、ポッド デプロイヤーが CIDR を使用してサブネットを作成し、同じ VNet 上で 2 つのポッドの作成を同時に開始します。これらのサブネットは、両方のポッドの作成で同時に VNet に追加されます。
 - 1 つのポッドのデプロイ中に、同じ VNet で別のポッドの削除を開始します。サブネットは、他のポッドのサブネットが同じ VNet から削除されると同時に、デプロイするポッドの VNet に追加されます。

- 別のポッドの削除が進行しているときに、ポッドを編集して、CIDR ブロックを使用してポッドの VNet に外部ゲートウェイ構成を追加します。サブネットは、他のポッドのサブネットが VNet から削除されると同時に、ゲートウェイ構成の VNet に追加されます。
- ポッドのデプロイ後に、ポッドのサブネットのサイズを拡張することは現在サポートされていません。ポッドをデプロイする前に、デプロイ ウィザードで指定するサブネットのアドレス空間で、想定される使用状況に対応できる十分な容量が確保されることを確認する必要があります。

注： この制限を回避するために、マニフェスト 2298.0 以降のポッドで利用できるようになった新機能では、ポッドがデプロイされた後、テナント サブネットを追加してファームと VDI デスクトップ割り当てで使用することができます。この機能により、ポッドのデプロイ後にファームとデスクトップ仮想マシンで使用するために、ポッドの同じ VNet またはピアリングされた VNet にあるテナント サブネットを柔軟に追加できます。詳細については、『[管理ガイド](#)』を参照してください。

- 複数のポッドが、Unified Access Gateway 構成に使用されている同一の完全修飾ドメイン名を共有することはできません。Unified Access Gateway インスタンスで構成された各ポッドはその固有の完全修飾ドメイン名 (FQDN) を必要とします。FQDN にアンダースコアを含めることはできません。

注： 2020 年 12 月 15 日時点のクラウド プレーンの更新では、ポッドの外部ゲートウェイと内部ゲートウェイの構成で異なる FQDN を使用することがサポートされます。2020 年 12 月 15 日以前は、システムにより強制的にマニフェスト 2298 以降のポッドに同じ FQDN を使用するようになっていました。ユーザーは現在、ポッドのゲートウェイで異なる FQDN を使用するか、同じ FQDN を使用するかを任意に選択できるようになりました。両方のゲートウェイで同じ FQDN を使用する場合は、ポッドのデプロイ後、スプリット DNS (スプリット Domain Name System) を構成して、エンド ユーザー クライアントの DNS クエリのオリジン ネットワークに応じて、外部ゲートウェイまたは内部ゲートウェイのいずれかにゲートウェイ アドレスを解決します。次に、エンド ユーザー クライアントで使用されているのと同じ FQDN で、クライアントがインターネット上にある場合は外部ゲートウェイにルーティングし、クライアントが内部ネットワーク上にある場合は内部ゲートウェイにルーティングできます。

- ポッドが Microsoft Azure にデプロイされた後にポッドのプロキシ設定を編集または更新することは、現在サポートされていません。また、プロキシ設定なしでデプロイされたデプロイ済みポッドにプロキシ構成を追加することは、現在サポートされていません。
- このリリースの NSX Cloud 機能は Microsoft Windows Server 2019 ではサポートされていません。
- 以前にデプロイされた Horizon Cloud ポッドに True SSO をすでに設定した後に Microsoft Azure で Horizon Cloud ポッドをデプロイする場合、システムによって新しいポッドが登録サーバと自動的にピアリングされることはありません。手動でピアリング バンドルをエクスポートして登録サーバにインポートする手順を繰り返す必要があります。手順については、[Horizon Cloud 環境で使用するための True SSO の構成](#)およびそのサブトピックを参照してください。
- ファーム、イメージ、および割り当ての作成など、システムで仮想マシンが作成されるワークフローでは、作成するアイテムに対してシステムでサポートされる長さを超える名前を入力しようとすると、システムはサポートされる文字数を超える文字の入力を受け付けません。サポートされるアイテムの名前の文字数は、ワークフローによって異なります。
- Microsoft Azure の複数ポッド環境では、1 つのポッドに使用した名前は、別のポッドでアイテムを作成する際に再使用することはできません。その理由は、複数ポッド環境のポッドが、同じ Active Directory ドメイン

および同じ VNet を共有するためです。そのような複数ポッド環境で名前が共有されると、予期しない動作が発生することがあります。この制限が適用されるのは、イメージ、ファーム、および VDI デスクトップ割り当ての名前です。イメージ、ファーム、および VDI デスクトップ割り当てには一意の名前が使用されるようにしてください。

- 管理コンソールで文字を入力するときは、次のルールに従います。
 - ユーザー名とパスワードの入力、および DaaS SSL ブートストラップ ファイルをダウンロードするためのパスワードの入力には、標準の ASCII 文字のみを使用します。これらの項目に ASCII 以外の文字を使用すると、予期しない結果が発生する可能性があります。
 - インポートしたイメージ、ファーム、割り当てなど、Microsoft Azure で仮想マシンを作成する際に使用するアセットの名前を入力するときは、12 文字を超える名前を入力しないでください。
 - ユーザー パスワードにはコンマを使用しないでください。
 - [仮想マシンのインポート] ウィザードを使用して Microsoft Azure Marketplace から基本イメージ仮想マシンを作成する場合：
 - 仮想マシンの管理者ユーザー名とパスワードに対する Microsoft Azure 要件に従ってユーザー名とパスワードを入力します。詳細については、[「Microsoft Azure FAQ のページ」](#)を参照してください。
 - 最後の文字がハイフン (-) のイメージ名を入力しないでください。
 - イメージ名にアンダースコア文字 (_) を含めないでください。

Microsoft Azure の Horizon Cloud ポッドの更新

- ポッドを以前のソフトウェア レベルから最新のレベルにアップデートする処理中に、エンド ユーザーがセッションをアップデートしているノードに接続している場合は、それらのアクティブなセッションを切断することになります。セッションをサービスしている RDSH ファームまたは VDI デスクトップ割り当てで [切断済みセッションのログオフ] を [ただちに] に設定している場合を除いて、データが失われることはありません。そのようなファームおよび VDI デスクトップ割り当てでは、切断されたセッションもただちにログオフされ、そのような状況で進行中のユーザーの作業も失われます。アップデート処理の完了後、それらのユーザーは再接続できます。ポッドの更新プロセスにかかる時間は、通常、30 分未満です。ただし、一部のポッドの更新には、これよりも時間がかかることがあります。
- 2020 年 10 月リリースの 2474 以前のマニフェストでポッドを実行していて、2474 以降に更新されたときに、Microsoft Azure ポータルを使用して、サブスクリプション内の Horizon Cloud によって作成されたリソースまたはリソース グループに直接タグを手動で追加した場合、たとえばファームまたは VDI デスクトップ割り当てのリソース グループにカスタム タグを作成した場合、これらのポッドが更新されると、ポッドの更新プロセスでは、Microsoft Azure ポータルを使用して直接追加したカスタム タグが保持されません。これらのカスタム タグは削除されます。ポッドを更新した後は、Horizon Universal Console 機能を使用してファームと VDI デスクトップ割り当てを編集し、システムによってそれらのファームと VDI デスクトップ割り当てのリソース グループにこれらのタグが適用されるようにする必要があります。コンソールの [Azure リソース タ

グ]機能の使用は、ファームおよび VDI デスクトップ割り当てのためにポッドで作成されたリソース グループにリソース タグを追加する方法としてサポートされています。次の各ドキュメント トピックで、[Azure リソース タグ] フィールドの説明をお読みください。ファームまたは VDI デスクトップ割り当てを編集するときに同じフィールドが使用されます。

- [ファームの作成](#)
- [Microsoft Azure のシングル ポッドによってプロビジョニングされる専用 VDI デスクトップ割り当ての作成](#)
- [Microsoft Azure のシングル ポッドによってプロビジョニングされるフローティング VDI デスクトップ割り当ての作成](#)
- [Microsoft Azure の Horizon Cloud ポッド - Horizon Cloud テナント環境での VDI マルチクラウド割り当ての作成](#)

インポートされた仮想マシン、ゴールド イメージ、ファーム、または VDI デスクトップ割り当て - Microsoft Azure の Horizon Cloud ポッド

- コンソールでは、コンソールのワークフローで Azure Marketplace 以外のオリジンから取得したイメージを使用することはできますが、そのようなイメージの使用はサポートされていません。Horizon Cloud on Microsoft Azure で使用できるようにするには、インポートされたすべての基本イメージを、Azure Marketplace をソースとする Windows ベースの仮想マシンから構築する必要があります。他のオリジンから取得したイメージを試し、コンソールがコンソール ワークフロー内でのイメージの使用を妨げない場合でも、そのような画像の使用はサポートされていません。

また、Windows 11 イメージの場合は、Azure Marketplace から直接提供される必要があり、後で処理することはできません。共有イメージ ギャラリー (SIG)、Azure 管理対象イメージ、Azure 仮想マシン スナップショットなど、その他のソースからの Windows 11 仮想マシンのインポートは現在サポートされていません。

- 現在、第 2 世代の Azure 仮想マシンは、Windows 11 単一セッション オペレーティング システムおよび Windows 11 Enterprise マルチセッション オペレーティング システムでのみ使用できます。
- 現在、AMD Radeon Instinct グラフィックス ドライバを使用する Azure GPU 対応の NVv4 仮想マシンは、カスタム インポート方法を使用してインポートされた場合にのみ使用できます。カスタム インポート方法は、このドキュメントでは手動インポートとも呼ばれます。自動化された [Marketplace からの仮想マシンのインポート] ウィザードでは、この機能は現在提供されていません。

また、このサービスは現在、これらの NVv4 仮想マシンおよび AMD Radeon Instinct グラフィックス ドライバでの Windows 11 の使用をサポートしていません。この使用は認定されていません。

- サービスの Windows 11 のサポートには、既知の考慮事項、制限事項、および問題があります。これらの詳細については、[Windows 11 ゲスト OS のサポート - 考慮事項、既知の制限、および既知の問題](#)を参照してください。
- Windows 10 バージョン 2004、Windows 10 バージョン 20H2、Windows Server バージョン 2004、または Windows Server バージョン 20H2 を実行しているイメージに基づいて、セッション デスクトップ、リモート アプリケーション、または VDI デスクトップで True SSO を使用するには、これらのオペレーティ

ングシステムに Microsoft パッチをインストールする必要があります。このパッチは、True SSO がこれらのオペレーティングシステムで認証されるのをブロックする Microsoft の問題を修正します。詳細については、Microsoft Update KB 4598291 を参照する [VMware のナレッジベース記事 KB79644](#) を参照してください。

- Microsoft Azure Government クラウドのポッドでは、ファームおよび VDI デスクトップ割り当てへのディスク暗号化機能の使用は現在サポートされていません。
- 現在、VMware Logon Monitor サービスという Horizon Agent 機能の使用はサポートされていません。デフォルトでは、Horizon Agents Installer により、インストーラがデフォルトで実行するすべてのインストールで VMware Logon Monitor サービスが無効になります。
- VMware Horizon Client for Android を使用して Horizon Cloud 環境により提供される仮想デスクトップとリモート アプリケーションにアクセスする場合、USB リダイレクト機能はサポートされません。
- サーバタイプのオペレーティングシステムに基づく GPU 対応のゴールド イメージに対しては、エンド ユーザー セッションの数が制限されないように、Microsoft Windows Server バージョン 2016 および 2019 を使用することをお勧めします。Windows Server 2012 R2 に対する NVIDIA ドライバの制限により、RDS デスクトップ サーバごとの最大セッション数は 20 です。
- Microsoft Windows 10 1709 (RS3) を使用しているイメージがあり、それを Windows 10 1803 (RS4) または Windows 10 1809 (RS5) にアップデートする場合は、まず Windows 10 1709 を最新の Horizon Agent バージョン 19.4 にアップグレードし、その後 Windows オペレーティングシステムをアップグレードします。
- デフォルトでは、Windows Server 2012 オペレーティングシステムを持つイメージの作成で自動化された [Marketplace からの仮想マシンのインポート] ウィザードを使用する場合、結果として生成されるイメージでは Desktop Experience が有効にされていません。結果として生成されるイメージに Desktop Experience を表示するには、結果として生成されるイメージで Desktop Experience を手動で有効にする必要があります。
- デスクトップのイメージへの変換を開始しても、タスクが終了する前にキャンセルした場合、再度デスクトップをイメージに変換すると失敗することがあります。この問題を回避するには、デスクトップをパワーオフして、再度パワーオンしてから、もう一度イメージに変換してください。
- URL リダイレクトのカスタマイズでは、Horizon Client によって URL パターンが受信されるときに大文字と小文字が区別されます。たとえば、パターン *google.com がリダイレクトされるとしても、*GOOGLE.com および *Google.com として指定された URL パターンに対しては URL リダイレクトは発生しません。指定されたパターンがターゲット ファイル システムで実際に使用されている大文字と小文字のパターンに一致しない場合、エンド ユーザーのリダイレクトは発生しません。

デプロイ - Horizon ポッド

Horizon ポッドは、Horizon Connection Server ソフトウェアに基づくタイプです。Horizon ポッドで使用されるさまざまなデプロイ アーキテクチャの背景情報については、[第1世代テナント - 第1世代 Horizon Cloud を使用した Horizon ポッドのデプロイ アーキテクチャ](#)を参照してください。さまざまなクラウドプレーン サービスの詳細については、[管理ガイド](#)を参照してください。

現在のリリースでは次の制限が適用され、Horizon Cloud Service のリリースごとに該当する場合は更新されません。

- Horizon Cloud Connector の自動更新機能は、オンプレミスでデプロイされた Horizon ポッドでのみサポートされます。クラウド環境にデプロイされた Horizon ポッドとペアリングされた Horizon Cloud Connector インスタンスを更新するには、[Horizon Cloud Connector 仮想アプライアンスの手動更新の手順](#)に従います。
- Horizon Image Management Service (IMS) は現在、VMware Tech Zone の『Horizon リファレンス アーキテクチャ』で説明されている Horizon デプロイ モデルのサブセットでのみ使用できます。IMS で現在サポートされている特定のデプロイ モデルの詳細については、[IMS システム要件](#)を参照してください。『Horizon リファレンス アーキテクチャ』のより多くのモデルが IMS サポートの対象になるにつれて、新しくサポートされたモデルがリストに追加されます。

Workspace ONE Hub サービスと Universal Broker - 統合

- この機能は VMware Workspace ONE[®] Access[™] Cloud でのみ使用できます。オンプレミスの VMware Workspace ONE Access ではサポートされません。
- この統合により、エンド ユーザーは Hub カタログから Horizon Cloud 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。[Workspace ONE Access : Horizon Cloud との統合のための Intelligent Hub の構成](#)の説明に従って、VMware Workspace ONE[®] Intelligent Hub に必要な設定を構成していることを確認します。
- このリリースでは、この統合はブラウザベースの Hub カタログ、Workspace ONE Intelligent Hub for Windows、および Workspace ONE Intelligent Hub for macOS のクライアントを使用したエンドユーザー アクセスをサポートします。このサポートに必要な Windows および macOS デスクトップ アプリケーションの最小バージョンは 21.05 です。
- 新しい Workspace ONE Access テナントでは、パスワードのキャッシュはデフォルトでオンになっていません。Horizon 環境で True SSO が有効になっていない場合、パスワードのキャッシュを有効にして、ユーザーのパスワードをキャッシュすることができます。これにより、Horizon Cloud デスクトップとアプリケーションの起動時にパスワードを再入力する必要がなくなります。詳細については、[仮想アプリケーションのパスワードキャッシュを構成する \(Workspace ONE Access クラウドのみ\)](#)を参照してください。
- Workspace ONE Access で設定したアクセス ポリシーは、Universal Broker が有効になっている Horizon Cloud 環境からアプリケーションやデスクトップには適用されません。
- 同じ物理クライアント エンドポイント上の複数のクライアントで同時に複数のエンドユーザー セッションを起動することはサポートされていません。つまり、エンドユーザーは、割り当てが専用デスクトップ割り当てかフローティング VDI デスクトップ割り当てかに関係なく、割り当てられた複数の仮想デスクトップまたはリモートアプリケーションに対して、物理クライアント エンドポイントごとに複数のセッションを起動できません。たとえば、システムは、1 台の物理クライアント システムを 2 台のモニターに並べて接続し、その同じクライアント システムから 2 つの個別の仮想デスクトップ セッションを同時に実行して、1 台のデスクトップを 1 台のモニターに表示し、もう 1 台のデスクトップを別の 1 台のモニターに表示するといったエンドユーザー エクスペリエンスを実行できません。この制限は、設計どおりのシステムの動作です。

Horizon Universal Console - 関連する注意点と制限事項

- コンソールは、割り当ての詳細ですでに指定されている Active Directory ユーザーおよびグループの現在の有効な名前を取得しません。Active Directory でユーザーまたはグループの名前を変更すると、コンソールの割り当ての詳細には、ユーザーまたはグループの以前の名前が引き続き表示されます。これは、ユーザーまたはグループが最初に割り当てに追加されたときの名前です。割り当てを編集し、検索フィールドでユーザーまたはグループを検索すると、ユーザーまたはグループの現在の有効な名前がコンソールに表示されます。ただし、更新された割り当てを保存した後も、割り当ての詳細には初期の古い名前が表示されたままになります。この制限による機能上の影響はありません。
- Web ベースの管理コンソールは Apple Safari ブラウザでサポートされていません。一部のユーザー インターフェイスが正常に機能しない場合があります。Mac OS では、Apple Safari の代わりに Chrome または Firefox ブラウザを使用できます。
- コンソールへの認証された（ログイン）セッションは、コンソールの [全般設定] 画面で設定された時間が経過するとタイムアウトになります。デフォルトは 30 分です。クラウド接続されたポッドが1つ以上ある場合は、デフォルトの設定を 30 分から 180 分までの値に変更できます。ほとんどの場合、構成された時間が経過すると、システムはユーザーを明示的に自動でログアウトし、再度ログインする必要があるというメッセージを表示します。ただし、システムが認証済みのセッションを終了したときに、ユーザーが明示的にログアウトされない場合があります。この場合は、コンソールで特定のタスクを実行するときに、現在の状態を正確に反映していないエラー メッセージが表示される可能性があります。たとえば、ノードのデプロイ ウィザードがサブスクリプション エントリの検証に失敗する、ドロップダウン メニューに値が表示されない、あるいはファームを作成するために利用できるノードがないというファーム ページのレポートや、「タイプ identity_node の service_sessions が提供されていません」というようなエラー メッセージが表示されます。このようなメッセージが表示され始め、コンソールを 30 分以上使用している場合は、手動でログアウトして再度ログインしてください。

第1世代テナント - Horizon Cloud - 既知の問題

このトピックでは、サービスの使用時に発生する可能性のある既知の問題および既知の回避策（ある場合）を示します。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

このドキュメントのトピックでは、Horizon Cloud Connector の既知の問題について説明します。ただし、Horizon Cloud Connector を使用して Horizon ポッドを Horizon Cloud に接続する場合でも、これらの Horizon ポッド内で実行されているソフトウェアの既知の問題については、ポッドの Connection Server のソフトウェア バージョンに応じて、次の場所にあるリリース ノートを参照してください。

- バージョン 7.13 - [Horizon 7 のドキュメント](#)で入手できます。
- VMware Horizon 8 バージョン - [Horizon のドキュメント](#)で入手できます。

すべての Horizon Cloud のユーザーが本番環境で利用できる Image Management Service (IMS) 機能に関連する IMS の既知の問題については、『[Cloud からの Horizon イメージの管理](#)』の既知の問題のページを参照してください。

注： それぞれの既知の問題の末尾に記載された括弧内の数字は、VMware 内部の問題追跡システムに関連します。

ログインに関する既知の問題

バックスラッシュ (\) を含む My VMware アカウントのパスワードを正常に作成した場合でも、これらの認証情報を使用した Horizon Cloud へのログインが失敗する (2595757)

My VMware の認証情報を使用して Horizon Cloud にログインする場合、バックスラッシュを含むパスワードはサポートされません。サポートされている特殊文字の一覧を表示するには、my.vmware.com にログインし、プロファイルの [パスワードの変更] セクションに移動します。このページには、サポートされている特殊文字が表示されます。回避策：My VMware アカウントのパスワードを新しいパスワードにリセットし、新しいパスワードにバックスラッシュ (\) が含まれていないことを確認します。

Active Directory に関する既知の問題

管理コンソールで Active Directory に関連する操作を行わない限りプライマリ バインド アカウントのロックアウトが検出されない。(2010669)

この問題により、Web ベースの管理コンソールにログインした管理者は、ユーザーを割り当てに追加するために Active Directory を検索するなどの、Active Directory に関連する操作をユーザー インターフェイスで実行するまで、プライマリ バインド アカウントのロックアウト通知が表示されません。基盤となるサービスがロックアウトされたサービス アカウントを検出するのは、(ユーザーまたはグループを) 認証または検索するために Active Directory との対話を要求するときのみです。回避策：なし。

Web ベースの管理コンソールがプライマリ ドメイン バインド アカウントのロックアウトまたはロック解除された状態を反映するのに最大 15 分かかる(2009434)

Active Directory へのシステムの接続オブジェクトは 15 分間キャッシュされます。この結果、プライマリ バインド アカウントがロックされてからシステムが管理者へ通知するまで 15 分かかる可能性があります。また、管理者がアカウントのロックアウト状態をクリアした後、システムがそのクリア済みのアカウントについての通知を停止するまでも、15 分かかる可能性があります。回避策：なし。

Microsoft Azure のポッド内のファームでは、同じ Active Directory フォレスト内の別のドメインと同じファーム名を再使用すると、重複するサービス プロバイダ名 (SPN) が原因でドメイン参加が失敗する可能性がある (1969172)

Microsoft Windows Server 2012 R2 以降でのドメイン コントローラの新機能により、ドメイン コントローラでの重複する SPN チェックが原因でドメイン参加が失敗します。Microsoft のナレッジベースの記事 [KB3070083](#) を参照してください。回避策：

- ファーム名を再使用しないようにします。

- Microsoft のナレッジベースの記事の説明に従って、Active Directory ドメインでの重複する SPN チェックを無効にします。

Azure AD Domain Services を使用している場合、Active Directory の登録ワークフローはドメインへの参加ステップで失敗し、パスワードのリセット権限がないというエラーが発生します。(2218180)

Horizon Cloud チームは、ポッドで Azure Active Directory (AD) ドメイン サービスを使用するときに、他の Active Directory ドメインのデプロイのときと同じように、必要なドメイン参加アカウント権限を追加できることを確認しました。組み込みコンテナ AADDC コンピュータについて説明した Microsoft のドキュメントトピック [Azure AD Domain Services のマネージド ドメインに組織単位 \(OU\) を作成する](#) を参照してください。また、このトピックの冒頭の、Azure AD Domain Services とのパスワード ハッシュ同期の有効化に関する重要な注意事項も参照してください。ドメイン参加サービス アカウントの権限を設定する前に、ドメイン参加サービス アカウントの Azure AD Domain Services へのパスワード ハッシュ同期の有効化に関する Microsoft のドキュメントに従うことが重要です。Microsoft のドキュメントに従っても Active Directory の登録ワークフローでドメイン参加権限エラーが発生する場合は、VMware サポートに連絡し、問題レポート番号 2218180 について問い合わせてください。

Microsoft Azure サブスクリプションに関連する既知の問題

Horizon Universal Console を使用してポッドの Azure サブスクリプション設定のプライベート キーを更新した後、新しい認証情報を有効にするにはポッド マネージャ仮想マシンを再起動する必要がある (2979394、3007687、3017415)

この既知の問題により、コンソールの [サブスクリプションの管理] ウィンドウで [アプリケーション キー] 設定を編集して保存した後、仮想マシンのオペレーティング システムで管理サービスが再開されるまで、新しく入力したプライベート キーがポッド マネージャ仮想マシンで有効になりません。管理サービスが再起動されない場合、サービスがサブスクリプション内のリソースを操作するために使用する API 呼び出しが失敗し始めます。回避策：ポッドのサブスクリプション プライベート キーを何らかの理由（有効期限が近づいている、または有効期限が切れているなど）で更新する必要がある場合、サービス リクエストを開いて、VMware のサポートと Horizon Cloud オペレーション チームの支援を受け、一連の手順が正常に完了するようにします。概要レベルでは、手順は次のとおりです。

- 1 Azure ポータルで、新しいプライベート キーを生成します。
- 2 Horizon Universal Console で、[デプロイされた Horizon Cloud ポッドに関連付けられたサブスクリプション情報の変更、修正、更新](#) ページの説明に従って、標準の手順に従って、古いキーに関連付けられているポッドで使用されるプライベート キーを更新します。
- 3 両方のポッド マネージャ仮想マシンで管理サービスの再起動を実行するように VMware のサポートに依頼します。

管理サービスを再起動する特定のコマンドを実行できるのは VMware チームだけであるため、ここでコマンドを公開することはできません。これらのチームは、社内の問題 3007687-update-9 を参照できます。

Cloud Connector に関連する既知の問題

Connection Server Monitoring Service (CSMS) のステータスが、Horizon Cloud Connector 構成ポータルの [健全性] 領域に [準備ができていません] と表示される (3236634)

[[VMware KB91124](#)] で説明されているように、Horizon Cloud Connector バージョン 2.3 の場合、Horizon Cloud Connector アプライアンスの再起動後、またはアプライアンスの Kubernetes クラスターの再起動後に、CSMS のステータスが [準備ができていません] と表示されます。

この問題は、バージョン 2.4 以降の Horizon Cloud Connector で解決されています。以前のバージョンでこの問題を回避するには、ナレッジベースの記事に記載されている手順に従ってください。

証明書の有効期限の問題 (3083444)

Horizon Cloud Connector バージョン 2.4 より前のバージョンの証明書には、アプライアンスのデプロイ時から1年で有効期限が切れるという問題が見つかりました。この証明書の有効期限が切れると、Horizon Cloud Connector は Horizon Cloud 制御プレーンに接続できなくなり、Horizon Cloud Connector によって提供されるクラウドベースのサービスが動作不能になります。修正の詳細と手順については、[KB90505](#) を参照してください。

Horizon Cloud Connector バージョン 2.4 以降では、期限切れ前に証明書が自動的に更新されます。

OVF テンプレートのデプロイ時に [プロキシなし] フィールドで指定されたプロキシなしのホスト構成は、デプロイされたアプライアンスに保存されない (2454245、2466306、2467017、DPM-5388)

この問題は、Horizon Cloud Connector バージョン 1.6 以降では解決されています。vSphere 環境で [OVF テンプレートのデプロイ] ワークフローを実行するときに、プロキシなしのホスト構成を [プロキシなし] フィールドに指定するオプションがあります。ただし、この既知の問題により、入力した設定はデプロイされたアプライアンスの構成ファイルにキャプチャされません。その結果、デプロイされたアプライアンスは、指定されたプロキシなしのホスト設定を考慮しません。

Horizon Cloud ポッドのゲートウェイ構成に関する既知の問題

ゲートウェイ構成で Syslog サーバ設定を有効にするための Horizon Universal Console 機能は、デフォルトでオフになっています。(3005985、3023935、3026855)

Syslog サーバ情報を使用して Unified Access Gateway 構成を更新するシステムの API 呼び出しで特定された問題により、以前にリリースされた機能はコンソールで使用しないよう切り替えられています。回避策：なし。

Universal Broker 関連の既知の問題

Horizon Cloud Connector の Horizon Universal Broker クライアントは、アプライアンスが最初にデプロイされた後でコネクタ アプライアンスに対して行ったプロキシ関連の更新を使用しない (HD-35551)

この問題は、Horizon Cloud Connector バージョン 1.6 以降では解決されています。コネクタ アプライアンスの Horizon Universal Broker クライアントは、アプライアンスの初回起動時にプロキシの詳細を取得します。初回の起動は、OVF テンプレートをデプロイした後、アプライアンスを初めてパワーオンしたときにのみ実行されるため、アプライアンスのプロキシ設定に対するその後の変更は、Horizon Universal Broker クライアントによって使用されません。この既知の問題と OVF テンプレートのデプロイ中のプロキシなしの構成に関する上記の既知の問題の存在により、Horizon Universal Broker に関連するホストをプロキシなしのホストとして設定できなくなります。

ブラウザの Horizon Client または Horizon HTML Access が Universal Broker への接続を開始すると、エラー メッセージ「Connection Server への接続に失敗しました」が表示される (2714266)

この問題は、エンド ユーザーのデスクトップを仲介するために Universal Broker を使用するように構成されたテナント内でマニフェスト 2632.x を実行している Microsoft Azure の Horizon Cloud ポッドに影響します。この問題のもう1つの兆候は、次の両方が同時に発生することです。

- デスクトップ仮想マシンが存在するポッドの詳細ページで、ポッド マネージャ仮想マシンの健全性がすべてのポッドのポッド マネージャ仮想マシンに対して「エラー」として報告される。
- ブラウザの Horizon Client または Horizon HTML Access が Universal Broker への接続を開始すると、エラー メッセージ「このデスクトップは現在使用できません。後でもう一度このデスクトップへの接続を試みるか、システム管理者にお問い合わせください。」と表示される。

この問題は、ポッド マネージャ インスタンスが再起動された場合に、マニフェスト 2632.x を実行している Microsoft Azure の Horizon Cloud ポッドで断続的に発生する可能性があります。ポッド マネージャ インスタンスが再起動されたとき（まれな、通常ではない状況）、ポッド マネージャ インスタンスがパワーオンされ、Universal Broker がポッドへの接続を試みた後に、認証された接続を確立できない場合があります。回避策：なし。このような状況が発生した場合は、サービス リクエストを開き、内部問題レポート番号 2714266 を伝えて、サポートを依頼します。

マニフェスト 2747.x 以降のポッドでは、この問題は解決されています。

イメージ、ファーム、割り当てに関する既知の問題

ここに記載した既知の問題は Microsoft Azure にデプロイされたポッドに適用されます。

イメージの公開中にタイムアウト エラーが発生し、仮想マシンがパワーオンされたままになり、公開フローが正常に完了しない (2954270、2962049)

この問題は、公開プロセスの sysprep 手順を実行するときに発生する Microsoft Azure ハイパーバイザーの問題の結果です。この問題は、一部の Azure 仮想マシン モデルで発生します。詳細については、VMware ナレッジベースの記事 [KB88343](#) を参照してください。

Microsoft Azure チームの推奨事項に基づいて、Horizon Cloud ユーザーに解決策を提供するために、サービスの自動化された [Marketplace からの仮想マシンのインポート] ウィザードで使用されるデフォルトの Azure 仮想マシン モデルは、サービスの v2204 リリースで変更され、GPU 以外の Windows 10 仮想マシン（単一セッションとマルチセッションの両方）の自動インポートに Standard_DS2_v2 モデルが使用されません。

- シングルポッド イメージの場合、自動化のデフォルトの仮想マシン モデルは、以前に使用された Standard_D4_v3 仮想マシン モデルから、Standard_DS2_v2 を使用するように変更されました。
- マルチポッド イメージの場合、自動化のデフォルトの仮想マシン モデルは、以前に使用された Standard_D2_v2 モデルから、Standard_DS2_v2 を使用するように変更されました。

v2204 リリースの時点で、ポッドの Azure サブスクリプションに Azure DSv2 シリーズの割り当てを含めてください。

Microsoft Azure サブスクリプションで仮想マシンとその関連リソースが完全に削除されないことがあります。(2824239、2681761、2750176)

この問題は、ポッド マニフェスト 2915.x 以降で解決されています。以前のマニフェストのポッドでこの問題が発生すると、VDI 割り当ての拡張などの問題が発生する可能性があります。この問題は、Microsoft の Azure

Resource Manager (ARM) の問題と、Microsoft Azure クラウドの複数のリージョン間でリソースのステータスを複製する際の遅延が原因で発生します。この Microsoft ARM の問題により、これらの仮想マシン関連リソースの一部が削除されずに残り、Azure サブスクリプションの仮想マシンに接続されないことがあります。このような接続されていないアイテムの例として、ディスクや NIC があります。回避策：この問題は、2915.x 以降のマニフェストを実行しているポッドで解決されています。この問題が発生した場合は、サービス リクエスト (SR) を発行して、古いデータのクリアに関するサポートを要求し、ポッドのアップグレードをスケジュールして問題の再発を防止してください。SR を発行する手順については、[ナレッジベースの記事 KB2006985](#) を参照してください。

Microsoft Azure Government クラウド サブスクリプションにデプロイされたポッドの場合、ファームとデスクトップ割り当てでディスク暗号化機能を使用すると失敗する。(2572579)

ポッドが Microsoft Azure Government クラウドにある場合、ディスク暗号化機能を選択してファームまたは VDI 割り当てを作成しようとする、エラー `Azure error encrypting the VM` により、作成プロセスが失敗します。回避策：なし。

既存のファームの [サーバ] タブでは、すべてのユーザー ログイン モードの選択によって、Horizon Agent を更新する必要があることを示すエラー メッセージが表示されます。(2528295)

管理コンソールを使用してユーザー ログイン モードを設定するには、ファーム仮想マシンで実行されているエージェント バージョン 20.1.0 の検出に依存します。ただし、既存のファーム仮想マシン内のエージェントを更新するために使用するクラウド制御プレーンでは、そのバージョンのエージェントはまだ利用できないことがあります。回避策：なし。エージェントの 20.1.0 バージョンがクラウド プレーンで使用可能で、ポッドがそのエージェントのバージョンを使用できるマニフェスト バージョンに更新された場合、ユーザー ログイン モードの選択を使用するために、ファーム仮想マシンをそのエージェントに更新できます。

大規模なフローティング VDI デスクトップ割り当ての一部のデスクトップ仮想マシンで、エージェントのステータスが不明として報告されることがある(DPM-3201)

多数のデスクトップ仮想マシンがあるフローティング VDI デスクトップ割り当てでは、既知の問題により、Horizon Agent の Blast サービスや Microsoft Azure サービスなどの一部の Windows サービスが起動しない、または起動に時間がかかることが原因で、これらのデスクトップ仮想マシンの一部において不明なエージェント状態になる可能性があります。その結果、管理コンソールで、エージェントのエラーが報告されるとともに、これらのデスクトップ仮想マシンの [エージェントのステータス] 列に「不明」の状態が表示されます。回避策：コンソールで、[再起動] アクションを使用して、これらの仮想マシンを再起動します。

[Marketplace からの仮想マシンのインポート] ウィザードでデスクトップ環境が有効にならないまま、Windows Server 2012 イメージが作成される。(2101856)

既知の問題により、Windows Server 2012 オペレーティング システムでのイメージの作成で自動化された [Marketplace からの仮想マシンのインポート] ウィザードを使用する場合、結果として生成されるイメージでは Desktop Experience が有効にされていません。回避策：結果として生成されるイメージに Desktop Experience を表示するには、結果として生成されるイメージで Desktop Experience を手動で有効にする必要があります。Windows Server 2012 オペレーティング システムでは、Horizon Agent をスキャナリダイレクト オプション付きでインストールするには Desktop Experience がオペレーティング システムで有効にされていることが必要であることにも注意してください。

インポートされた仮想マシンを公開(シーリング)しようとする、プロセスがタイムアウトになる、または sysprep の障害により公開が失敗する (2036082、2080101、2120508、2118047)

インポートされた仮想マシンで [デスクトップへの変換] をクリックし、公開済み (シールド状態) のイメージにするためにその仮想マシンについて [公開] をクリックすると、その仮想マシンに対して多くの処理が行われます。その処理には、Windows System Preparation (sysprep) プロセスの実行、仮想マシンのシャットダウン、電源オフなどが含まれます。Windows sysprep プロセスおよび仮想マシンのカスタマイズについての業界内で既知の問題により、公開プロセスはさまざまな原因で失敗することがあります。[アクティビティ] 画面には、「タイムアウト エラー: 仮想マシンがパワー オフするのを 20 分間待機しました。(Timeout Error Waited 20 minutes for virtual machine to power off.)」のようなメッセージ、およびその他の sysprep 失敗メッセージが表示されます。

一般的に、[Marketplace からの仮想マシンのインポート] ウィザードを使用して仮想マシンを作成し、ウィザードの [Windows イメージを最適化] トグルで [はい] を選択すると、このような sysprep 問題を回避できます。このオプションを使用しなかったインポートされた仮想マシンでこのエラーが発生している場合や、その仮想マシンを手動で作成した場合は、Microsoft のナレッジベースの記事 [KB2769827](#)、[Microsoft MVP 記事 615](#) を参照して、イメージの公開時に sysprep 問題が発生する確率を最小限に抑えるためのイメージ仮想マシンの構成に関するベスト プラクティスを確認してください。sysprep の問題が解決されない場合は、自動化された [Marketplace からの仮想マシンのインポート] ウィザードを使用して sysprep の問題の変更を削減する方法について、記事 [\[Marketplace からの仮想マシンのインポート\]](#) を使用する場合は [Windows イメージの最適化の決定および \[デスクトップのインポート\] ウィザードを使用する場合の \[Windows ストア アプリを削除\] オプションの使用](#) を参照してください。タイムアウト エラーが [アクティビティ] 画面に表示された場合、この回避策を [イメージ] 画面で試行し、そのイメージで [デスクトップへのイメージの変換] アクションを使用します。[アクティビティ] 画面に、デスクトップへのイメージの変換が正常に完了したと示されている場合は、[インポートされた仮想マシン] 画面に移動します。仮想マシンに接続し、ナレッジベースに記載されているベスト プラクティスを適用します。[インポートされた仮想マシン] ページに仮想マシンがパワーオンされたことを示す画面が表示されたら、仮想マシンを選択して [イメージに変換] をクリックして、公開プロセスを再度実行します。

ファームの作成中に、サーバ仮想マシンがカスタマイズの手順から先に進めなくなる場合がある(2010914, 2041909)

ファームのサーバ仮想マシン上での sysprep プロセスで、tiledatamodelsvc という名前の Windows サービスにより、sysprep が、sysprep のカスタマイズ プロセスの完了に必要な Windows ファイルにアクセスできなくなることがあります。この結果として、ファームのサーバ仮想マシンはカスタマイズ ステップ以降に移動できません。sysprep エラー ログに、「Error SYSPRP setupdigetclassdevs failed with error 0」という行が含まれています。回避策：この問題が発生し、sysprep エラー ログ ファイルにそのエラー メッセージがある場合は、イメージの tiledatamodelsvc サービスを停止して無効にすることを試してください。その後、ファームを作成します。

イメージを複製した後や Microsoft Azure でイメージを手動で作成した後に、エージェントのステータスが [インポートされた仮想マシン] 画面で「定義されていません」として表示される(2002798)

公開済みのイメージのクローンを作成するために [複製] ボタンを [イメージ] 画面で使用する場合は、Microsoft Azure でイメージ仮想マシンを手動で作成する場合に、結果として生成される仮想マシンが [インポートされた仮想マシン] 画面のリストに表示されます。この問題により、仮想マシンが完全にパワーオンになっているときでも、エージェントのステータスが「定義されていません」として表示されることがあります。し

かし、仮想マシンを選択して公開するために [イメージへの変換] を選ぶと、ユーザー インターフェイスでエージェントが「アクティブ」状態であると報告されます。回避策：なし。[エージェント ペアリングをリセット]、[新しいイメージ] または [イメージに変換] のワークフローでエージェントが「アクティブ」であると報告される場合は、[インポートされた仮想マシン] 画面での「未定義」ステータスを無視してかまいません。

Microsoft Azure 内のポッドの App Volumes に関連する既知の問題

ここに記載した既知の問題は Microsoft Azure にデプロイされたポッドに適用されます。

異なる時刻にキャプチャされた同じファイル名を持つアプリケーション パッケージ (.vhd ファイル) を同じ場所 (ファイル共有) にアップロードすると、ユーザーがログインしたときに App Volumes サービスがアプリケーションを VDI デスクトップに接続できなくなる (2783560)

App Volumes がアプリケーション パッケージ (.vhd ファイル) をキャプチャするたびに、システムは一意的な GUID を生成してボリュームやキャプチャ セッションを識別します。以前にアップロードしたファイル名 (.vhd) を使用して、Horizon Cloud Azure ポッドのステージング ファイル共有にアプリケーション パッケージをアップロードすることを試みると、Horizon Cloud Azure ポッドとクラウド サービスにすでに存在する GUID 間で不一致が発生します。

Horizon Cloud Azure ポッドで実行されている App Volumes Manager サービスは、ファイル共有からアプリケーション パッケージを定期的にインポートします。Horizon Universal Console のインポートの [インベントリ] - [アプリケーション] ページからアプリケーションをインポートすることを試みると、新しくインポートされたアプリケーション パッケージとそれらに対応する GUID が、Horizon Cloud Azure ポッドを実行している App Volumes Manager サービスにある GUID と一致しません。この不一致のため、割り当てられたアプリケーションは資格のあるユーザーに接続されません。

コンソールの App Volumes 割り当てから一部のユーザーまたはグループを削除すると、割り当て内の残りのユーザーまたはグループの一部から資格が削除される場合がある (2704889)

この問題により、一連のアプリケーションと指定されたユーザーまたはグループを含む App Volumes 割り当てを作成し、その割り当てを編集して特定のユーザーまたはグループをいくつか削除したシナリオにおいて、その割り当てに残っている構成されたユーザーとグループの一部に対して、資格が付与されたデスクトップでアプリケーションが表示されません。

この問題はポッド マニフェスト 2747 以降で解決されましたが、以前のバージョンのマニフェストのポッドでこの問題が発生する可能性があります。この問題が発生した場合は、必要なアプリケーションとユーザーとグループを使用して新しい App Volumes 割り当てを作成し、以前に作成した App Volumes 割り当てを削除することで問題を回避できます。

Microsoft Azure に複数のポッドがある環境では、プロセスの完了後に、キャプチャ プロセスが不明な状態になることがある。(2600573)

環境内に App Volumes を使用している複数のポッドがある場合、キャプチャ プロセスの実行後に、仮想マシンのキャプチャ プロセスが完了しているにもかかわらず、コンソールでキャプチャが不明な状態であることが示されます。この問題を回避するには、[インベントリ] - [アプリケーション] - [新規] - [インポート] 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。その結果、アプリケーション パッケージは個別のアプリケーションとして正常にインポートされ、その後の割り当てとアプリケーション起動が機能します。

Microsoft Windows 10 Enterprise のマルチセッション展開で、別のユーザーが同じマシンにログインすると、印刷ジョブが終了する場合があります。

この環境では、プリンタ ドライバを含むアプリケーション パッケージ割り当てを持つユーザーが初めてログインすると、そのマルチセッション マシン上の別のユーザーで進行中の印刷ジョブがエラー状態になる場合があります。この問題を回避するには、数分以上待って印刷ジョブが終了してから、印刷ジョブを再試行します。関連するベスト プラクティス情報については、『Horizon Cloud テナント環境およびオンボーディング ポッドの管理』ガイドを参照してください。

Microsoft Windows 10 Enterprise マルチセッション展開で、アプリケーション パッケージが割り当てられていないユーザーがアプリケーションのイメージを受け取る

この環境では、プロビジョニング中にアプリケーションの自動更新をオフにしないと、マルチセッション デスクトップのすべてのユーザー（アプリケーションを割り当てられたユーザーだけではない）にデスクトップ ショートカットやアプリケーション バイナリの形式など、アプリケーションの更新された部分が誤って表示されることがあります。この問題を回避するには、自動更新サービスを使用するアプリケーションの場合、アプリケーション サービス名をマルチストリング svservice レジストリ構成 DisableAppServicesList に追加して、自動更新サービスが開始されないようにします。関連するベスト プラクティス情報については、『Horizon Cloud テナント環境およびオンボーディング ポッドの管理』ガイドを参照してください。

エージェントのアップデートに関連する既知の問題

ここに記載した既知の問題は Microsoft Azure にデプロイされたポッドに適用されます。

Windows Update が保留中になっているイメージに対してエージェントを更新しようとすると、更新プロセスが失敗することがある(2234964)

イメージに対して Windows OS のアップデートが必要な場合、OS 以外のマイナーなアップデートの場合とは対照的に、OS リソースがオフラインになりエージェントの更新で使用できなくなることがあります。回避策：Windows のアップデートが完了するまで待ってから、エージェントの更新を再試行します。すべての Windows アップデートが完了したことを確認するには、イメージをオフラインにし、すべての保留中のアップデートを実行し、エージェントの更新を開始する前にイメージを再公開します。

関連する既知の問題のレポートと監視

ここに記載した既知の問題は Microsoft Azure にデプロイされたポッドに適用されます。

ユーザー アクティビティ レポートで、週の平均（時間）の表示が直感的でない(1817065)

この問題により、週の統計は時間に合わせて変動します。これは、計算ロジックが現在の週の期間を 7 で除算し、1 週間への切り上げを行わないことが原因です。たとえば、直近の 30 日間を選択すると、完了した週のデータは変更されませんが、現在の週のデータは 7 で除算されます。現在のロジックは、週の平均（時間）= 1 日の平均（時間）* 7 日であるため、直近の 30 日間の週平均 = （合計期間/30 日）* 7 日となります。回避策：なし

[デスクトップの健全性] レポートで、ファーム名または VDI デスクトップ割り当て名の変更後 1 時間経過するまで、その新しいファーム名または VDI デスクトップ割り当て名が反映されない(1756889)

ファーム名または VDI デスクトップ割り当て名を変更すると、[デスクトップの健全性] レポートの [割り当て] ドロップダウン メニューおよび [割り当て] 列で新しい名前が反映されるのに 1 時間かかります。回避策：新しい名前がレポートに表示されるまで 1 時間お待ちください。

[レポート] のユーザー インターフェイスの画面からエクスポート可能な一部の CSV ファイルのフォーマットが画面上の表と一致しない。(2015500)

一部の [レポート] 画面のサブ画面で、表示されたデータを CSV 形式でエクスポートする機能が利用できます。この問題により、デスクトップの健全性、同時実行、セッション履歴のレポートからエクスポートされた CSV ファイルのフォーマットが、画面上に表示されるものと正確に一致しくなくなります。たとえば、列の見出しが異なる場合や、CSV ファイルに画面上の表よりも多くのデータ列が含まれることがあります。回避策：なし。

ID 管理、Workspace ONE Access、True SSO に関連する既知の問題

ここに記載した既知の問題は Microsoft Azure にデプロイされたポッドに適用されます。

1763 より前のマニフェスト バージョンのポッドがマニフェスト 1763 以降に更新され、そのポッドの Unified Access Gateway インスタンスに 2 要素 RADIUS が構成されており、Workspace ONE Access と統合されている場合は、ブラウザを使用して Workspace ONE Access からデスクトップを起動すると、ユーザー名フィールドにあらかじめユーザーの UPN が入力された RADIUS ログイン フォームが表示されます。(2248160)

この症状は VMware Horizon HTML Access 4.10 でリリースされた変更が原因で発生します。以前の Horizon Cloud リリースの Microsoft Azure のポッドが Unified Access Gateway インスタンスと 2 要素 RADIUS 認証で構成されていて、Workspace ONE Access を使用するようにそのポッドを構成した場合、以前はブラウザを使用して Workspace ONE Access からデスクトップを起動すると、RADIUS ログイン フォームでユーザー名とパスワードの入力が求められていました。これに応じて、エンド ユーザーはフォームにユーザー名とパスワードを入力していました。ただし、この既知の問題により、そのポッドをこのリリースにアップグレードした後に同じ手順を使用してデスクトップを起動すると、RADIUS ログイン フォームのユーザー名フィールドに、ドメイン ユーザーの UPN が事前入力されるようになります。これは、ブラウザを使用してデスクトップを起動する場合にのみ発生します。Horizon Client を使用する場合は発生しません。回避策：これが発生した場合、エンド ユーザーは事前入力されたユーザー名フィールドを消去して、自分自身の情報を入力することができます。通常、Workspace ONE Access と統合されているほとんどの環境では、2 要素認証は Workspace ONE Access で構成され、基盤となる Unified Access Gateway インスタンスには構成されません。この場合、この問題は発生しません。

Horizon Client を使用して Workspace ONE Access から 2 台目のデスクトップを起動すると、「このデスクトップまたはアプリケーションを実行する権限がありません (You are not entitled to that desktop or application)」のメッセージとともに失敗することがある。(1813881, 2201599)

この症状は、次のような状況で発生します。ユーザーが、1 つのグループ資格を通じて 2 つの専用 VDI 割り当てに対する資格を保持している場合。ユーザーがログインすると、両方の専用 VDI デスクトップ割り当てが Workspace ONE Access に表示されます。ユーザーは Horizon Client を使用して最初のデスクトップを起動します。デスクトップが接続される。次にもう 1 つの割り当てから同じく Horizon Client を使用して別のデスクトップを起動する。この場合、ユーザーに資格がないというエラーが表示され、2 台目のデスクトップの起動が失敗します。ただし、これは 2 台目のデスクトップで最初の試行時にのみ見られる問題です。ユーザーがブラウザを使用して 2 台目のデスクトップを起動すると、以降、Horizon Client を使用した 2 台目のデスク

トップの起動は成功します。回避策：この状況が起きた場合は、2 台目のデスクトップはブラウザで起動してください。

Workspace ONE Access で、Horizon Cloud 管理コンソールから設定したリモート アプリケーションの表示名が表示されない。(2131583)

この問題は Workspace ONE Access Connector バージョン 19.03 を使用することで解決されます。19.03 より前のバージョンの Workspace ONE Access Connector の既知の問題により、Workspace ONE Access が Horizon Cloud から同期するリモート アプリケーションを表示すると、Horizon Cloud でリモート アプリケーションに設定した表示名が Workspace ONE Access に表示されません。Horizon Cloud が表示名を Workspace ONE Access に送信した場合でも、Workspace ONE Access はリモート アプリケーションの launchID を代わりに使用します。その結果、Workspace ONE Access はリモート アプリケーションの基底名を表示します。

ユーザー インターフェイスに関する既知の問題

既知の問題に特に記載がない限り、ここに記載されている既知の問題は、Microsoft Azure にデプロイされているポッドに適用されます。

セッション ダッシュボードで表示されるログイン セグメント チャートにデータがない。

この問題は、すべてのタイプのポッドに適用されます。VMware Logon Monitor サービスにより、セッション ダッシュボードに表示するログイン セグメント チャートのデータが提供されます。ただし今回のリリースでは、VMware Logon Monitor の使用がサポートされず、Horizon Agents Installer では、対象となるすべてのインストールで VMware Logon Monitor サービスがデフォルトで無効になります。このため、ログイン セグメント チャートで表示可能なデータがないと報告されても、セッション ダッシュボードにはログイン セグメント チャートが表示されることになります。回避策：なし。

1つのブラウザ タブで管理コンソールを使用するとき、同じブラウザの別のブラウザ タブにある切断されたデスクトップを起動しようとすると、HTML Access ポータルもログオフされ、HTML Access ポータル自身に再度ログインしなければならない。(2118293)

通常、デスクトップを起動し、デスクトップからログアウトせずに切断すると、HTML Access ポータル自身にログインされたままになり、HTML Access ポータルの認証情報を入力しなくても切断されたデスクトップに再接続できます。この問題のために、ブラウザ内の1つのブラウザ タブでコンソールにログインし、別のブラウザ タブを使用して HTML Access ポータルにログインしてデスクトップを起動すると、そのデスクトップから切断して再度接続する際に、HTML Access ポータルはログオフします。その後、そのデスクトップに再接続するには、HTML Access ポータルの認証情報を再入力する必要があります。回避策：この問題を回避するには、HTML Access ポータルのある場所とは別のブラウザ ウィンドウを使用して管理コンソールにログインします。この動作は、HTML Access ポータルを使用しているのと同じブラウザ ウィンドウのブラウザ タブでコンソールにもログインしている場合にのみ発生します。

特定のユーザーの [ユーザー カード] 画面で、VDI 専用デスクトップ割り当てが、ユーザーがその割り当てから専用デスクトップを初めて起動した後に [割り当て] タブから削除される(1958046)

ユーザーが Active Directory グループとしてではなく、個々のユーザーとして VDI 専用デスクトップ割り当て内で指定されると、ユーザーがその割り当てから専用デスクトップを初めて起動するまで、そのユーザーのみの VDI 専用デスクトップ割り当てが [ユーザー カード] 画面の [割り当て] タブに表示されます。ユーザーがそ

の割り当てから VDI 専用デスクトップを最初に起動すると、ユーザー カードの [割り当て] タブには、そのユーザーの VDI 専用デスクトップ割り当てが表示されなくなります。ユーザーの最初の起動により、そのユーザーは割り当てによって定義された基盤となるプールから特定の専用デスクトップを要求し、システムはその特定の専用デスクトップをユーザーにマッピングします。このマッピングにより、特定の専用デスクトップは「割り当て済み」の状態になり、そのユーザーのユーザー カードの [デスクトップ] タブに表示されます。

回避策：この場合、特定のユーザーに割り当てられた起動済みの VDI 専用デスクトップを表示するには、ユーザー カードの [割り当て] タブではなく、[デスクトップ] タブを使用します。そのユーザーとデスクトップのマッピングが実行される特定の VDI 専用デスクトップ割り当てを見つける必要がある場合は、ユーザー カードの [デスクトップ] タブからデスクトップ名を取得し、上部バナーにある仮想マシン別の検索機能を使用して、特定のデスクトップ仮想マシンをリストします。仮想マシン別の検索結果で名前をクリックし、該当の専用デスクトップがある特定の割り当てページを開きます。これで、割り当ての詳細からユーザーを見つけることができます。

以前にオプションを選択して [新機能] 画面が表示されないように設定した後も、[新機能] 画面が表示される (2075825)

この問題は、すべてのポッド タイプの環境で発生します。この問題のため、ブラウザのキャッシュをクリアするか、以前に [新機能] 画面を表示しないというオプションを選択したブラウザとは別のブラウザを使用すると、管理コンソールにログインしたときにこの画面が表示されることがあります。[新機能] 画面を表示するかどうかのフラグは、ユーザーごとに保存されるのではなく、ブラウザのローカル キャッシュに保存されます。回避策：なし。

イメージ作成のプロセスが完全に完了していない場合でも、[はじめに] 画面の [イメージの作成] 手順に [完了] と表示される (2100467)

この問題のため、[イメージの作成] 手順が完了していないのに [完了] と表示されます。回避策：[アクティビティ] 画面を使用して、イメージの作成プロセスが完了したことを確認します。

管理コンソールを使用しているときに、実際のテキスト文字列の代わりにプレースホルダが表示される場合や、ページのボタンをクリックしても何も起こらない場合がある。 (2045967)

この問題は、すべてのポッド タイプの環境で発生します。VMware は Web ベースのコンソールをホストするクラウド内の管理環境を定期的にアップデートします。この問題が発生するのは、最新のクラウド内アップデートよりも前に、ブラウザで静的コンテンツがキャッシュされているときです。これは一時的な問題で、ブラウザのキャッシュがクリアされると解決されます。回避策：コンソールからログアウトし、ブラウザのキャッシュをクリアしてから、ブラウザを再起動してコンソールに再びログインしてください。

エンド ユーザーが Workspace ONE Access を使用してアプリケーションにアクセスすると、アプリケーション名が小文字で表示される。 (1967245)

Horizon Cloud 環境が Workspace ONE Access に統合されている場合、エンド ユーザーは Workspace ONE Access を使用して割り当てられたデスクトップおよびアプリケーションにアクセスします。この既知の問題により、アプリケーション名に大文字が使用されていても、表示されるアプリケーション名はすべて小文字になります。この制限は、Workspace ONE Access が古い Horizon Cloud REST API を使用して Horizon Cloud から起動 ID を作成する方法に関係します。回避策：なし。

デスクトップの健全性レポートに対して報告され、デスクトップの健全性アラートのために使用されるメモリ使用量の割合は、コミットされているメモリの割合に基づく。これは、物理メモリとページファイルのサイズの合計に等しく、物理メモリのみの割合に基づくものではない。 (2015772)

デスクトップ仮想マシンでコミットされたメモリは物理メモリにページファイル サイズを加えたものとして計算されます。デスクトップのメモリ使用量の割合を計算するときに、システムはその合計（物理メモリとページファイルのサイズ）に使用される割合を示します。デスクトップの健全性アラートと、デスクトップの健全性レポート内のメモリ使用率レポートの両方で、その割合の計算が使用されます。ただし、デスクトップ仮想マシンにログインして Windows タスク マネージャーを開き、デスクトップの Windows オペレーティング システムのメモリ使用量を表示する場合、Windows タスク マネージャーには物理メモリのみに基づく割合が表示されます。このため、デスクトップの Windows タスク マネージャーに表示されるメモリ使用量の割合は、デスクトップの健全性レポートまたはデスクトップの健全性アラートに表示されるメモリ使用量の割合と一致しません。回避策：デスクトップの Windows タスク マネージャーによって報告されるメモリ使用量の割合と、コンソールのデスクトップの健全性レポートとデスクトップの健全性アラートでそのデスクトップについて報告されるメモリ使用量の割合の比較を実施する場合は、この差異を考慮します。

デスクトップ仮想マシンの CPU 使用率が 100% または 100% に近い場合に、デスクトップ アラートがトリガされない(1446496)

デスクトップ仮想マシンのアプリケーションなどによって仮想マシンの CPU 使用率が 100% に到達すると、CPU がビジー状態のため、デスクトップ エージェントは通常で Horizon Cloud に送信可能な量のデータ サンプルを送信することができません。返されるサンプル数が少ないことにより、デスクトップ アラートをトリガするためにシステムによって使用される計算に影響します。回避策：なし。

エンド ユーザー、Horizon Agent、Horizon Client 関連の既知の問題

ここに記載した既知の問題は Microsoft Azure にデプロイされたポッドに適用されます。

最近開いているオプション (またはクライアント タイプに基づく同等のオプション) を使用して Horizon Client から専用デスクトップを起動すると、専用デスクトップが正しく起動しないことがある (SR23422432704、HCS-39121)

さまざまな Horizon Client は、クライアントが以前に起動したデスクトップまたはリモート アプリケーションを記憶するメカニズムを提供します。エンド ユーザーは、資格が付与されているデスクトップとアプリケーションの完全なリストに移動することなく、以前に開いたデスクトップまたは公開アプリケーションを起動できます。

たとえば、Horizon Client for iOS と Horizon Client for Android では、[最近使用したアイテム] というラベルの付いた画面から、以前に起動したデスクトップやリモート アプリケーションにアクセスできます。

『VMware Horizon Client for Mac 製品のドキュメント』で説明されているように、Horizon Client for Mac では、最近使用したデスクトップとリモート アプリケーションを開く方法として、クライアントの [ファイル] - [最近使用したアイテムを開く] オプションを使用する方法と、Dock のアイコンを使用してクライアントを Dock に追加する方法の 2 つがあります。『VMware Horizon Client for Windows 製品のドキュメント』で説明されているように、Horizon Client for Windows には、ジャンプ リスト統合と呼ばれる GPO 設定があり、通常はデフォルトで有効になっています。これにより、ユーザーは Windows タスクバーの Horizon Client アイコンを使用して最近使用したデスクトップや公開アプリケーションに接続できます。

Horizon Cloud on Microsoft Azure によってプロビジョニングされた専用デスクトップの場合、最初のデスクトップの起動後に、Horizon Client がデスクトップの正しい ID を最近の起動として保存しないことがあります。

この問題により、エンド ユーザーが上記のクライアントの recent メカニズムのいずれかを使用してデスクトップを再度開くと、デスクトップが起動しないことがあります。

この問題は、Horizon Cloud on Microsoft Azure デプロイで Workspace ONE Access が使用され、Horizon Client がユーザーを Workspace ONE にリダイレクトして専用デスクトップの起動を調整する場合にも発生する可能性があります。エンド ユーザーが以前に Workspace ONE ポータルからデスクトップを直接起動したことがあり、その後、ユーザーがクライアントの recent メカニズムのいずれかを使用してデスクトップを起動しようとした場合、クライアントが起動を調整するために Workspace ONE にリダイレクトすると、この問題が原因でデスクトップが起動しないことがあります。

回避策：この問題が発生しないようにするには、常にクライアントの完全なデスクトップ リストからデスクトップを直接選択してデスクトップを起動するか、すべての起動を Workspace ONE ポータルから実行する必要があるように環境が構成されている場合は、Workspace ONE ポータル内でデスクトップを選択して起動を開始します。クライアントの recent メカニズムを使用しないでください（[ファイル] - [最近使用したアイテムを開く]、[最近使用したアイテム] リスト、またはクライアントによって提供される recent メカニズムを使用しないでください）。

注： Horizon Cloud on Microsoft Azure デプロイで Workspace ONE リダイレクトが有効になっていて、エンド ユーザーが recent メカニズムを使用し、デスクトップの起動に失敗すると、起動に失敗したことを示す Workspace ONE 監査イベントが書き込まれます。

Microsoft Windows 10 Enterprise マルチセッション 2004 以降を実行している仮想マシンの場合、DPI の同期とディスプレイのスケーリング機能に問題がある (2587685、DPM-6352)

Microsoft Windows 10 Enterprise マルチセッション 2004 以降を実行している仮想マシンで現在の DPI をクエリできないため、これらの仮想マシンの当該機能は、Horizon Client ドキュメントに記載されているとおりに機能しません。DPI の同期とディスプレイのスケーリング機能は、PCoIP セッションの再接続では動作しません。DPI スケーリング機能は、Blast セッションの再接続では動作しません。回避策：セッションからログアウトし、ログインし直します。

Microsoft Windows 10 Enterprise クライアント オペレーティング システム 1903 以降を実行している仮想マシンの場合、DPI の同期とディスプレイのスケーリング機能に問題がある (2589129)

Microsoft Windows 10 Enterprise クライアント オペレーティング システム 1903 以降を実行している仮想マシンで現在の DPI をクエリできないため、PCoIP または Blast セッションを再接続すると、これらの機能が Horizon Client のドキュメントに記載されたとおりに動作しません。回避策：セッションからログアウトし、ログインし直します。

VMware HTML Access を使用して VDI デスクトップを起動するときに、接続解除に関するエラー メッセージが表示され、その後起動に成功することがある(2243471)

VDI デスクトップ仮想マシンにはデフォルトのセッション接続タイムアウトが設定されており、タイムアウトに達するとセッションは切断されます。デスクトップを起動するときに、デスクトップのデフォルトのセッション接続タイムアウトに達した場合にエンド ユーザーの HTML Access セッションがタイムアウトすると、デスクトップで最初にそのエラーが発生し、デスクトップの起動を続行することがあります。回避策：なし。

VDI デスクトップ割り当てにディスク暗号化を選択していて、1つまたは2つのコアの仮想マシンがあり、かつデスクトップの基盤となる仮想マシンの電源がオフの場合、Horizon Client の自動再試行オプションが接続できないことがある(2167432)

VDI デスクトップ割り当ての電源管理設定により、VDI デスクトップの仮想マシンの電源がオフの場合、仮想マシンの電源をオンにして準備完了になってから、エンド ユーザーがそのデスクトップに接続できるようになります。エンド ユーザーが VDI デスクトップ割り当ての仮想マシンへの接続を試みたときに仮想マシンがオフになっていると、システムはその仮想マシンでの起動を開始します。暗号化されていない仮想マシンの場合、通常、この仮想マシンは 10 分以内にクライアント接続を受け入れる準備を完了します。ただし、暗号化された仮想マシンに備えられているコアが 1~2 個の場合、1つの接続に対する準備を完了するのに通常、10 分以上かかります。Horizon Client の [クライアントの再試行] オプションには 12 分間の上限が設けられています。[クライアントの再試行] オプションではこの上限が適用されるため、デスクトップの基盤となる仮想マシンに電源が投入され、準備を実施している間、12 分以内に接続が完了する前に、エンド ユーザー側からクライアントに対して自動的に接続が再試行されると、クライアントの自動再試行が放棄されます。暗号化された仮想マシンでは通常、クライアント接続を準備するまでに 12 分以上要するため、エンド ユーザーは Horizon Client の自動再試行が失敗し、暗号化デスクトップ仮想マシンへの接続が完了しなかったと判断することがあります。回避策: VDI デスクトップ割り当てにディスク暗号化を設定する場合は、2 つ以上のコアを持つ仮想マシン モデルを選択します。また別の方法として、VDI デスクトップ割り当てにディスク暗号化が選択され、1 つの仮想マシン モデルに 1 つ以上のコアが選択されている場合、エンド ユーザーに対し、暗号化されたデスクトップの仮想マシンに [[クライアントの再試行]] オプションを使用すると、この問題が生じることがあるということを通知します。

専用 VDI デスクトップ割り当ての仮想デスクトップの場合、Horizon Client の [最近使用したアイテム] 画面でショートカット リンクをクリックしてもデスクトップが起動しないことがある(1813881、HD-3686、DPM-1140)

Horizon Client の iOS および Android バージョンの場合、[最近使用したアイテム] 画面に最近起動したデスクトップのリンクが表示されます。ユーザーが専用プールの仮想デスクトップを初めて起動するときに、デスクトップが通常どおり起動し、クライアントが [最近使用したアイテム] ページに起動アイコンを作成します。ユーザーがデスクトップを切断した後で [最近使用したアイテム] ページからデスクトップを起動しようとする、起動アイコンがデスクトップ名の短縮バージョンを使用するため、デスクトップを起動できません。回避策: [最近使用したアイテム] 画面ではなく、クライアントのメイン画面からデスクトップを起動してください。

1976.0 マニフェスト バージョンのポッドとエージェント レベル 19.4 を実行しているファーム仮想マシン: HTML Access (Blast) および PCoIP プロトコルを使用している場合、ユーザーはデスクトップまたはリモートアプリケーション セッションから 1 時間後に切断されます。(2519400)

この問題は、Microsoft Windows 10 Enterprise マルチセッション システムの Microsoft ターミナル サービスの問題によるものです。Microsoft Windows 10 Enterprise マルチセッション オペレーティング システムに基づいた RDSH ファームからプロビジョニングされるセッション ベースのデスクトップおよびリモートアプリケーションの場合、エンド ユーザーが HTML Access (Blast) または PCoIP プロトコルを使用して既存のデスクトップまたはリモート アプリケーション セッションに再接続した後、1 時間が経過すると、ユーザーのセッションは強制的に切断されます。データが失われることはありません。ユーザーは再接続でき、セッションが切断時と同じ状態ですが、この動作が繰り返され、再接続されたセッションが 1 時間後にまた強制的に切断されます。

この問題は、Horizon Agents Installer (HAI) 20.1 以降を使用して解決されています。1976.0 ポッドが 1976.1 以降のマニフェストに更新されると、[Marketplace からの仮想マシンのインポート] ウィザードにより、この修正が適用されたエージェント ソフトウェアが自動的にインストールされます。ポッドのマニフェストレベルがまだ 1976.0 にある場合、ウィザードを実行しても、問題のあるエージェント ソフトウェアがインストールされます。ただし、仮想マシンをシールすると、[イメージ] ページに青色のドットが表示されます。これはエージェントのアップデート機能を使用してエージェントを修正が適用されたレベルにアップデートできることを意味します。

マニフェスト バージョン 2298 より前のポッド：クライアントでプロトコルを切り替えるときに、[ログアウトして再接続] ではなく [接続] を選択すると、クライアントが応答しなくなることがあります。(2528014)

この問題は、マニフェスト 2298 以降に更新されたポッドで解決されています。この問題は、1つのプロトコルを使用して RDSH ファームへのセッションを確立した後に、クライアントでプロトコルを切り替えると発生します。1つのプロトコルを使用してデスクトップまたはアプリケーションを起動するときに、そのセッションを切断し、クライアントのメニューを使用して別のプロトコルに切り替え、同じデスクトップまたはアプリケーションを起動すると、クライアントは、「このデスクトップはサーバ上で開いていますが、異なるプロトコルを実行しています」というダイアログ ボックスを表示します。接続するか、ログアウトして再接続するかを選択できます。[接続] ボタンを選択すると、ダイアログが再度表示されます。もう一度 [接続] を選択すると、クライアントが応答しなくなります。

エージェントのアップデート機能を使用して 18.2.2 バージョンより前のエージェントを含むイメージを更新すると、アップデート プロセスが失敗することがある (2200962)

マニフェスト レベルが 965 以前のノードで作成したイメージで、この問題が生じることがあります。場合によっては、イメージの RunOnce レジストリに、エージェントのアップデート プロセスの実行を妨げる値が生じることがあります。回避策：エージェントのアップデートを再度実行し、[エージェントのアップデート] ウィザードの [コマンド ライン] タブで次のコマンド ライン引数を追加します。

VDM_SUPPRESS_RUNONCE_CHECK=1

第 1 世代テナント - Horizon テナントの基本的な概念 - クラウド サービス、制御プレーン、Horizon Universal Console、およびクラウド接続されたポッド

2

この記事では、第 1 世代 Horizon 制御プレーンおよび第 1 世代 Horizon Cloud Service の使用に関連するいくつかの基本的な概念の概要について説明します。テナント環境全体は、VMware Cloud ベースのサービス、制御プレーン、およびオンプレミス、VMware SDDC、またはパブリック クラウド環境にデプロイされ、制御プレーンに接続されたポッドで構成されます。単一のクラウドベースの Horizon Universal Console から、ポッドが物理的に配置されている場所に関係なく、ポッド フリート全体で仮想デスクトップとアプリケーションを効率的にデプロイ、管理、および監視できます。

注目: この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

2022 年 8 月の時点で、Horizon Cloud Service - next-gen は一般公開され、独自の『Horizon 制御プレーン next-gen の使用』ガイドを入手できます。

次世代と第 1 世代のどちらの環境を使用しているかは、環境にログインし、Horizon Universal Console ラベルに表示されるブラウザの URL フィールドのパターンで確認することができます。次世代環境の場合、コンソールの URL アドレスには `/hcsadmin/` のような部分が含まれます。第 1 世代コンソールの URL の場合は、異なるセクション (`/horizonadmin/`) があります。

Horizon 制御プレーン



VMware は制御プレーンをクラウドでホストします。各制御プレーン サービスは、Horizon 環境と仮想デスクトップおよびアプリケーションの管理を簡素化するために機能します。Horizon サブスクリプション ライセンスにサインアップすると、VMware はこの制御プレーンにテナント環境を作成し、そのライセンスの条件に従って構成します。

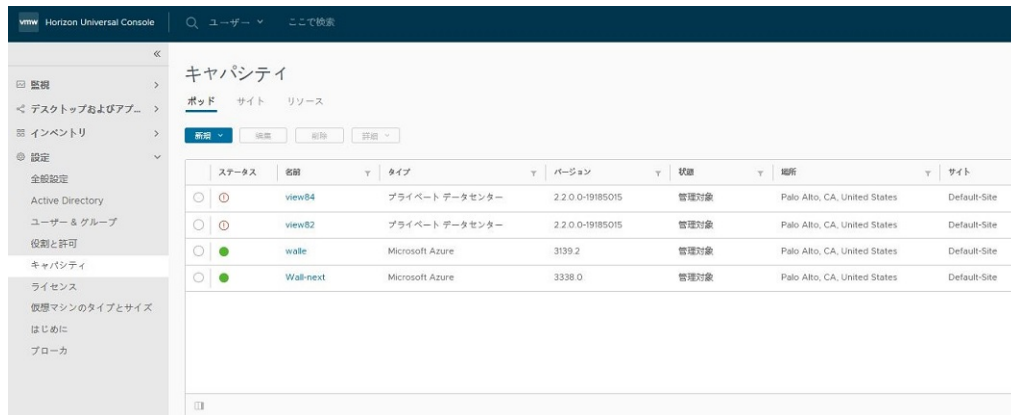
VMware は、責任を持ってサービスをホスティングし、SaaS（サービスとしてのソフトウェア）環境の機能を更新および強化しています。Horizon Cloud はマルチテナント環境であり、いくつかのリージョンの制御プレーン インスタンスがあります。リージョンの制御プレーン インスタンスはそれぞれ、[VMware Horizon サービスの説明およびサービス レベル アグリーメントのページ](#)から入手可能なサービスの説明ドキュメントに記載されているように、ホストの地理的なデータセンターに対応します。テナント アカウントは、アカウントの作成時に特定のリージョン インスタンスに関連付けられます。

制御プレーンの詳細については、Tech Zone の [Horizon 制御プレーン サービスのアーキテクチャ](#)を参照してください。

Horizon Universal Console

制御プレーンは、Horizon Universal Console（または単にコンソール）と呼ばれる、共通のクラウドベースおよび Web ベースの管理ユーザー インターフェイスもホストします。このコンソールは、業界標準のブラウザで実行されます。このコンソールは、ユーザー割り当て、仮想デスクトップ、リモート デスクトップ セッション、およびアプリケーションに関与する管理タスクを IT 管理者のために 1 つにまとめた場所です。このコンソールは、テナントの現在の状態を動的に反映し、時間や場所に関係なくアクセスできるので、非常に柔軟に利用できます。

次のスクリーンショットは、テナントのポッド フリートに 4 つのポッドがある場合のコンソールの [キャパシティ] ページの [ポッド] タブを示しています。



クラウド接続されたポッド

Horizon デプロイでは、ポッドは主に概念的なエンティティです。ポッドは、パブリック クラウド、VMware SDDC、オンプレミス データセンターなど、サポートされている環境にデプロイされたさまざまなソフトウェア コンポーネントに基づいています。ポッドの相互に関連するコンポーネントは、仮想デスクトップとアプリケーションのプロビジョニングを提供し、エンド ユーザー クライアントの要求をその使用資格のある仮想デスクトップまたはアプリケーションにルーティングすることを容易にします。

クラウド接続されたポッドを構成するソフトウェア コンポーネントの特定のコレクションは、ポッドの構築に使用されるデプロイのタイプによって異なります。現在のサービス リリースでは、テナントでの次のポッド構造の使用がサポートされています。

Horizon ポッド

Horizon Connection Server ソフトウェアおよび関連するソフトウェア コンポーネント上に構築されます。コンポーネントは、オンプレミス、オールイン SDDC アーキテクチャ、フェデレーション アーキテクチャなど、VMware がそのようなポッドでの使用をサポートするアーキテクチャに従ってデプロイされます。これらのデプロイには、VMware SDDC が何らかの形式で含まれます。このポッド構造は、基盤となるソフトウェアが Horizon Connection Server であるため、Horizon ポッドと呼ばれています。簡単な概要については、[第1世代テナント - 第1世代 Horizon Cloud を使用した Horizon ポッドのデプロイ アーキテクチャ](#)を参照してください。

Horizon Cloud ポッド

Microsoft Azure クラウドおよび Microsoft Azure 仮想デスクトップで使用するための Horizon Cloud ポッド マネージャ テクノロジー上に構築されます。ポッド コンポーネントは、Horizon Cloud on Microsoft Azure デプロイ ウィザードを実行してデプロイされます。ウィザードは、Microsoft Azure サブスクリプションへのポッドのデプロイを自動化します。概要については、[Horizon Cloud on Microsoft Azure](#)を参照してください。

最初のテナント環境

テナント環境は、クラウド接続されたポッドのないクリーンスレートで新たに起動します。最初の必要な手順は、そのクリーンスレート環境にポッドをオンボーディングすることです。そのポッドは、テナントのクラウド接続された最初のポッドになります。

次のスクリーンショットは、管理者が初めてログインしたときに、新しい Horizon Cloud 環境がどのように表示されるかを示しています。このクリーン スレート画面は、サービスにオンボーディングできるポッド タイプ (Horizon ポッドと Microsoft Azure の Horizon Cloud ポッド) を中心にしています。1つのポッドがオンボーディングされ、Active Directory ドメイン登録が完了するまで、左側のナビゲーションにある他のすべてのユーザー インターフェイス ページにアクセスできません。



最初のポッドをポッド フリートに追加するために必要な項目については、ポッドのタイプ (Horizon ポッドまたは Horizon Cloud ポッド) に対応する要件チェックリストを参照してください。

- [Horizon ポッド - 要件チェックリスト](#)
- [Horizon Cloud ポッド - 要件チェックリスト](#)

第1世代テナント - 2023年11月2日のサービス更新以降の新しいポッドデプロイに対する VMware Horizon Cloud Service on Microsoft Azure 要件チェックリスト

このチェックリストの目的は、第1世代 Horizon Cloud on Microsoft Azure のデプロイに必要な要素について通知することです。このチェックリストに従って、ポッド デプロイを正常に実行し、Day-1 タスクを完了します。

注目: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。KB-92424 で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

2022年8月の時点で、Horizon Cloud Service - next-gen は一般公開され、独自の『Horizon 制御プレーン next-gen の使用』ガイドを入手できます。

次世代と第1世代のどちらの環境を使用しているかは、環境にログインし、Horizon Universal Console ラベルに表示されるブラウザの URL フィールドのパターンで確認することができます。次世代環境の場合、コンソールの URL アドレスには /hcsadmin/ のような部分が含まれます。第1世代コンソールの URL の場合は、異なるセクション (/horizonadmin/) があります。

チェックリスト対象者

このチェックリストは、主に、2023年11月2日のサービス更新以前に、テナント環境で Horizon Cloud on Microsoft Azure をデプロイしたことがない Horizon Cloud ユーザー 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。

ここで説明するセットは、主に本番環境用です。通常、試用版およびほとんどの事前検証のためのデプロイは、[第1世代テナント - 事前検証のための簡素化された Horizon Cloud Service on Microsoft Azure ポッド環境の使用開始](#)に示すようにサブセットで処理できます。

新しいポッドのデプロイ ウィザードを実行する前に、以下に示すセクションの一部を配置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されるまで延期できます。

一部の項目は、Horizon Cloud on Microsoft Azure デプロイの選択に関連するため、オプションとして表示されます。

たとえば、新しいポッド ウィザードを実行するとき、Unified Access Gateway 構成を選択せずに、後でゲートウェイ構成を追加できます。この場合、後でゲートウェイ構成を追加するまで、Unified Access Gateway の要件を満たす必要はありません。

新しいポッド ウィザードを実行する前に以下を実行する	ポッドのデプロイ後に実行可能
<ul style="list-style-type: none"> ■ 制御プレーン テナント アカウント ■ Microsoft Azure サブスクリプション項目 ■ ネットワーク ■ ポートおよびプロトコル ■ オプションの Unified Access Gateway 項目 	<ul style="list-style-type: none"> ■ Active Directory ■ オプションの Unified Access Gateway (デプロイ後に追加) ■ Universal Broker ■ DNS レコード ■ ゴールド イメージ、デスクトップ、ファームのキャパシティ ■ Microsoft Windows オペレーティング システム ライセンス

いくつかの重要な考慮事項

試用版または事前検証のための Horizon Cloud on Microsoft Azure デプロイを行う場合は、デプロイに使用する Microsoft Azure サブスクリプションの所有者である可能性があります。または、サブスクリプションを所有する組織に代わって、事前検証を行う可能性があります。

サブスクリプションの所有者は、ポッドのサブスクリプションで有効な Microsoft Azure ポリシーがポッドのコンポーネントの作成をブロック、拒否、または制限しないようにする必要があります。

これは、ポッドのデプロイ中に、ポッドのデプロイヤーが API 呼び出しを使用して、新規ポッド ウィザードで指定されたサブスクリプション内にリソースを作成するためです。そのサブスクリプションでポッドのコンポーネントの作成をブロック、拒否、または制限する Microsoft Azure ポリシーが有効になっている場合、デプロイは失敗し、VMware のサポートへのサポート リクエストが必要になります。

一例として、ポッド デプロイヤーは、ポッドのサブスクリプションで有効になっている Microsoft Azure ポリシーのいずれもが Azure ストレージ アカウントでのコンポーネントの作成をブロック、拒否、または制限していないことを要求します。

新しいポッド ウィザードを実行する前に、サブスクリプションの所有者に、Microsoft Azure ポリシーの組み込みポリシー定義がポッドのコンポーネントの作成をブロック、拒否、または制限していないことを確認します。

Horizon Cloud 制御プレーンの要件

□	<p>VMware によって Horizon Cloud 制御プレーンにログインするように構成されている VMware Customer Connect アカウント。</p> <p>このアカウントと Horizon Cloud テナント アカウントの関係の概要については、Horizon Service のポッドのデプロイとオンボーディングページを参照してください。</p>
---	---

Microsoft Azure サブスクリプションの要件

<input type="checkbox"/>	<p>サポートされている Microsoft Azure 環境（Azure Commercial、Azure China、Azure Government）で有効な Microsoft Azure サブスクリプション。外部 Unified Access Gateway を専用のサブスクリプションを使用して個別の VNet にデプロイする場合、同じ Microsoft Azure 環境に追加の有効な Microsoft Azure サブスクリプションを取得します。</p> <hr/> <p>注： Horizon Cloud は、大部分の Microsoft Azure リージョンをサポートしています。現在サポートされていない Microsoft Azure リージョンのリストについては、VMware ナレッジベースの記事「Microsoft Azure Regions with Horizon Cloud Service on Microsoft Azure (77121)」を参照してください。</p>
<input type="checkbox"/>	<p>Microsoft Azure ポータルを使用して、第 1 世代テナント - 第 1 世代 Horizon Cloud ポッドを Microsoft Azure にデプロイする前の準備を実行するための Microsoft Azure サブスクリプションで有効な Microsoft Azure 管理者権限。</p>
<input type="checkbox"/>	<p>ポッドのサブスクリプションで作成された、Horizon Cloud アプリケーションの登録とクライアント プライベート キー。第 1 世代テナント - ポッドのサブスクリプションでの Horizon Cloud アプリケーション登録の作成を参照してください。</p> <p>管理者または組織がポッドのサブスクリプションとは別のサブスクリプションで外部ゲートウェイ構成をデプロイするためにこの機能を使用する場合、そのゲートウェイ サブスクリプションにも Horizon Cloud アプリケーションの登録とクライアント プライベート キーが必要です。</p>
<input type="checkbox"/>	<p>サブスクリプションで Horizon Cloud アプリケーションの登録を作成すると、標準の Microsoft Azure の動作によってサービス プリンシパルが自動的に作成されます。</p> <p>このサービス プリンシパルには、Horizon Cloud がポッドのサブスクリプションで API 呼び出しを行うことができるロールを割り当てます。</p> <p>通常、ポッドのサブスクリプション レベルで Contributor ロールが割り当てられます。</p> <p>または、ポッドのサブスクリプション レベルでカスタム ロールを割り当てることもできます。</p> <p>外部ゲートウェイ構成を別のサブスクリプションの既存のリソース グループにデプロイする場合は、そのゲートウェイ サブスクリプションのサービス プリンシパルにカスタム ロールまたは Contributor ロールを割り当てることができます。</p> <p>ユーザーまたはユーザーの組織が、Horizon Cloud アプリケーションの登録でカスタム ロールを使用する場合は、カスタム ロールに必要なアクションについて説明している次のページ（第 1 世代テナント - 組織が第 1 世代 Horizon Cloud のアプリケーション登録にカスタム ロールを使用することを希望する場合）を参照してください。</p> <hr/> <p>注： ロールは、Horizon Cloud アプリケーションの登録のサービス プリンシパルに直接割り当てる必要があります。このサービス プリンシパルへのロールのグループ ベースの割り当ての使用はサポートされていません。</p>
<input type="checkbox"/>	<p>必要なリソース プロバイダが各 Microsoft Azure サブスクリプションで登録されていること。リソース プロバイダの登録を参照してください。</p>
<input type="checkbox"/>	<p>デプロイ ウィザードで指定するサブスクリプションに対して特定された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 およびキー。</p>
<input type="checkbox"/>	<p>サブスクリプションでは、Azure StorageV2 アカウント タイプの使用を許可する必要があります。サブスクリプションの Microsoft Azure ポリシーが、Azure StorageV2 アカウント タイプを必要とするコンテンツの作成を制限したり拒否したりしないようにします。</p>

<p>□</p>	<p>ポッドのデプロイ ウィザードでカスタム リソース タグを指定しない限り、サブスクリプションは、タグを持たないリソース グループの作成を許可する必要があります。ポッドのデプロイ プロセスでは、ウィザードでカスタム リソース タグを指定しない限り、タグなしでポッドのサブスクリプションにリソース グループが作成されます。</p> <p>デプロイ ウィザードの [カスタム リソース タグ] 機能を使用する予定がない場合は、Microsoft Azure ポリシーによって、ポッドのタグなしリソース グループをターゲット サブスクリプションで作成できることを確認する必要があります。ウィザードでカスタム リソース タグが指定されておらず、Microsoft Azure サブスクリプションに何らかの種類のリソース タグ要件がある場合、そのサブスクリプションにポッドをデプロイしようとする、ポッドのデプロイが失敗します。または、ポッドの更新時やポッドにゲートウェイ構成を追加する際に、ポッドのデプロイが失敗します。デプロイヤが作成したリソース グループの名前については、Microsoft Azure にデプロイされたポッド用に作成されたリソース グループを参照してください。</p>
<p>□</p>	<p>任意。組織によっては、ポッドのサブスクリプションとは別の VNet とサブスクリプションで、外部の Unified Access Gateway 用に組織が命名する、特定の事前作成済みリソース グループを使用するように指定されている場合があります。また、組織は、組織が命名する特定の事前に作成されたリソース グループを使用する必要があり、ユーザーは、この機能を使用して、外部の Unified Access Gateway を独自の名前を付けられたリソース グループにデプロイします。この機能を使用しない場合、ポッド デプロイヤは独自の命名規則でリソース グループを自動的に作成します。</p> <p>この機能を使用するには、ポッド デプロイヤを実行する前に、サブスクリプションにそのリソース グループを作成する必要があります。また、ポッド デプロイヤが Unified Access Gateway 構成をそのリソース グループにデプロイし、構成を管理し、標準のポッド更新プロセスで Unified Access Gateway ソフトウェアを更新するために必要な権限が設定されていることを確認する必要があります。カスタム ロールに含める必要がある権限の詳細については、第 1 世代テナント - 組織が第 1 世代 Horizon Cloud のアプリケーション登録にカスタム ロールを使用することを希望する場合を参照してください。</p>

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、ポッド 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。

仮想マシン ファミリに関連するキャパシティの場合、Microsoft Azure ポータルでは「割り当て」という用語も使用されます。

<p>□</p>	<p>コアの Horizon Cloud ポッド アーティファクト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 (このリストには、オプションの Unified Access Gateway 構成と、予想されるデスクトップおよびアプリケーションのワークロードに必要なキャパシティは含まれていません)。</p> <p>ポッド</p> <ul style="list-style-type: none"> ■ ポッド マネージャ - Standard_D4_v3 x 2 (リージョン内に Standard_D4_v3 がない場合は Standard_D3_v2 x 2) ■ Microsoft Azure Database for PostgreSQL サービス - 第 5 世代、メモリ最適化、2 つの vCore、10 GB ストレージ ■ ポッドを使用する準備ができたなら、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、ゴールドイメージ、仮想デスクトップ、RDSH ファーム、およびそのポッドで作成する 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。以下の Horizon Cloud ゴールド イメージ、デスクトップ、およびファームのセクションを参照してください。 ■ ユーザーがサポート リクエストを発行し、VMware のサポートがそのリクエストに対応する方法として、サポート関連のジャンプ ボックス仮想マシンを一時的にデプロイすることを決定した特別な状況では、ユーザーのキャパシティは、その時点での Standard_F2 モデル仮想マシンのデプロイに対応する必要があります。
<p>□</p>	<p>任意。ポッドに Unified Access Gateway の使用を指定する場合に必要なキャパシティ。</p> <hr/> <p>注： A4_v2 仮想マシン モデルが十分に機能するのは、ポッド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。</p> <hr/> <p>ポッドの同じ VNet 内の外部 Unified Access Gateway</p> <p>Standard_A4_v2 x 2 または Standard_F8s_v2 x 2</p> <p>独自の VNet 内の外部 Unified Access Gateway</p> <ul style="list-style-type: none"> ■ 外部ゲートウェイ コネクタ — Standard_A1_v2 x 1 ■ 外部 Unified Access Gateway — 2 x Standard_A4_v2 または 2 x Standard_F8s_v2。 <p>内部 Unified Access Gateway</p> <p>Standard_A4_v2 x 2 または Standard_F8s_v2 x 2</p> <p>サブスクリプションのリージョンが Standard_F8s_v2 VM のサイズに対応していない場合、ポッドのデプロイ ウィザードでは、[ゲートウェイの指定] ウィザードの手順のセレクトにその選択肢が表示されません。</p>

ネットワーク要件

□	<p>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。第 1 世代 Horizon Cloud - Microsoft Azure での必要な仮想ネットワークの構成を参照してください。</p> <p>外部 Unified Access Gateway をポッドの VNet とは別の独自の VNet にデプロイする場合、ポッドの VNet と同じ Microsoft Azure リージョンに必要なサブネットをカバーする適切なアドレス空間を持つ Unified Access Gateway VNet を作成し、2 つの VNet をピアリングします。</p>
□	<p>ポッドの VNet の重複していない 3 つのアドレス範囲 (CIDR 形式) がサブネット用に予約済みであること。</p> <ul style="list-style-type: none"> ■ 管理サブネット - /27 以上 ■ 仮想マシン サブネット - プライマリ (テナント) - /27 以上。/24 ~ /22 を推奨 (デスクトップおよび RDS サーバの数に基づく) ■ DMZ サブネット - ポッドの VNet に Unified Access Gateway がデプロイされている場合は /28 以上 (オプション) <p>サブネットは、VNet 上で手動で作成することも、デプロイ中に Horizon Cloud によって作成することもできます。手動で作成されたサブネットを使用する場合、他のリソースは接続できません。</p> <hr/> <p>ヒント: ポッドがデプロイされた後に、ポッドを編集して、ファームおよびデスクトップ割り当ての仮想マシンで使用するためのテナント サブネットを追加できます。追加のテナント サブネットは、ポッドがデプロイされているのと同じ VNet、またはピアリングされた VNet に配置できます。詳細については、複数のテナント サブネットの使用の概要を参照してください。</p>
□	<p>外部 Unified Access Gateway をポッドの VNet とは別の独自の VNet にデプロイする場合、Unified Access Gateway の VNet で 3 つの重複しないアドレス範囲 (CIDR 形式) がサブネット用に予約されていること。</p> <ul style="list-style-type: none"> ■ 管理サブネット - /27 以上 ■ バックエンド サブネット - /27 以上。/24 ~ /22 を推奨 (デスクトップおよび RDS サーバの数に基づく) ■ DMZ (フロント エンド) サブネット - /28 以上 <p>サブネットは、VNet 上で手動で作成することも、デプロイ中に Horizon Cloud によって作成することもできます。手動で作成されたサブネットを使用する場合、他のリソースは接続できません。この使用事例では通常、サブネットは手動で作成されます。この使用事例では、バックエンド サブネットの目的は、前述の表の行に記載されている [仮想マシンのサブネット (プライマリ)] の目的と同様です。</p>
□	<p>Horizon Cloud ポッドおよび Unified Access Gateway インスタンスからアクセス可能な 1 つまたは複数の NTP サーバ。</p>
□	<p>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。</p>
□	<p>ポッドおよびゲートウェイのデプロイに使用している VNet 上のアウトバウンド インターネット アクセスは、特定のポートおよびプロトコルを使用して特定の DNS 名を解決し、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。DNS 名とポートのリストについては、第 1 世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名および第 1 世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件を参照してください。</p>
□	<p>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。</p>
□	<p>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。</p>

ポートとプロトコルの要件

□	<p>ポッドのオンボーディングと 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。第 1 世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件を参照してください。</p>
---	---

Unified Access Gateway の要件

Unified Access Gateway 構成を選択せずに新しいポッド ウィザードを実行し、後でゲートウェイ構成を追加できます。この場合、後でゲートウェイ構成を追加するまで、Unified Access Gateway の要件を満たす必要はありません。定義上、外部 Unified Access Gateway は外部ネットワーク上のクライアントが仮想デスクトップとアプリケーションを起動できるようにし、内部 Unified Access Gateway は内部ネットワーク上のクライアントが信頼された HTML Access (Blast) 接続を確立することができるようにします。インターネットからのエンドユーザー接続をサポートし、仮想デスクトップおよびアプリケーションを起動できるようにするには、ポッドで外部 Unified Access Gateway が構成されている必要があります。

新しいポッド ウィザード内で Unified Access Gateway オプションを選択すると、ウィザードは以下の特定の項目を必須にします。

<input type="checkbox"/>	Unified Access Gateway 構成の FQDN。
<input type="checkbox"/>	<p>FQDN に一致する PEM 形式の Unified Access Gateway の証明書。</p> <p>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 ゲートウェイ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、ポッドのデプロイは接続フェーズにおいて失敗します。これらの名前は、証明書の取得に使用した CA に大きく依存しているため、VMware のコントロールには含まれません。</p>
<input type="checkbox"/>	<p>オプション (エンド ユーザーが 2 要素認証を使用する場合を除く)。この場合、Unified Access Gateway は、Horizon Cloud on Microsoft Azure デプロイでの使用がサポートされている認証システム タイプのいずれかを使用する 2 要素認証用に構成する必要があります。</p> <p>構成には以下のものが含まれている必要があります。</p> <ul style="list-style-type: none"> ■ 当該認証サーバの名前を解決するための Unified Access Gateway の DNS アドレス ■ 当該認証サーバへのネットワーク ルーティングを解決するための Unified Access Gateway のルート <p>注： ポッドをデプロイした後、Universal Broker 設定で 2 要素認証を構成した場合、内部エンド ユーザーにもその 2 要素認証の使用をスキップさせるには、いくつかの追加構成が必要です。ポッドに内部 Unified Access Gateway 構成がある場合、その構成はそのような内部エンド ユーザーの仮想デスクトップとアプリケーションに接続要求をルーティングします。Universal Broker で内部エンド ユーザーの 2 要素認証手順をスキップする場合は、ポッドをデプロイして、Universal Broker を構成した後、内部エンド ユーザー トラフィックに対応する出力 NAT アドレスの範囲を入力します。これらの範囲により、2 要素認証をスキップする目的で、Universal Broker は内部エンド ユーザーからのクライアント トラフィックを外部エンド ユーザーからのクライアント トラフィックと区別できます。詳細については、ドキュメント トピック Universal Broker の内部ネットワーク範囲の定義を参照してください</p>

ポッドのデプロイ ワークフロー

上記の項目は、ポッドのデプロイ ウィザードを開始する前に必要です。上記の項目が整っていることを確認したら、[第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - 概要レベルの手順](#) のポッド デプロイの手順 4 までを実行してポッドをデプロイします。

ポッドが正常にデプロイされたら、次のセクションで説明する項目を確認し、概要レベル ワークフローの残りの主要な手順を完了します。

Active Directory の要件

コンソールの Active Directory 登録ワークフローでは、次の項目が必須です。このワークフローをよく理解するには、[Horizon Cloud 環境での最初の Active Directory ドメイン登録の実行](#)を参照してください。

<input type="checkbox"/>	<p>サポートされている次の Active Directory 構成のいずれか：</p> <ul style="list-style-type: none"> ■ 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 ■ Microsoft Azure の Active Directory ドメイン サービス
<input type="checkbox"/>	<p>サポートされる Microsoft Windows Active Directory Domain Services (AD DS) ドメイン機能レベル：</p> <ul style="list-style-type: none"> ■ Microsoft Windows Server 2008 R2 ■ Microsoft Windows Server 2012 R2 ■ Microsoft Windows Server 2016
<input type="checkbox"/>	<p>同じ Horizon Cloud 顧客アカウントのすべてのクラウド接続されたポッドは、それらのポッドをデプロイするときに、Active Directory ドメインの同じセットを認識できる必要があります。この要件は、最初のポッドの後に Microsoft Azure にデプロイする追加のポッドだけでなく、Horizon Cloud Connector を使用して同じ顧客アカウントにクラウド接続されるすべての Horizon ポッドにも適用されます。</p>
<input type="checkbox"/>	<p>ドメイン バインド アカウント</p> <p>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。</p> <p>アカウントは、以下の権限を持つ必要があります。</p> <ul style="list-style-type: none"> ■ 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） <p>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する必要があります。</p> <ul style="list-style-type: none"> ■ VMware Horizon オンプレミス製品に精通しているのであれば、上記の権限は、Horizon オンプレミス製品のセカンダリ認証情報アカウントに必要なセットと同じであることがわかります。 ■ 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、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る必要があります。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。 <p>Horizon Cloud の運用に必要なサービス アカウントを参照してください。</p>

**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する必要があります。

- VMware Horizon オンプレミス製品に精通しているのであれば、上記の権限は、Horizon オンプレミス製品のセカンダリ認証情報アカウントに必要なセットと同じであることがわかります。
- 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、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る必要があります。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。

[Horizon Cloud の運用に必要なサービス アカウント](#)を参照してください。

□

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。

また、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する必要があります。

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

ファームおよび VDI デスクトップ割り当て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。

詳細については、[Horizon Cloud の運用に必要なサービス アカウント](#)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。

また、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する必要があります。

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

ファームおよび VDI デスクトップ割り当て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。

詳細については、[Horizon Cloud の運用に必要なサービス アカウント](#)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。

<input type="checkbox"/>	<p>Active Directory グループ</p> <ul style="list-style-type: none"> ■ Horizon Cloud 管理者 — Horizon Cloud 管理者の Active Directory セキュリティ グループ。Horizon Cloud 管理者ユーザーが含まれます。このグループには、Horizon Cloud でスーパー管理者ロールが付与されます。 ■ Horizon Cloud ユーザー — Horizon Cloud の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と公開済みアプリケーションにアクセスするユーザーの Active Directory セキュリティ グループ。 <p>Horizon Cloud では、管理者ログインとエンド ユーザー資格の両方で Active Directory セキュリティ グループの使用がサポートされます。ネストされたグループがサポートされます。グループ メンバーシップは、tokenGroups コンピューティング属性を要求することによって評価されます。つまり、Horizon Cloud にはネストの深さの制限はなく、Active Directory で設定されたものは何でもサポートされます。</p> <p>Active Directory グループおよび Horizon Cloud、Universal Broker、Workspace ONE Access Cloud の組み合わせに関して、追加の考慮事項または追加の制限があるかどうかを尋ねられた場合、その質問に対する答えは、「いいえ、ありません」になります。</p> <p>テナント環境の Microsoft Azure に 1600.0 より古いマニフェストを実行している Horizon Cloud ポッドがある場合、ドメイン参加アカウントと補助ドメイン参加アカウントも Horizon Cloud 管理者グループ、または Horizon Cloud でスーパー管理者ロールが付与された Active Directory グループに含まれている必要があります。</p>
<input type="checkbox"/>	<p>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)。</p> <p>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。</p>

LDAPS 用に構成された Active Directory を使用する場合、LDAP でサポートされている機能の有効化を Horizon Cloud テナントで要求する必要があります。詳細については、[LDAPS 用に構成された Active Directory 環境の使用](#)を参照してください。

Universal Broker 構成

Universal Broker 構成の場合は、次の表に記載されている項目のうち、目的のオプションに該当する項目を満たしていることを確認してください。詳細については、[Universal Broker の構成](#)を参照してください。

<input type="checkbox"/>	<p>ポッド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 Universal Broker の構成および継続的な運用のために必要です。DNS 名とポートのリストについては、第 1 世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名 と 第 1 世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件 を参照してください。</p>
<input type="checkbox"/>	<p>提供するエンドユーザー接続のタイプに応じて、以下の構成が必要です。</p> <ul style="list-style-type: none"> ■ インターネットからのエンドユーザー接続で、仮想デスクトップおよびアプリケーションを起動する場合は、ポッドで外部 Unified Access Gateway が構成されている必要があります。 ■ すべてのエンドユーザー接続が常に内部ネットワークからのものである場合、ポッドでは Unified Access Gateway は必要ありません。ただし、Universal Broker でこれらの内部エンドユーザー接続に 2 要素認証を適用する場合は除きます。

□	<p>任意。Universal Broker で 2 要素認証を適用する場合、ポッドには、Horizon Cloud on Microsoft Azure デプロイでの使用がサポートされている認証システム タイプの 1 つを使用する 2 要素認証用に構成された外部 Unified Access Gateway が必要です。</p> <p>Universal Broker は認証要求を Unified Access Gateway に渡します。後者は認証サーバと通信し、応答を中継して Universal Broker に返します。</p> <p>この外部 Unified Access Gateway 構成には、次の項目が必要です。</p> <ul style="list-style-type: none"> ■ 認証サーバの名前を解決するための Unified Access Gateway の DNS アドレス ■ 認証サーバへのネットワーク ルーティングを解決する Unified Access Gateway のルート
□	<p>オプション：カスタムの FQDN。エンド ユーザーがこれを使用して Universal Broker サービスおよびその FQDN に基づく証明書にアクセスします。VMware 提供の仲介 FQDN を使用する場合、カスタム FQDN は必要ありません。</p>

DNS レコードの要件

ポッドが Microsoft Azure クラウドにデプロイされた後、ビジネス状況および使用する機能に応じて、完全修飾ドメイン名 (FQDN) をポッド関連の IP アドレスにマッピングするレコードを DNS サーバに設定することが重要です。DNS レコード マッピングの背景情報については、Microsoft クラウド サービスのドキュメント ページ [Azure クラウド サービスのカスタム ドメイン名の構成](#) を参照してください。

注： 外部と内部のゲートウェイ構成で同じ FQDN を使用しているポッドをデプロイした場合は、ポッドのデプロイ後、スプリット DNS (スプリット Domain Name System) を構成して、エンド ユーザー クライアントの DNS クエリのオリジン ネットワークに応じて、外部ゲートウェイまたは内部ゲートウェイのいずれかにゲートウェイ アドレスを解決します。

カスタム FQDN を使用してテナントの Universal Broker を構成する場合

□	<p>Universal Broker 構成で、カスタム FQDN を VMware 提供の仲介 FQDN にマッピングするパブリック DNS レコードを作成します。Universal Broker の構成 を参照してください。</p>
---	--

ポッドに外部 Unified Access Gateway がある場合

□	<p>外部ゲートウェイ構成の FQDN に一致する外部エンドユーザー アクセス用のパブリック DNS レコードを作成します。この DNS レコードは、その FQDN をポッドの外部 Unified Access Gateway 構成の Microsoft Azure 外部ロード バランサにポイントします。</p> <p>DNS レコード マッピングの背景情報については、Microsoft のドキュメント ページ Azure クラウド サービスのカスタム ドメイン名の構成 を参照してください。</p>
---	--

ポッドに内部 Unified Access Gateway がある場合

□	<p>内部ゲートウェイ構成の FQDN に一致する内部エンドユーザー アクセス用の内部 DNS レコードを作成します。この DNS レコードは、その FQDN をポッドの内部 Unified Access Gateway 構成の Microsoft Azure 内部ロード バランサにポイントします。</p>
---	--

Horizon Cloud ゴールド イメージ、デスクトップ、およびファーム

Microsoft Azure サブスクリプションは、デプロイされたポッドからプロビジョニングするゴールド イメージ、VDI デスクトップ、および RDS ファームの種類に応じて、次の要件を満たす必要があります。

注： アカウントで App Volumes の機能を使用できるようになっていて、コンソールの [キャプチャ] アクションを使用して App Volumes アプリケーションをインベントリに追加すると、システムは、2 台のデスクトップ仮想マシンのデスクトップ割り当てを生成して、キャプチャ ワークフローをサポートします。キャパシティは、キャプチャ ワークフローの実行中に、これらのデスクトップの作成にも対応する必要があります。環境のアプリケーションのキャプチャが完了したら、そのデスクトップ割り当てを削除できます。

また、Microsoft Azure 仮想マシン モデルの第1世代仮想マシン、第2世代仮想マシンを使用する場合は、Windows 10 および Windows 11 のゲスト OS に関する次のサポート マトリックスに注意してください。

Azure 仮想マシン モデル	Windows 10	Windows 11
第1世代仮想マシン	サポートされています	サポート対象外
第2世代仮想マシン	サポート対象外	サポートされています

<input type="checkbox"/>	<p>ゴールド イメージの基本 - サポートされている1つまたは複数の Microsoft Azure 仮想マシン構成。</p> <ul style="list-style-type: none"> Standard_DS2_v2 Standard_NV12s_v3 (サービスの自動化された [Marketplace からの仮想マシンのインポート] ウィザードまたは手動インポート、および NVIDIA GRID グラフィックス ドライバの場合)、Standard_NV8as_v4 (手動インポート方法と AMD グラフィックス ドライバの場合) Standard_D4s_v3 <p>コンソールの自動化された [Marketplace からの仮想マシンのインポート] ウィザードを使用してベース仮想マシンを作成する場合、システムはデフォルトで上記の仮想マシン サイズの1つを自動的に使用します。システムのデフォルトの選択は、内部設定と特定のオペレーティング システム (OS) に基づいています。</p> <p>システムは、シングルポッド イメージとマルチポッド イメージの両方に示されているモデルを使用します。</p> <p>[Marketplace からの仮想マシンのインポート] ウィザードで以下が作成されます。</p> <ul style="list-style-type: none"> 非 GPU、Windows 11 以外、Standard_DS2_v2 仮想マシン 非 GPU、Windows 11 使用、Standard_D4s_v3 仮想マシン GPU 対応、Standard_NV12s_v3 仮想マシン
<input type="checkbox"/>	<p>VDI デスクトップ割り当てのデスクトップ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構成を除く)。</p> <p>本番環境の場合、VMware スケール テストでは、最低2つの CPU を持つモデルを使用することをお勧めします。</p>
<input type="checkbox"/>	<p>ファームの RDSH 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 RDS ファーム操作と互換性のない構成を除く)。</p> <p>この要件は、Microsoft Windows 10 Enterprise マルチセッションまたは Windows 11 Enterprise マルチセッションを実行している仮想マシンが Horizon Cloud で使用されている場合にも適用されます。Microsoft Azure Virtual Desktop ドキュメントの Microsoft Windows Enterprise マルチセッション FAQ で説明されているように、Microsoft Windows Enterprise マルチセッションは、以前は Microsoft Windows Server オペレーティング システムのみが提供できた複数の同時対話型セッションを許可する Remote Desktop Session Host (RDSH) タイプです。RDS サーバに適用される Horizon Cloud ワークフローは、Microsoft Windows Enterprise マルチセッションに適用できます。</p> <p>本番環境の場合、VMware スケール テストでは、最低2つの CPU を持つモデルを使用することをお勧めします。</p>

Image Management Service (IMS) の要件

2021年7月のリリースより、Horizon Cloud ポッドがすべてマニフェスト 2632 以降を実行していて、テナントで Universal Broker が有効になっている場合、それらのポッドで Horizon Image Management Service 機能を使用することができます。このサービスが提供するマルチポッド イメージ機能を使用する場合、追加要件があります。これらの機能を使用するためのシステム要件の詳細については、[Horizon Image Management Service のシステム要件](#)の「Microsoft Azure」セクションを参照してください。ポッドのサブスクリプションに関する追加要件の概要と、マルチポッド イメージを使用する場合のそのサブスクリプションの Horizon Cloud アプリケーション登録とそのサービス プリンシパルの概要を次の表に示します。

□	マルチポッド イメージに参加しているポッドによって使用されるサブスクリプションは、単一の Microsoft Azure Active Directory (AAD) テナント内にある必要があります。
□	<p>マルチポッド イメージに参加しているポッドによって使用される Horizon Cloud アプリケーション登録のサービス プリンシパルは、以下の要件のいずれか1つを満たす必要があります。</p> <ul style="list-style-type: none"> ■ 参加しているすべてのポッドとサブスクリプションで同じサービス プリンシパルが使用されている。 ■ 各サービス プリンシパルに、参加しているポッドで使用されるすべての Microsoft Azure サブスクリプションへの読み取りアクセス権がある。 <p>ポッドは異なるサブスクリプションに含まれている可能性が高いため、この読み取りアクセス権の要件により、参加している各ポッドのサブスクリプションは他の参加しているポッドのサブスクリプションを認識できるようになります。このように認識できることは、サービスにとって、マルチポッド イメージを作成するために Azure 共有イメージ ギャラリーの機能を使用する際に必要となります。</p>
□	<p>参加しているポッドのサービス プリンシパルによって使用される任意のカスタム ロールには、Azure 共有イメージ ギャラリーの使用に関連する次の権限が含まれている必要があります。</p> <ul style="list-style-type: none"> ■ Microsoft.Compute/galleries/read ■ Microsoft.Compute/galleries/write ■ Microsoft.Compute/galleries/delete ■ Microsoft.Compute/galleries/images/* ■ Microsoft.Compute/galleries/images/versions/*

Microsoft Windows オペレーティング システムのライセンス

項目は、インポートされた仮想マシン、ゴールド イメージ、RDSH 対応のファーム仮想マシン、および仮想デスクトップ仮想マシンの Microsoft Windows オペレーティング システムに関連します。Horizon Cloud がサポートする Microsoft Windows オペレーティング システムのリストについては、[VMware ナレッジベースの記事 KB78170](#) および [VMware ナレッジベースの記事 KB70965](#) を参照してください。

Horizon Cloud は、Horizon Cloud ワークフローを使用する過程で使用される 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。

ヒント: Windows 11 Enterprise マルチセッション、Windows 10 Enterprise マルチセッション、および Windows 7 Enterprise に固有の Microsoft Azure Virtual Desktop ライセンスの詳細については、Microsoft Azure のドキュメント トピック [Azure Virtual Desktop の価格設定](#) を参照してください。

<input type="checkbox"/>	次のいずれかのタイプのライセンス : Microsoft Windows 7 Enterprise、Microsoft Windows 10、Microsoft Windows 11 (単一セッション、VDI クライアント タイプ)
<input type="checkbox"/>	Microsoft Windows 10 Enterprise マルチセッションまたは Microsoft Windows 11 Enterprise マルチセッションのライセンス
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	Microsoft RDS ユーザーまたはデバイス CAL (またはその両方)

リファレンス アーキテクチャ

以下のアーキテクチャ ダイアグラムを参照してください。

図 3-1. ポッドが外部および内部ゲートウェイの両方で構成された Horizon クラウド ポッド アーキテクチャの図 (外部ゲートウェイはポッドと同じ VNet にデプロイされた; 外部ゲートウェイ仮想マシンに 3 つの NIC、内部ゲートウェイ仮想マシンに 2 つの NIC がある; 外部ゲートウェイのロード バランサに対してパブリック IP アドレスが有効)

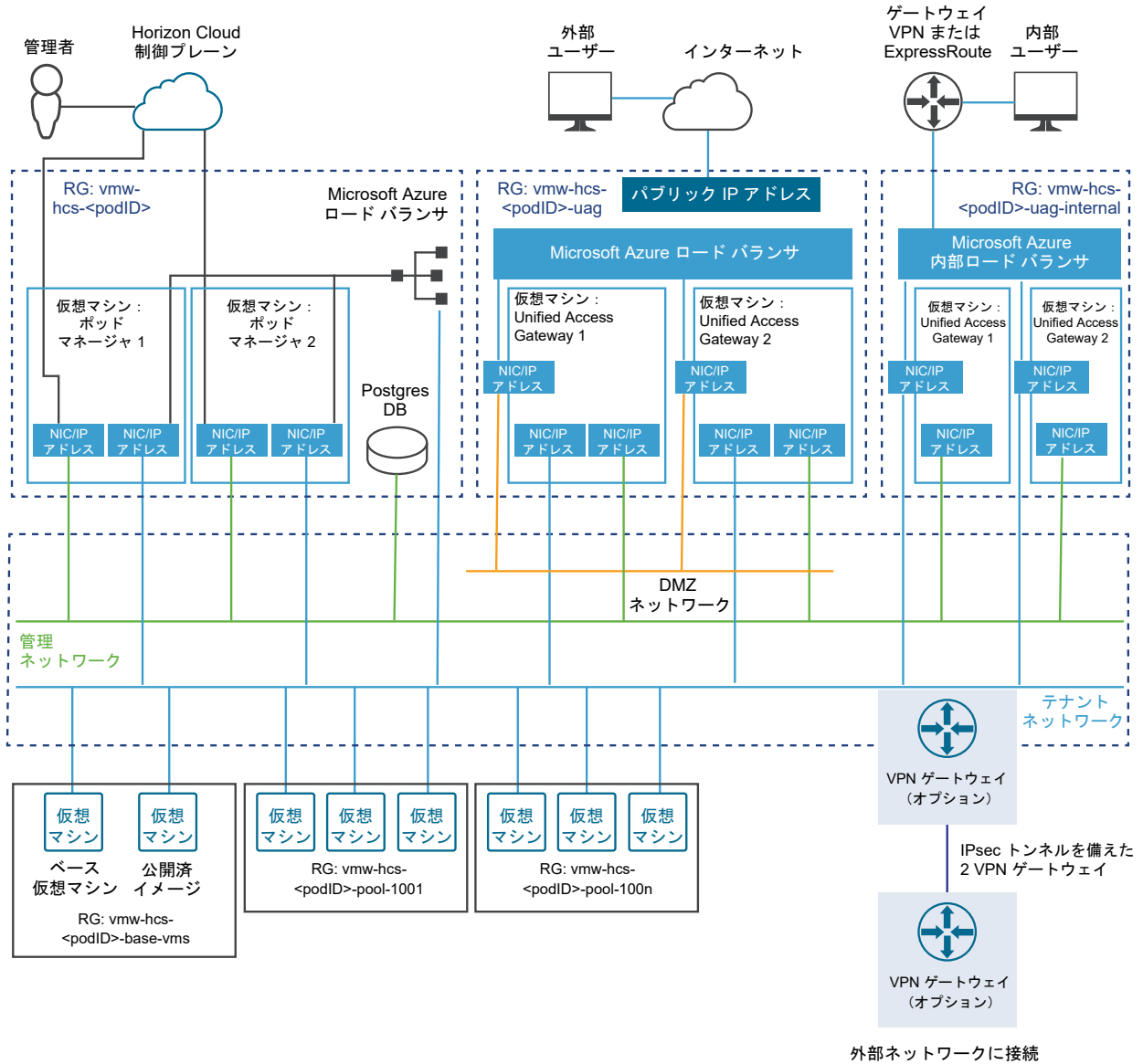
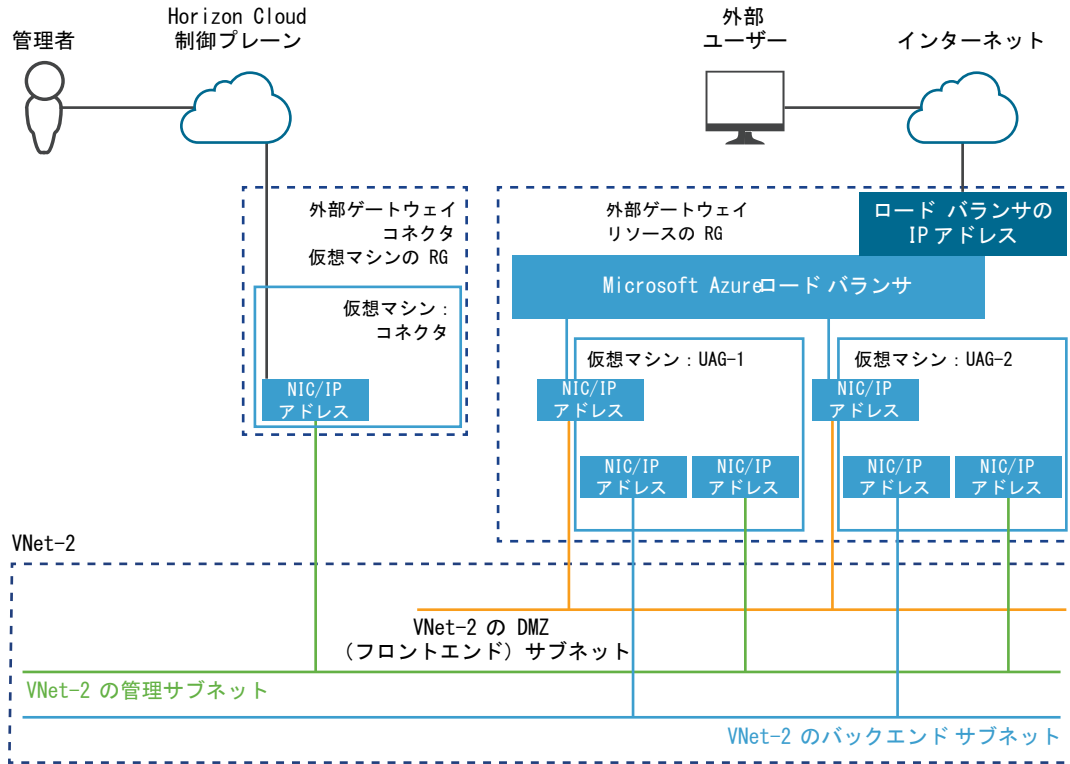


図 3-2. 外部ゲートウェイが独自の VNet にデプロイされ、3つのNICを備えたポッドのVNetから切り離され、ポッドデプロイヤーによって作成されたリソースグループにデプロイされたときの、外部ゲートウェイのアーキテクチャ要素の図



第1世代の Horizon Cloud 制御プレーンを使用する VMware Horizon 8 ポッド - 要件チェックリスト - 2023年11月2日のサービス更新に合わせて適切に更新されました

このページは、第1世代の Horizon Cloud 環境があり、Horizon ポッドをその環境にオンボーディングする場合にのみ使用します。

注目: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。KB-92424 で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

2022年8月の時点で、Horizon Cloud Service - next-gen は一般公開され、独自の『Horizon 制御プレーン next-gen の使用』ガイドを入手できます。

次世代と第1世代のどちらの環境を使用しているかは、環境にログインし、Horizon Universal Console ラベルに表示されるブラウザの URL フィールドのパターンで確認することができます。次世代環境の場合、コンソールの URL アドレスには /hcsadmin/ のような部分が含まれます。第1世代コンソールの URL の場合は、異なるセクション (/horizonadmin/) があります。

重要: Horizon Plus サブスクリバの場合は、このページを使用してポッドをオンボーディングしないでください。Horizon Plus サブスクリバの場合、Horizon Plus サブスクリプションでライセンス供与された機能を使用するには、これらの Horizon デプロイを次世代の制御プレーンにオンボーディングする必要があります。このページの内容は、第1世代の制御プレーンのみを対象としています。

Horizon Plus サブスクリバの場合は、次世代の制御プレーンにオンボーディングして Horizon Edge のデプロイを開始する最初の手順について、このページの [Horizon Plus](#) に関する情報を参照してください。

概要

次のタスクを完了して、ポッドを第1世代の Horizon Cloud 制御プレーンにオンボーディングするために Horizon 8 ポッド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。

注: 本書の執筆時点では、第1世代の Horizon Cloud は Horizon 7 バージョン 7.13 および Horizon 8 バージョン 1以降をサポートしています。Horizon ポッドと Horizon 8 ポッドの名前は、第1世代のドキュメントで同じ意味で使用され、Horizon Connection Server タイプのポッドのサポート対象バージョンを意味します。

チェックリスト対象者

このチェックリストは、主に、2023年5月のサービスリリース以前に、ポッドがテナント環境にオンボーディングされていないクリーンスレート、グリーンフィールドの Horizon Cloud ユーザー アカウントを対象としています。

次のセクションに記載されている要件の一部は、ポッドでサブスクリプション ライセンスを使用する目的で Horizon ポッドを正常にオンボーディングするために必要なものです。一部の要件は、ポッドでの Horizon Cloud 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。

参考までに、Horizon ポッドをクラウド接続するワークフローの概要については、[Horizon ポッドの Horizon Cloud 制御プレーンへのオンボーディング](#)を参照してください。

Horizon Cloud 制御プレーンの要件

☐	Horizon Cloud 制御プレーンにログインするためのアクティブな VMware Customer Connect アカウント (My VMware という名前は、VMware Customer Connect の以前の名前でした)。
☐	有効な Horizon ユニバーサル ライセンス。このライセンスの詳細については、 Horizon ユニバーサル ライセンスページ を参照してください。

Horizon ポッドと Horizon Cloud Connector の要件

☐	<p>VMware 相互運用性マトリックスに記載されているように、Horizon Cloud Connector バージョンと Horizon バージョン間の相互運用性のためには Horizon ポッドが 7.13.0 より前のバージョンで実行されてはなりません。また、クラウド接続されたポッドで最新のクラウド サービスと機能を使用するには、最新バージョンの Horizon ポッド ソフトウェアを実行する必要があります。</p> <p>重要： Horizon Connection Server の複製されたインスタンスをクラウド プレーンに接続するユースケースはサポートされていません。クラウド プレーンにすでに接続されている Horizon Connection Server インスタンスがあり、その Horizon Connection Server インスタンスを複製し、その複製されたインスタンスをクラウド プレーンに接続しようとすると、予期しない結果が発生します。</p>
☐	<p>本書の執筆時点では、新しいデプロイの場合は、Horizon Cloud Connector バージョン 2.2.x 以降を使用することを強くお勧めします。最新バージョンの 2.2.x より前のバージョンは、最新の修正および改善が含まれていないため、新しいデプロイには使用しないでください。</p> <p>クラウド接続されたポッドで最新のクラウド サービスおよび機能を使用し、最新のセキュリティの修正を適用するには、最新バージョンの Horizon Cloud Connector を実行する必要があります。</p> <p>Horizon Cloud Connector アプライアンスのデプロイ手順では、次を使用します。</p> <ul style="list-style-type: none"> ■ 固定 IP アドレス ■ DNS 正引きおよび逆引き参照レコード

□

Horizon Cloud Connector 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 ポッドのアーキテクチャ（オールイン SDDC またはフェデレーション 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。

オールイン SDDC アーキテクチャ

オールイン SDDC アーキテクチャでは、アプライアンスの OVA 形式が VMware SDDC 内にデプロイされます。

バージョン 2.2.x

- プライマリ ノード：vCPU x 4、8 GB メモリ (RAM)、40 GB データストア
- 追加の各ワーカー ノード：vCPU x 4、8 GB メモリ (RAM)、40 GB データストア

バージョン 2.3.x

- プライマリ ノード：vCPU x 4、8 GB メモリ (RAM)、40 GB データストア
- 追加の各ワーカー ノード：vCPU x 4、8 GB メモリ (RAM)、40 GB データストア

バージョン 2.4.x

- プライマリ ノード：vCPU x 4、8 GB メモリ (RAM)、40 GB データストア
- 追加の各ワーカー ノード：vCPU x 4、8 GB メモリ (RAM)、40 GB データストア

フェデレーション アーキテクチャ

フェデレーション アーキテクチャでは、クラウドネイティブ形式のアプライアンスが特定のクラウドネイティブ インフラストラクチャ内にデプロイされます。以下のリストは、現在サポートされているクラウドネイティブ形式で、ファイルのダウンロードが可能です。使用可能なクラウドネイティブ形式は、Horizon Cloud Connector の特定のバージョンごとに異なります。

アプライアンスのデプロイに使用する基盤となるマシン インスタンスは、次のリソース要件以上を満たしている必要があります。

バージョン 2.2.x

これらのデプロイでは、プライマリ ノードのみの使用がサポートされます。

- Azure VMware Solution (AVS) - vCPU x 8、32 GB メモリ (RAM)、40 GB データストア。Azure Cloud インスタンス Standard_D8_v3 は、8 個以上の vCPU に対して提供するサポート検証済みのインスタンスです。
- Google Cloud VMware Engine (GCVE) - vCPU x 8、32 GB メモリ (RAM)、40 GB データストア。Google Cloud インスタンス n2-standard-8 は、8 個以上の vCPU に対して提供するサポート検証済みのインスタンスです。
- VMware Cloud on AWS - vCPU x 8、16 GB メモリ (RAM)、40 GB データストア。Amazon インスタンス c5.2xlarge は、8 個以上の vCPU に対して提供するサポート検証済みのインスタンスです。

バージョン 2.3.x

これらのデプロイでは、プライマリ ノードのみの使用がサポートされます。

- Azure VMware Solution (AVS) - vCPU x 8、32 GB メモリ (RAM)、40 GB データストア。Azure Cloud インスタンス Standard_D8_v3 は、8 個以上の vCPU に対して提供するサポート検証済みのインスタンスです。
- Google Cloud VMware Engine (GCVE) - vCPU x 8、32 GB メモリ (RAM)、40 GB データストア。Google Cloud インスタンス n2-standard-8 は、8 個以上の vCPU に対して提供するサポート検証済みのインスタンスです。
- VMware Cloud on AWS - vCPU x 8、16 GB メモリ (RAM)、40 GB データストア。Amazon インスタンス c5.2xlarge は、8 個以上の vCPU に対して提供するサポート検証済みのインスタンスです。

バージョン 2.4.x

これらのデプロイでは、プライマリ ノードのみの使用がサポートされます。

- Azure VMware Solution (AVS) - vCPU x 8、32 GB メモリ (RAM)、40 GB データストア。Azure Cloud インスタンス Standard_D8_v3 は、8 個以上の vCPU に対して提供するサポート検証済みのインスタンスです。
- Google Cloud VMware Engine (GCVE) - vCPU x 8、32 GB メモリ (RAM)、40 GB データストア。Google Cloud インスタンス n2-standard-8 は、8 個以上の vCPU に対して提供するサポート検証済みのインスタンスです。

	<ul style="list-style-type: none"> ■ VMware Cloud on AWS - vCPU x 8、16 GB メモリ (RAM)、40 GB データストア。Amazon インスタンス c5.2xlarge は、8 個以上の vCPU に対して提供するサポート検証済みのインスタンスです。
□	<p>Horizon Cloud Connector とポッドの Connection Server をペアリングするときにポッドのオンボーディング プロセスに必須の Active Directory ユーザー。この Active Directory ユーザーには、ポッドの Horizon Console ([グローバル管理者ビュー] - [ロールの権限] - [管理者]) に示すように、root アクセス グループにポッドの事前定義された 管理者 ロールが必要です。つまり、ポッドのソフトウェア バージョンに適用される VMware Horizon 7 または VMware Horizon 8 ドキュメントの『Horizon 管理』ガイドまたは『Horizon Console 管理』ガイドで説明されているように、ポッドのオンボーディング プロセスに指定された Active Directory ユーザーはそのポッドのスーパー ユーザーです。</p>

Active Directory ドメイン - ライセンスを超えて完全なコンソールサービスとクラウド プレーン サービスが必要な場合を除き、Horizon 8 ポッドのオプション

ヒント: 第1世代の管理ガイドの「[Active Directory ドメイン登録](#)」で説明されているように、Active Directory ドメイン登録は省略することができ、クラウド接続された Horizon ポッドのデプロイは引き続きライセンスを受け取ります。少なくとも1つのドメインが構成されるまで、コンソールの「はじめに」ページで使用できるいくつかの機能を除き、ほとんどのコンソールはロックされたまま使用できなくなります。

コンソールを使用してクラウド接続された Horizon ポッドの Active Directory ドメインを登録する場合は、次の要件を満たしていることを確認してください。

注: テナントの最初のポッドが Horizon Connection Server タイプのポッドである場合は、コンソールを使用して Active Directory ドメインを登録するときに、ドメイン参加アカウント情報の入力を省略することができ、このようなポッドのクラウド プレーン サービスは正常に動作します。

ただし、ドメイン参加アカウント情報の入力を省略することを選択し、後でこの同じテナントに Horizon Cloud ポッド デプロイを追加し、そのポッドが以前に登録した Active Directory ドメイン内のエンド ユーザーにリソースをプロビジョニングするように計画する場合は、そのポッドをデプロイした後にドメイン参加情報を構成することを忘れないでください。Horizon Cloud ポッドをデプロイした後、ドメイン参加情報が構成解除されたことがコンソールから自動的に通知されることはなく、そのポッドからエンドユーザー リソースをプロビジョニングするには、ドメイン参加情報が必要です。このようなポッドのドメイン参加要件については、Horizon Cloud ポッドのチェックリストを参照してください。

□	<p>サポートされる Microsoft Windows Active Directory Domain Services (AD DS) ドメイン機能レベル:</p> <ul style="list-style-type: none"> ■ Microsoft Windows Server 2008 R2 ■ Microsoft Windows Server 2012 R2 ■ Microsoft Windows Server 2016
□	<p>同じ Horizon Cloud テナントのすべてのクラウド接続されたポッドは、それらのポッドをクラウド制御プレーンにオンボーディングするときに、Active Directory ドメインの同じセットを認識する必要があります。この認識要件は、最初のポッドの後にポッド フリートにオンボーディングされる追加の Horizon ポッドだけでなく、同じクラウド テナントを使用して Microsoft Azure にデプロイされる Horizon Cloud ポッドにも適用されます。</p>

<p>□</p>	<p>ドメイン バインド アカウント。</p> <ul style="list-style-type: none"> ■ 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。 <ul style="list-style-type: none"> ■ 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) ■ VMware Horizon オンプレミス製品に精通しているのであれば、上記の権限は、この Horizon オンプレミスのドキュメント トピックに記載されている、Horizon オンプレミス製品のセカンダリ認証情報アカウントに必要なセットと同じであることがわかります。 ■ 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、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る必要があります。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。 <p>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する必要があります。</p> <p>詳細および要件については、Horizon Cloud の運用に必要なサービス アカウントを参照。</p>
<p>□</p>	<p>補助ドメイン バインド アカウント (上記と同じアカウントは使用できません)。</p> <ul style="list-style-type: none"> ■ 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。 <ul style="list-style-type: none"> ■ 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) ■ VMware Horizon オンプレミス製品に精通しているのであれば、上記の権限は、この Horizon オンプレミスのドキュメント トピックに記載されている、Horizon オンプレミス製品のセカンダリ認証情報アカウントに必要なセットと同じであることがわかります。 ■ 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、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る必要があります。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。 <p>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する必要があります。</p> <p>詳細および要件については、Horizon Cloud の運用に必要なサービス アカウントを参照。</p>
<p>□</p>	<p>Active Directory グループ</p> <ul style="list-style-type: none"> ■ Horizon Cloud 管理者 — Horizon Cloud 管理者の Active Directory セキュリティ グループ。Horizon Cloud 管理ユーザーとドメイン参加アカウントが含まれています。このグループには、Horizon Cloud でスーパー管理者ロールが付与されます。 ■ Horizon Cloud ユーザー — Horizon Cloud の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と公開済みアプリケーションにアクセスするユーザーの Active Directory セキュリティ グループ。

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 ボッドを Horizon Cloud にオンボーディングするため、およびボッド、そのボッドとペアリングされた Horizon Cloud Connector、Horizon Cloud 制御プレーンを使用する Horizon Cloud Connector での継続的な運用のために必要です。Horizon Cloud Connector と Horizon ボッドを使用するときの DNS、ポート、およびプロトコルの要件を参照してください。
---	---

Universal Broker

コンソールを使用してテナントの Universal Broker を構成する場合は、次の表に記載されている項目のうち、目的のオプションに該当する項目を満たしていることを確認してください。詳細については、[Universal Broker の構成](#)を参照してください。

□	ボッドのペアリングされた Horizon Cloud Connector からのアウトバンド通信は、特定のポートおよびプロトコルを使用して特定の DNS 名を解決し、アクセスする必要があります。これは Universal Broker の構成および継続的な運用のために必要です。Horizon ボッド - Universal Broker のポートとプロトコルの要件を参照してください。
□	提供するエンドユーザー接続のタイプに応じて、以下の構成が必要です。 <ul style="list-style-type: none"> ■ インターネットからのエンドユーザー接続で、仮想デスクトップおよびアプリケーションを起動する場合は、ボッドで外部 Unified Access Gateway が構成されている必要があります。 ■ すべてのエンドユーザー接続が常に内部ネットワークからのものである場合、ボッドでは Unified Access Gateway は必要ありません。ただし、Universal Broker でこれらの内部エンドユーザー接続に 2 要素認証を適用する場合は除きます。
□	オプション：カスタムの FQDN。エンド ユーザーがこれを使用して Universal Broker サービスおよびその FQDN に基づく証明書にアクセスします。VMware 提供の仲介 FQDN を使用する場合、カスタム FQDN は必要ありません。
□	任意。Universal Broker で 2 要素認証を適用する場合、ボッドには、認証サーバへの 2 要素認証用に構成された外部 Unified Access Gateway が必要です。Universal Broker は認証要求を Unified Access Gateway に渡します。後者は認証サーバと通信し、応答を中継して Universal Broker に返します。この外部 Unified Access Gateway 構成には、次の項目が必要です。 <ul style="list-style-type: none"> ■ 認証サーバの名前を解決するための Unified Access Gateway の DNS アドレス ■ 認証サーバへのネットワーク ルーティングを解決する Unified Access Gateway のルート

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 サーバー 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）

第1世代テナント - Horizon ポッドをオンボーディングしてそのポッドで第1世代の Horizon 制御プレーン サービスを使用する

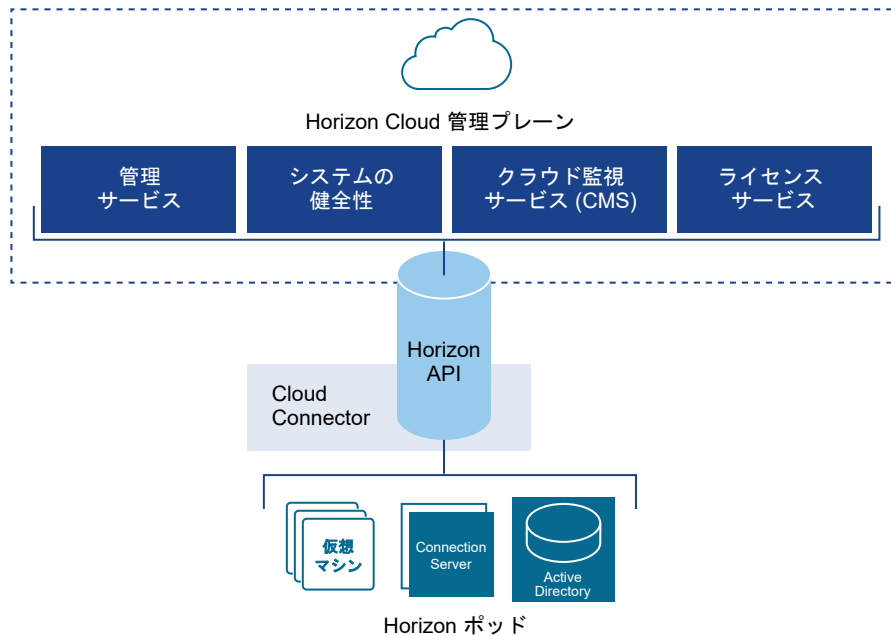
Horizon ポッドを第1世代の Horizon Cloud テナント環境にオンボーディングし、そのポッドでクラウド ホスト型のサービスを使用します。このようなクラウド ホスト型サービスには、クラウド接続されたポッド向けの機能およびワークフローが含まれます。どちらのユースケースでも、Horizon のデプロイを Horizon Cloud のクラウドベース管理プレーンに接続するコンポーネントである VMware Horizon® Cloud Connector™ を使用する必要があります。この接続により、クラウド接続された Horizon ポッドにサブスクリプション ライセンスが適用され、ポッドでの Cloud Monitoring Service (CMS) や Universal Broker などの制御プレーン サービスが有効になります。

注目: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

2022年8月の時点で、Horizon Cloud Service - next-gen は一般公開され、独自の『Horizon 制御プレーン next-gen の使用』ガイドを入手できます。

次世代と第1世代のどちらの環境を使用しているかは、環境にログインし、Horizon Universal Console ラベルに表示されるブラウザの URL フィールドのパターンで確認することができます。次世代環境の場合、コンソールの URL アドレスには /hcsadmin/ のような部分が含まれます。第1世代コンソールの URL の場合は、異なるセクション (/horizonadmin/) があります。

サポートされるポッド タイプを第1世代のクラウド制御プレーンに初めてオンボーディングするプロセスの概要については、「[第1世代テナント - Horizon Cloud のポッドのデプロイとオンボーディング](#)」を参照してください。



重要： テナントのポッド フリートは、Horizon Cloud ポッドと Horizon ポッドの両方で構成できます。ポッド フリート内のすべてのポッドは、同じ Active Directory ドメインのセットを認識できる必要があります。フリート内にすでに Horizon Cloud のポッドがあり、最初の Horizon ポッドを接続する場合は、Horizon ポッドを接続したときに Horizon ポッドがすでに Horizon Cloud テナントに登録されている Active Directory ドメインを認識できることを確認する必要があります。Active Directory のドメイン登録ワークフローの詳細については、[Horizon Cloud 環境での最初の Active Directory ドメイン登録の実行を参照してください](#)。

Horizon Cloud Connector を使用した、Horizon ポッド向けのサブスクリプション ライセンスのアクティブ化と、クラウド ホスト型サービスの有効化

Horizon Cloud Connector は、Horizon ポッドと Horizon Cloud の橋渡しをする仮想アプライアンスです。Horizon Cloud Connector は、Horizon サブスクリプション ライセンス、健全性ステータス ダッシュボード、および Horizon ヘルプ デスク ツールなどを含む、お使いの Horizon ポッドでのクラウド ホスト型のサービスを使用するために必要となります。

Horizon サブスクリプション ライセンス

Horizon サブスクリプション ライセンスは、スタンドアローンの Horizon パッケージとして利用できます。また、Workspace ONE エンタープライズ バンドルの一部としても使用できます。Horizon サブスクリプション ライセンスでは、同じ製品をより「柔軟な展開」オプションがある状態で提供します。Horizon サブスクリプション ライセンスにより、データセンター、プライベート クラウド、および VMware Cloud on AWS などのサポートされているパブリック クラウドでの Horizon のデプロイが可能になります。Horizon Cloud Connector を使用してポッドを Horizon Cloud にオンボーディングする手順を完了すると、VMware はサブスクリプション ライセンスをアクティブ化します。48 時間以内に、ライセンス サービスはそのクラウド接続されたポッドにライセンスを適用し、Horizon 管理のライセンス画面に次のメッセージが表示されます。

ライセンスと使用状況

ライセンス 使用量 カスタマー エクスペリエンス プログラム

ライセンスを編集 ① 無期限ライセンスを使用する ②

ライセンスキー

✔ Horizon サブスクリプションライセンス
License Service に接続されています。
Horizon は、License Service に接続され、サブスクリプション ライセンスを使用しています。

ライセンスの有効期限 Mon Mar 01 2027 08:00:00 GMT+0800 (中国標準時)

<https://my.vmware.com> から Horizon ライセンスを購入するには、アクティブな My VMware アカウントが必要です。Horizon Cloud Connector を OVA ファイルとしてダウンロードできるリンクがよろこ E メールで届きます。

vSphere Web Client から Horizon Cloud Connector 仮想アプライアンスをデプロイする場合、Cloud Connector を、サブスクリプション ライセンスまたはクラウド ホスト型サービスを使用するために Horizon Cloud に接続するポッドの Connection Server とペアリングします。ペアリング プロセスにおいて、Horizon Cloud Connector 仮想アプライアンスが Connection Server を Horizon Cloud に接続し、Horizon サブスクリプション ライセンスおよびその他のサービスを管理します。Horizon サブスクリプション ライセンスがある場合、VMware Horizon 製品のアクティベーションのための Horizon ライセンス キーを手動で入力する必要はありません。ただし、vSphere、App Volumes などのサポート コンポーネントを有効にするには、ライセンス キーを使用する必要があります。

Horizon ポッド用のクラウド ホスト型サービス

Horizon ポッドをクラウド接続されたポッド フリートに追加すると、Cloud Monitoring Service (CMS) などの Horizon Cloud が提供するクラウド ホスト型サービス、機能、およびワークフローを活用できます。「Horizon Cloud で提供されるクラウド監視サービスの統合された可視性、健全性監視、およびヘルプ デスク機能の紹介」を参照してください。

次のトピックを参照してください。

- 第1世代テナント - 第1世代 Horizon Cloud を使用した Horizon ポッドのデプロイ アーキテクチャ
- 第1世代テナント - Horizon ポッドの第1世代の Horizon Cloud 制御プレーンへのオンボーディング
- 第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件
- 第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備
- 第1世代テナント - 第1世代 Horizon Cloud Service を既存の Horizon ポッドに接続してクラウド ホスト型サービスを使用する

第1世代テナント - 第1世代 Horizon Cloud を使用した Horizon ポッドのデプロイ アーキテクチャ

この記事では、Horizon ポッドで使用されるさまざまなデプロイ アーキテクチャについて説明します。Horizon ポッドを第1世代 Horizon Cloud にオンボーディングする前に、まずそのデプロイ アーキテクチャを特定する必要

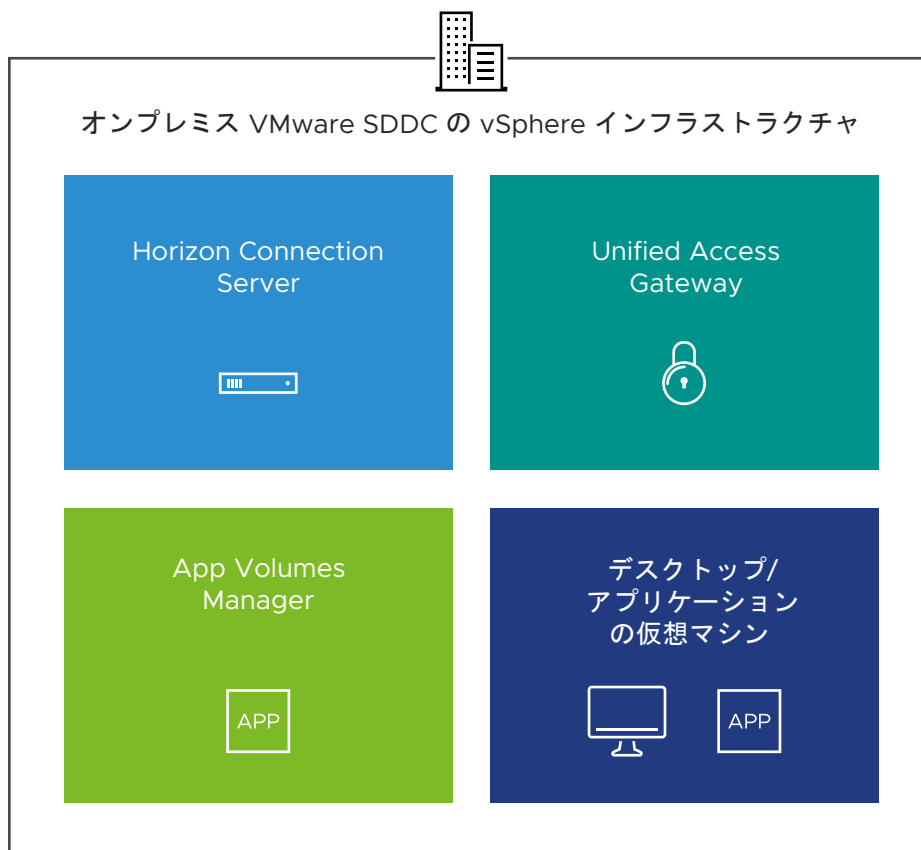
があります。これで、Horizon Cloud Connector アプライアンスをそのアーキテクチャにデプロイするために実行する必要がある手順が決定されます。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

Horizon ポッドは、[オンプレミス]、[オールイン SDDC]、または [フェデレーション] のいずれかのデプロイ アーキテクチャを使用してデプロイできます。

オンプレミス デプロイ アーキテクチャ

オンプレミス デプロイ アーキテクチャ



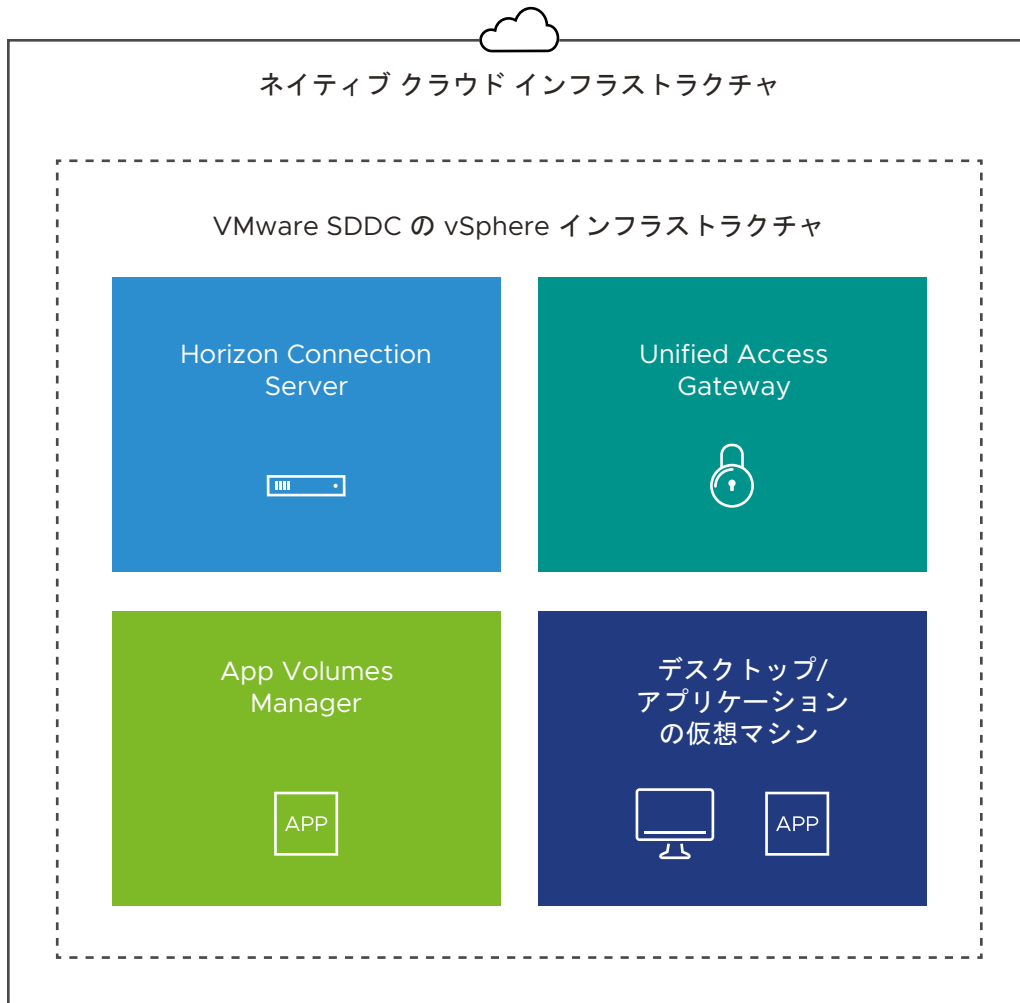
Horizon ポッドがオンプレミスでデプロイされると、ポッド コンポーネントは次のようにデプロイされます。

ポッド コンポーネント :	デプロイ先 :
<ul style="list-style-type: none"> ■ Horizon Connection Server ■ Unified Access Gateway ■ App Volumes Manager ■ 仮想デスクトップ、公開デスクトップ、公開アプリケーション用の仮想マシン (VM) 	オンプレミス VMware SDDC の vSphere インフラストラクチャ

注： オンプレミス ポッドを Horizon Cloud にオンボーディングする場合は、Horizon Cloud Connector をオンプレミス VMware SDDC の vSphere インフラストラクチャにデプロイする必要があります。

オールイン SDDC デプロイ アーキテクチャ

オールイン SDDC デプロイ アーキテクチャ



Horizon ポッドがオールイン SDDC アーキテクチャを使用してクラウド環境にデプロイされる場合、ポッド コンポーネントは次のようにデプロイされます。

ポッド コンポーネント :	デプロイ先 :
<ul style="list-style-type: none"> ■ Horizon Connection Server ■ Unified Access Gateway ■ App Volumes Manager ■ 仮想デスクトップ、公開デスクトップ、公開アプリケーション用の仮想マシン 	クラウド環境内の VMware SDDC の vSphere インフラストラクチャ

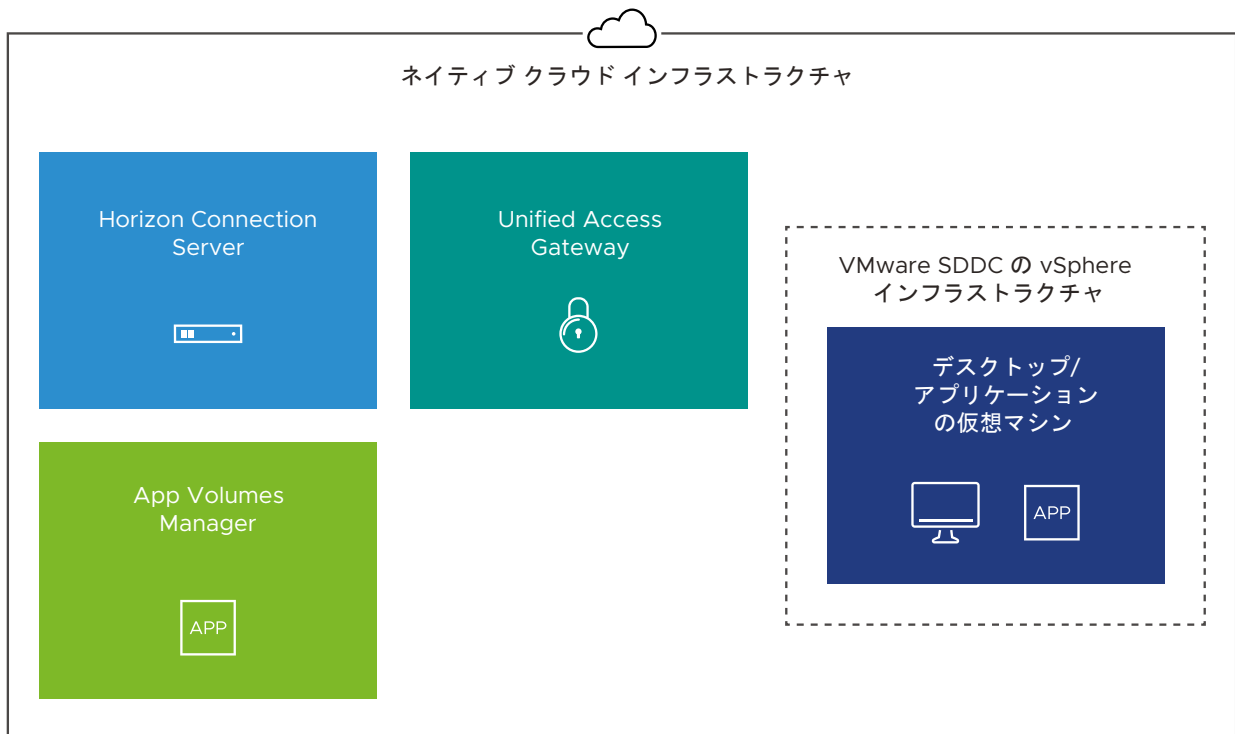
注： オールイン SDDC ポッドを Horizon Cloud にオンボーディングする場合は、Horizon Cloud Connector を VMware SDDC の vSphere インフラストラクチャにデプロイする必要があります。

たとえば、VMware Cloud on AWS にデプロイされたオールイン SDDC ポッドについて考えてみます。この場合：

- すべてのポッド コンポーネントは、VMware Cloud on AWS の vSphere インフラストラクチャ内にあります。
- Horizon Cloud Connector を VMware Cloud on AWS の vSphere インフラストラクチャにデプロイする必要があります。

フェデレーション デプロイ アーキテクチャ

フェデレーション デプロイ アーキテクチャ



Horizon ポッドがフェデレーション アーキテクチャを使用してクラウド環境にデプロイされる場合、ポッド コンポーネントは次のようにデプロイされます。

ポッド コンポーネント :	デプロイ先 :
仮想デスクトップ、公開デスクトップ、公開アプリケーション用の仮想マシン	クラウド環境内の VMware SDDC の vSphere インフラストラクチャ
<ul style="list-style-type: none"> ■ Horizon Connection Server ■ Unified Access Gateway ■ App Volumes Manager 	VMware SDDC 外のネイティブ クラウド インフラストラクチャ

注： 連携したポッドを Horizon Cloud にオンボーディングする場合は、Horizon Cloud Connector を VMware SDDC 外のネイティブ クラウド インフラストラクチャにデプロイする必要があります。

たとえば、Google Cloud VMware Engine (GCVE) にデプロイされた連携したポッドについて考えてみましょう。この場合：

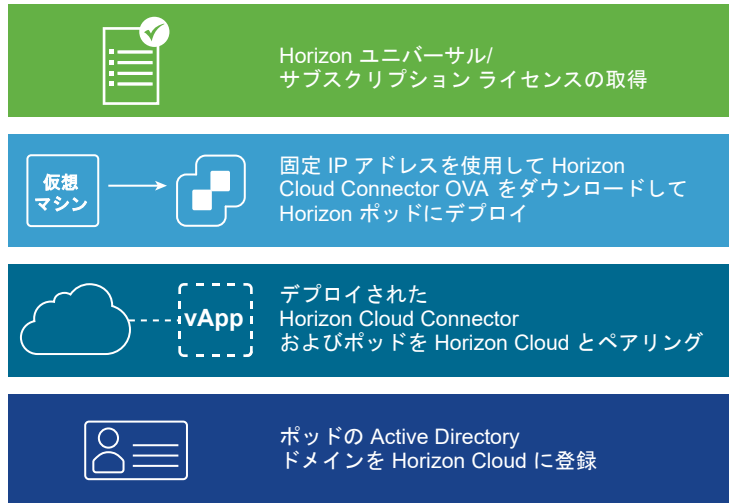
- 仮想デスクトップ、公開デスクトップ、公開アプリケーション用の仮想マシンは、GCVE の vSphere インフラストラクチャ内にあります。
- Horizon Connection Server、Unified Access Gateway、および App Volumes Manager はすべて、GCVE の外部にあるネイティブの Google Cloud Platform (GCP) インフラストラクチャにあります。
- Horizon Cloud Connector を GCVE 外のネイティブ GCP インフラストラクチャにデプロイする必要があります。

第1世代テナント - Horizon ポッドの第1世代の Horizon Cloud 制御プレーンへのオンボーディング

このリストは、最初のポッドを第1世代の制御プレーンにオンボーディングしていて、そのポッドがサポートされているデプロイ アーキテクチャのいずれかを使用してすでに有効になっている既存の Horizon ポッドである場合の手順の概要です。Horizon ポッドは、Horizon Connection Server ソフトウェアに基づいています。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

次の図は、全体的なフローを示しています。



オンボーディングの理由

Horizon ポッドを第1世代のクラウド プレーンにオンボーディングして、第1世代のクラウド プレーンが Horizon ポッドに提供する Cloud Monitoring Service (CMS) などのクラウド ホスト型サービスの使用を有効にします。CMS は、Horizon Cloud で提供される中心的なサービスの1つです。CMS は、クラウドに接続されたポッドに可視性、健全性監視、ヘルプ デスク サービスを提供します。

第1世代の制御プレーンにオンボーディングすると、そのポッドの Horizon Universal サブスクリプション ライセンスも有効になります。

クラウド接続された最初のポッドに対してこれらのオンボーディング手順を完了すると、オンボーディングされたポッドのサブスクリプション ライセンスが有効になります。さらに、Cloud Monitoring Service (CMS) など、制御プレーンがそのポッド タイプに提供するクラウドホスト型サービスの使用を開始できます。その時点で、追加のポッドをオンボーディングすることもできます。

開始する前にポッドをすべて準備する

このワークフローを開始する前に、サポートされているデプロイ設計のいずれかを使用して Horizon ポッドをデプロイしておく必要があります。次のリソースから特定のポッド デプロイ手順を取得します。

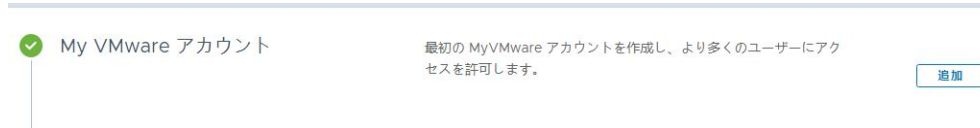
- [Horizon 7 のドキュメント](#)、[Horizon のドキュメント](#)。
- [Horizon on VMware Cloud on AWS の製品ページ](#)。
- [Tech Zone の Horizon on Azure VMware Solution アーキテクチャ](#)、[Tech Zone の Horizon on Azure VMware Solution 構成](#)。
- [Tech Zone の Horizon on Google Cloud VMware Engine アーキテクチャ](#)。

シーケンス

重要： 最初のポッドを Horizon Cloud に完全に接続する完全なシーケンスを完了してから、追加の Horizon ポッドを使用して Horizon Cloud Connector をデプロイします。このリリースの既知の問題により、Active Directory ドメイン登録およびスーパー管理者ロール割り当ての手順を一度も完了することなく Horizon Cloud Connector を使用して複数のポッドをクラウドに接続すると、Active Directory ドメイン登録の手順が失敗します。その時点で、必要な Active Directory ドメイン登録とスーパー管理者ロールの割り当ての手順を正常に完了する前に、クラウド接続された Horizon ポッドの1つ以外のすべてを接続解除する必要があります。

- 1 Horizon ユニバーサル ライセンスなどの Horizon サブスクリプション ライセンスの取得を含む**前提条件**を満たします。ポッドをクラウド制御プレーンにオンボーディングするプロセスの概要については、[Horizon Cloud のデプロイとポッドのオンボーディング](#)も参照してください。
- 2 Horizon ポッドを Horizon Cloud と接続するための DNS、ポート、およびプロトコルの要件が満たされていることを確認します。[第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件](#)を参照してください。
- 3 ご使用の環境で Horizon Cloud Connector 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プロキシ サーバを使用する必要がある場合は、必要なプロキシ設定を取得して、アプライアンスをポッドの環境にデプロイするときに指定できるようにします。
- 4 必要に応じて Horizon Cloud テナント ポータルにログインし、テナント環境に追加の管理者を構成します。

ヒント： テナント環境に最初に関連付けられている My VMware アカウントのみを使用して次の手順を実行してポッドをオンボーディングすることができますが、このプロセスの開始時に追加の管理者を構成することをお勧めします。テナント アカウントに関連付けられている My VMware アカウントが1つだけの場合に認証情報にアクセスできなくなると、新しい My VMware アカウントをテナント アカウントに関連付けるために VMware へのサービス リクエストを開く必要があるため、遅延が発生する可能性があります。このような遅延を防ぐには、最初に関連付けられた My VMware アカウントで cloud.horizon.vmware.com のテナント ポータルにログインし、画面の [全般設定] セクションの行を使用して「[Horizon Cloud テナント環境にログインする管理者を追加する](#)」に説明されている手順を実行します。



- 5 Horizon Cloud Connector 仮想アプライアンスをポッドの環境にデプロイします。[Horizon Cloud Connector をダウンロードしてデプロイする](#)の手順に従います。

注： Horizon Cloud Connector 1.9 をデプロイし、CMS などの Horizon Cloud Service の使用を有効にする場合は、デプロイ中に [フル機能] プロファイルを選択する必要があります。

- 6 仮想アプライアンスがパワーオンされた後、仮想アプライアンスへの SSH アクセスを有効にして、アプライアンスのオペレーティング システムでコマンドをリモートで実行できるようにします。コマンド ライン インターフェイスの使用による Horizon Cloud Connector への SSH アクセスの有効化の手順に従います。

注： SSH を有効にする手順は、ポッドがまだ Horizon Cloud とペアリングされていないときに使用されます。ポッドが Horizon Cloud と正常にペアリングされると、ブラウザベースの Horizon Cloud Connector 構成ポータルを使用して、仮想アプライアンスへの SSH アクセスを有効または無効にできます。

- 7 環境でプロキシを使用する必要があり、OVF デプロイ ウィザードでプロキシ関連の設定を指定しなかった場合は、仮想アプライアンスのプロキシ関連の設定を構成します。詳細については、[Horizon Cloud Connector 1.6 以降のプロキシ設定の変更](#)を参照してください。
- 8 Horizon Cloud Connector 仮想アプライアンスの IP アドレスを使用する代わりに、完全修飾ドメイン名 (FQDN) を使用してブラウザベースの Horizon Cloud Connector 構成ポータルにアクセスする場合は、FQDN を仮想アプライアンスの 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 Cloud Connector 仮想アプライアンスへの SSH セッションを開き、precheck.sh 診断スクリプトを実行して、ポッドのシステム コンポーネントとサービスの健全性を確認します。詳細については、[第1世代テナント - Horizon ポッドと仮想アプライアンスの第1世代 Horizon 制御プレーンとのペアリングの準備ができていることを確認する](#)を参照してください。
- 10 マッピングされた FQDN または仮想アプライアンスの IP アドレスを使用して、ブラウザベースの Horizon Cloud Connector 構成ポータルにログインし、コネクタとポッドの Connection Server をペアリングするオンボーディング手順を完了します。第1世代テナント - Horizon Cloud Connector 構成ポータルを使用して Horizon ポッドと第1世代 Horizon Cloud のペアリングを完了するで説明する手順を実行します。

ヒント： コネクタと Connection Server が正常にペアリングされると、Horizon Cloud Connector 構成ポータルに完了メッセージが表示されます。この時点で、VMware はサブスクリプション ライセンスをアクティベーションします。通常、アクティベーションは 30 分後に完了しますが、場合によっては最大 4 時間かかることがあります。ライセンスが有効になると、ポッドの Web ベースのコンソールの [製品ライセンスと使用] 画面に「ライセンス サービスに接続されました」というメッセージが表示されます。

ライセンスと使用状況

- 11 チームの標準的なプラクティスと環境に応じて、CA 署名付き証明書構成や、アプライアンスの root ユーザーのパスワード有効期限の設定などの領域で、Horizon Cloud Connector 仮想アプライアンスをオプションで構成します。このような一般的なタスクのリストと手順へのリンクについては、[ペアリングされた Horizon Cloud Connector の一般的な管理およびメンテナンス タスク](#)を参照してください。

- 12 デプロイ済みのポッドで **Active Directory** ドメインを登録します。ここでは、サービス アカウントの名前を提供することも含まれます。これらのサービス アカウントが、**Horizon Cloud の運用に必要なサービス アカウント**で説明されている要件を満たしていることを確認します。

ヒント: Active Directory ドメイン登録ワークフローを完了すると、Cloud Monitoring Service (CMS) など、すべてのクラウド ホスト型サービスを利用できます。ポッドの Active Directory ドメインがテナント環境に登録されるまで、これらの機能を含むコンソールの領域にはアクセスできません。

- 13 まれな、通常ではない状況として、テナント環境に 1600.0 より古いマニフェストを実行している Microsoft Azure の Horizon Cloud ポッドがすでにある場合、ドメイン参加アカウントをメンバーとして含む Active Directory グループに Horizon Cloud スーパー管理者ロールを付与する必要があります。『管理ガイド』の **Active Directory グループへの Horizon Cloud 管理ロールの割り当て**のトピックを参照してください。

第 1 世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件

Horizon Cloud Connector 仮想アプライアンスを Horizon ポッドとともに使用しているときに、アプライアンスが必要なドメイン ネーム サービス (DNS) のアドレスにアクセスできるように、ファイアウォールを構成する必要があります。さらに、このトピックで説明するように、プロキシ設定には構成済みのポートとプロトコルが必要で、DNS は特定の名前を解決する必要があります。次に、Horizon Cloud Connector 仮想アプライアンスがデプロイされ、ポッドを Horizon Cloud に正常に接続するための手順が完了したら、Horizon Cloud と仮想アプライアンス間の継続的な運用のために、特定のポートとプロトコルが必要となります。

重要: この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

「Horizon ポッドをオンボーディングし、そのポッドで Horizon サブスクリプション ライセンスまたはクラウド ホスト型のサービスを使用する場合」で説明されているように、Horizon Cloud Connector 仮想アプライアンスは、Horizon デプロイでサブスクリプション ライセンスをアクティブ化し、その Horizon デプロイでクラウド ホスト型のサービスを使用できるようにします。

注: (Horizon Cloud Connector 2.0 以降) 特に指定がない限り、次の DNS、ポート、およびプロトコルの要件は、Horizon Cloud Connector アプライアンスのプライマリ ノードとワーカー ノードに同様に適用されます。

VMware エコシステム内の**緊密な連携**で説明されているように、Horizon Cloud は、幅広い VMware エコシステムから入手可能な他の製品と併用できます。これらの他の製品には、追加の DNS 要件がある場合があります。このような追加の DNS 要件については、ここでは詳しく説明しません。このような DNS 要件については、クラウド 接続された Horizon ポッドと統合する特定の製品のドキュメント セットを参照してください。

テナント全体に適用されるポッドの接続およびサービス運用の DNS 要件

このセクションでは、テナント全体に適用されるポッドの接続およびサービス運用の DNS 要件について説明します。

Horizon Cloud Connector を使用して Horizon Cloud と Horizon ポッドを接続するための手順には、ブラウザを使用して Horizon Cloud Connector アプライアンスの IP アドレスに移動し、ログイン画面が表示される手順が含まれています。そのログイン画面を表示するためには、Horizon Cloud Connector アプライアンスと Horizon Cloud クラウド制御プレーン間のインターネット接続が必要です。アプライアンスは最初に HTTPS を使用して Horizon Cloud クラウド制御プレーンへの接続を確立してから、アウトバウンド インターネット ポート 443 を使用して永続的な WebSocket 接続を開きます。継続的な運用のために、Horizon Cloud Connector アプライアンスと Horizon Cloud 間の接続では、ポート 443 を使用するアウトバウンド インターネット接続が常に開いている必要があります。以下の Domain Name Service (DNS) 名が解決可能であり、以下の表に記載されている特定のポートおよびプロトコルを使用してアクセス可能であるようにする必要があります。

重要： 次の重要な点に注意してください。

- すべてのテナント アカウントで、DNS 名 `cloud.horizon.vmware.com` へのアクセスが必要です。テナント アカウントで指定されているリージョンの地域別制御プレーンの DNS 名へのアクセスに加えて、`cloud.horizon.vmware.com` へのアクセスが必要です。
- Horizon Cloud Connector は、業界で信頼されている認証局 (CA) である DigiCert によって署名された SSL 証明書を使用します。これらの証明書は、DigiCert ドメインの特定の DNS 名を参照する CRL (証明書失効リスト) と OCSP (オンライン証明書ステータス プロトコル) クエリを使用します。Horizon Cloud Connector 接続を確保するには、これらの DNS 名を、解決可能で仮想アプライアンスからアクセスできるように構成する必要があります。これらの DNS 名にアクセスできない場合、Horizon Cloud Connector 構成ポータルにアクセスできなくなります。特定の名称は DigiCert によって決定されるため、VMware によって管理されません。
- ポッドで Universal Broker の使用を有効にする場合は、DNS 名に加えて接続性の要件があります。詳細については、[Universal Broker のシステム要件](#) およびその関連トピックを参照してください。

「Horizon Service へようこそ」E メールには、自分のテナント アカウントがどの地域の制御プレーン インスタンスで作成されたかが示されます。「ようこそ」E メールが送信されたときに存在していた既知の問題により、受信した E メールには判読可能な名前ではなく、リージョンで使用されているシステム文字列名が表示されることがあります。「ようこそ」E メールにシステム文字列の名前が表示されている場合は、次の表を使用して、E メールに表示される文字列と地域別制御プレーンの DNS 名を関連付けることができます。

表 5-1. 地域別制御プレーンの DNS 名にマッピングされた「ようこそ」E メール内の地域

「ようこそ」E メール内の記載	地域別の DNS 名
USA	<code>cloud.horizon.vmware.com</code>
EU_CENTRAL_1 または Europe	<code>cloud-eu-central-1.horizon.vmware.com</code>
AP_SOUTHEAST_2 または Australia	<code>cloud-ap-southeast-2.horizon.vmware.com</code>
PROD1_NORTHCENTRALUS2_CP1 または USA-2	<code>cloud-us-2.horizon.vmware.com</code>
PROD1_NORTHEUROPE_CP1 または Europe-2	<code>cloud-eu-2.horizon.vmware.com</code>
PROD1_AUSTRALIAEAST_CP1 または Australia-2	<code>cloud-ap-2.horizon.vmware.com</code>
Japan	<code>cloud-jp.horizon.vmware.com</code>

表 5-1. 地域別制御プレーンの DNS 名にマッピングされた「ようこそ」E メール内の地域 (続き)

「ようこそ」E メール内の記載	地域別の DNS 名
UK	cloud-uk.horizon.vmware.com
Europe-3	cloud-de.horizon.vmware.com

ソース	ターゲット (DNS 名)	ポート	プロトコル	目的
Horizon Cloud Connector	<p>Horizon Cloud テナント アカウントで指定されている地域別制御プレーン インスタンスに応じた、次のいずれかの名前の cloud.horizon.vmware.com plus one。地域別のインスタンスは、Microsoft Azure および Horizon ボッドの Horizon Cloud へのデプロイとオンボーディングの記載どおりに、アカウントの作成時に設定されます。</p> <ul style="list-style-type: none"> ■ cloud-us-2.horizon.vmware.com ■ cloud-eu-central-1.horizon.vmware.com ■ cloud-eu-2.horizon.vmware.com ■ cloud-ap-southeast-2.horizon.vmware.com ■ cloud-ap-2.horizon.vmware.com ■ cloud-jp.horizon.vmware.com ■ cloud-uk.horizon.vmware.com ■ cloud-de.horizon.vmware.com 	443	TCP	<p>地域別制御プレーン インスタンス。</p> <hr/> <p>注： 以下に示すように、地域のインスタンスに加えて、すべてのテナント アカウントで Horizon Cloud Connector が cloud.horizon.vmware.com にアクセスできる必要があります。</p> <ul style="list-style-type: none"> ■ 米国： cloud.horizon.vmware.com, cloud-us-2.horizon.vmware.com ■ ヨーロッパ： cloud-eu-central-1.horizon.vmware.com, cloud-eu-2.horizon.vmware.com ■ アジア パシフィック： cloud-ap-southeast-2.horizon.vmware.com, cloud-ap-2.horizon.vmware.com ■ 日本： cloud-jp.horizon.vmware.com ■ 英国： cloud-uk.horizon.vmware.com ■ ドイツ： cloud-de.horizon.vmware.com
<p>注： (Horizon Cloud Connector 2.0 またはそれ以降) この要件は、プライマリ ノードのみ適用されます。</p> <p>Horizon Cloud Connector</p>	<p>Horizon Cloud アカウントにどの地域別制御プレーンが指定されているかに応じて異なります。</p> <ul style="list-style-type: none"> ■ 北米： kinesis.us-east-1.amazonaws.com ■ ヨーロッパ、ドイツ： kinesis.eu-central-1.amazonaws.com ■ オーストラリア： kinesis.ap-southeast-2.amazonaws.com 	443	TCP	Cloud Monitoring Service (CMS)

ソース	ターゲット (DNS 名)	ポート	プロトコル	目的
	<ul style="list-style-type: none"> ■ 日本 : kinesis.ap-northeast-1.amazonaws.com ■ 英国 : kinesis.eu-west-2.amazonaws.com 			
Horizon Cloud Connector	<p>*.digicert.com</p> <p>許可される DNS 名にワイルドカードを使用することを組織が推奨しない場合は、代わりに特定の名前を許可できます。たとえば、この記事の執筆時点では、証明書の検証に必要な特定の DNS 名は次のとおりです。</p> <ul style="list-style-type: none"> ■ ocsp.digicert.com ■ crl3.digicert.com ■ crl4.digicert.com ■ www.digicert.com/CPS <p>これらの DNS 名は、DigiCert によって決定され、変更される可能性があります。証明書に必要な特定の名前を取得する方法については、VMware ナレッジベースの記事 KB79859 を参照してください。</p>	80、443	HTTP、HTTPS	認証局 DigiCert から検証を取得するために使用される CRL または OCSP クエリ

ソース	ターゲット (DNS 名)	ポート	プロトコル	目的
Horizon Cloud Connector	Horizon Cloud テナント アカウントで指定されている地域別制御プレーンのインスタンスに応じた、次のいずれかの名前。地域別のインスタンスは、 Microsoft Azure および Horizon ボードの Horizon Cloud へのデプロイとオンボーディングの記載どおりに、アカウントの作成時に設定されます。 <ul style="list-style-type: none"> ■ connector-azure-us.vmwarehorizon.com ■ connector-azure-eu.vmwarehorizon.com ■ connector-azure-aus.vmwarehorizon.com ■ connector-azure-jp.vmwarehorizon.com ■ connector-azure-uk.vmwarehorizon.com ■ connector-azure-de.vmwarehorizon.com 	443	TCP	Universal Broker サービスのリージョンインスタンス <ul style="list-style-type: none"> ■ 米国： connector-azure-us.vmwarehorizon.com ■ ヨーロッパ： connector-azure-eu.vmwarehorizon.com ■ オーストラリア： connector-azure-aus.vmwarehorizon.com ■ 日本： connector-azure-jp.vmwarehorizon.com ■ 英国： connector-azure-uk.vmwarehorizon.com ■ ドイツ： connector-azure-de.vmwarehorizon.com
Horizon Cloud Connector	hydra-softwarelib-cdn.azureedge.net	443	TCP	Horizon Cloud Connector の自動更新中に CDN リポジトリから必要な OVF および VMDK ファイルをダウンロードするために使用されます。

Horizon Cloud Connector 仮想アプライアンスで必要となるポートとプロトコル

Horizon Cloud Connector と Horizon Cloud の間の継続的な運用のためには、次の表のポートとプロトコルが必要です。

表 5-2. Horizon Cloud Connector のポート

ソース	ターゲット	ポート	プロトコル	説明
Horizon Cloud Connector	Horizon Cloud	443	HTTPS	Horizon Cloud Connector を Horizon Cloud とペアリングしてデータを転送するために使用されます。
Horizon Cloud Connector	Connection Server	443	HTTPS	Connection Server への API 呼び出し。
Horizon Cloud Connector	Connection Server	4002	TCP	Cloud Connector と Connection Server との間の Java Message Service (JMS) 通信
Horizon Cloud Connector アプライアンスの新しいバージョン	Horizon Cloud Connector アプライアンスの既存のバージョン	22	SSH	更新プロセスの開始要求を待ちます。
Web ブラウザ	Horizon Cloud Connector	443	HTTPS	ペアリング プロセスの開始を待ちます。
ネットワーク上のクラウド接続された Horizon ボッドからのデスクトップまたはサーバ仮想マシンの Cloud Monitoring Service エージェント	Horizon Cloud Connector アプライアンス	11002	TCP	サーバまたはデスクトップ仮想マシン上の Cloud Monitoring Service エージェントがデータを Horizon Cloud Connector に送信するために使用されます。
Horizon Cloud Connector	vCenter Server の SDK エンドポイント。 例 : <code>https://<vCenter Server の FQDN>/sdk</code>	443	TCP	このオプションのポート構成は、自動更新機能で使用するために必要です。自動更新機能はデフォルトで無効になっており、リクエストがあった場合のみボッドごとに有効にできます。Horizon Cloud Connector 仮想アプライアンスの自動更新の構成を参照してください。
Horizon Cloud Connector	vCenter Server の SDK エンドポイント。 例 : <code>https://<vCenter Server の FQDN>/sdk</code>	443	HTTPS	このオプションのポート構成は、Horizon Image Management Service で使用するために必要です。テナント アカウントで Horizon Image Management Service 機能が有効になっている場合にのみ、このポートとプロトコルを構成する必要があります。『クラウドからの Horizon イメージの管理』を参照してください。

第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備

Horizon ポッドをオンボーディングして第1世代の Horizon 制御プレーン サービスを使用する場合は、Horizon Cloud Connector アプライアンスをデプロイしてオンボーディング ウィザードを実行する前に、以下の項目を確認します。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。KB-92424 で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

- 4章 第1世代の Horizon Cloud 制御プレーンを使用する VMware Horizon 8 ポッド - 要件チェックリスト - 2023年11月2日のサービス更新に合わせて適切に更新されましたに記載されている前提条件を満たしていることを確認する。
- Horizon Cloud Connector 仮想アプライアンスとペアリングするポッドの Connection Server インスタンスを決定し、その Connection Server インスタンスの FQDN を確認する。一度に、Horizon Cloud Connector 仮想アプライアンスを1つのみポッドのインストール済みの Connection Server インスタンスとペアリングできます。
- Connection Server と Horizon Cloud Connector をペアリングするときに指定するポッドの管理者アカウントを決定し、その管理者アカウントがペアリングに必要な要件を満たしていること。この Active Directory ユーザーには、ポッドの Web ベースのコンソール ([グローバル管理者ビュー] - [ロールの権限] - [管理者]) に示すように、root アクセス グループに Horizon で事前定義された 管理者 ロールが必要です。つまり、Horizon ドキュメントの『[Horizon Console 管理ガイド](#)』で説明されているように、ポッドのオンボーディング プロセスに指定された Active Directory ユーザーはそのポッドのスーパー ユーザーです。
- <https://my.vmware.com> に有効な My VMware アカウントがあり、そのアカウントに Horizon サブスクリプション ライセンスが関連付けられていること。このアカウントは、Horizon Cloud Connector オンボーディング ワークフローを実行してポッドを特定のサービス テナントとペアリングし、クラウドベースの管理コンソールにログインして、テナントへの管理者の追加を含む管理タスクを実行するために必要です。
- その My VMware アカウントに、サービス テナントにログインする権限があること。ユーザーがサービスの最初のサブスクリイバである、または最初のサブスクリイバがユーザーの My VMware E メールを管理者としてテナントに追加した、あるいは組織の既存の管理者がユーザーの My VMware E メールを管理者としてテナントに追加している可能性があります。これらのケースはすべて、権限のあるアカウントを作成します。My VMware アカウントにサービス テナントにログインする権限があるかどうかを確認するには、<https://cloud.horizon.vmware.com> に移動し、My VMware アカウントの認証情報を入力します。システムにログインできた場合、アカウントに権限があるということです。ログインできない場合、組織のテナント管理者の1人にサービス テナントにログインしてユーザーを追加するよう依頼するか、[ナレッジベース記事 KB2006985](#) の手順を使用して Customer Connect で技術以外のサポート リクエストを提出し、ユーザーを組織の既存のテナント レコードに追加するよう要求する必要があります。
- Horizon Cloud Connector バイナリ コンポーネントは、customerconnect.vmware.com のページ URL https://customerconnect.vmware.com/downloads/info/slug/desktop_end_user_computing/vmware_horizon_service/1_x 内にある [Horizon Cloud Connector] という行からダウンロードする必要があります。

- Microsoft Internet Explorer Web ブラウザを使用している場合は、互換モードが無効であることを確認します。この設定により、その Web ブラウザで Horizon Cloud Connector アプライアンスのオンボーディング ユーザー インターフェイスが表示されます。
- **第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件を満たしていることを確認する。**
- Horizon Cloud Connector 仮想アプライアンスに使用する固定 IP アドレスを決定する。この IP アドレスは、Horizon Cloud Connector 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： Horizon Cloud Connector 仮想アプライアンスで IPv6 を使用しないでください。IPv6 はサポートされていません。

- DNS 検索ドメイン、DNS サーバの IP アドレス、デフォルトのゲートウェイ アドレス、サブネット マスクなど、ポッドの環境に Horizon Cloud Connector アプライアンスをデプロイするときに使用する、環境に適した一般的なネットワーク情報があることを確認する。

注： Horizon Cloud Connector 仮想アプライアンスの自己署名証明書では、プロキシの SSL 設定を使用できません。

- 仮想アプライアンスの強力な root パスワードを決定すること。オールイン SDDC デプロイの場合、OVF デプロイ ウィザードで大文字、数字、特殊文字をそれぞれ 1 個以上含む 8 文字以上のパスワードを求められます。フェデレーション デプロイの場合、パスワードはネイティブ クラウド プラットフォームの要件に従っている必要があります。

重要： オールイン SDDC デプロイでは、OVF デプロイ ウィザードを使用してアプライアンスを VMware SDDC にデプロイします。OVF テンプレートをデプロイするときは、強力なパスワードのセキュリティ基準を満たす root パスワードを指定する必要があります。ただし、既知の制限により、特殊文字を含まない root パスワードを指定した場合でも、OVF デプロイ ウィザードは仮想アプライアンスのデプロイを続行します。この場合、デプロイは成功しますが、デプロイ後は仮想アプライアンスのオペレーティング システムへのログインがブロックされます。

仮想アプライアンスのデプロイ後も仮想アプライアンスへのアクセスを確保するには、OVF デプロイ ウィザードのプロンプトに従って、必ず少なくとも 1 つの特殊文字を含む強力な root パスワードを指定します。

- Horizon ポッドで Horizon サブスクリプション ライセンスを使用する最小のユースケースについて、上記の記載に加えて、以下の前提条件を満たしていることを確認する。
 - Horizon Cloud Connector とペアリングする Connection Server インスタンスは、バージョン 7.10 以降を実行している必要がある。バージョン 7.10 は、クラウド サービスとペアリングできる最小バージョンです。

ヒント： 技術的には、最新のバージョンよりも古いバージョンを実行している Horizon ポッドをペアリングすることもできますが、クラウドでホストされる最新の機能をそのポッドで取得するためには、ポッドの Connection Server に最新バージョンのソフトウェアを使用することを推奨します。Connection Server と Horizon Cloud Connector の最新バージョンの組み合わせを使用することによってのみ、そのポッドでサブスクリプション ライセンスを使用するだけでなく、クラウドでホストされる最新の機能にもアクセスできます。

Horizon Cloud Connector の既知の考慮事項

Horizon Cloud Connector を使用している場合は、これらの考慮事項に留意してください。

- Horizon Cloud Connector アプライアンスを VMware SDDC 環境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。
- Horizon Cloud Connector 仮想アプライアンスでの IPv6 の使用はサポートされていません。
- Horizon Cloud Connector 仮想アプライアンスのデプロイ中は、プロキシの SSL 設定を使用できません。
- デプロイされた Horizon Cloud Connector 仮想アプライアンスの固定 IP アドレスとプロキシの設定に関する情報は、特定のコンテナ ファイルに保存されます。仮想アプライアンスでこれらの設定を変更する場合は、仮想アプライアンスに接続し、それらのコンテナ ファイルを編集する必要があります。デプロイされた仮想アプライアンスの固定 IP アドレスを変更する場合、仮想アプライアンスのオペレーティング システムで適切なコンテナ ファイルを編集し、コマンドを実行して、仮想アプライアンスに依存するポッドのすべてのコンポーネントで新しい IP アドレスが共有されるようにする必要があります。[Horizon Cloud Connector 仮想アプライアンスの固定 IP アドレスの更新](#)を参照してください。
- Horizon Cloud Connector 仮想アプライアンスをデプロイ先の環境から削除する前に、Horizon Cloud Connector アプライアンスの IP アドレスにブラウザをポイントし、[接続解除] アクションを使用して、ポッドと Horizon Cloud 間の接続を削除します。
- Horizon ポッドとペアリングされた Horizon Cloud Connector の個別の vdmadmin アカウントを使用するのがベスト プラクティスです。個別の vdmadmin アカウントを使用すると、クラウド管理とオンプレミス管理の間で構成が書き換えられるのを回避できます。個別のアカウントを使用することで、クラウドベースの操作の監査も容易になります。
- Horizon Cloud Connector と Horizon Cloud 間の接続には、インターネットの送信ポート 443 を使用します。コネクタに必要なすべての DNS、ポート、およびプロトコルについては、[第 1 世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件](#)を参照してください。
- デプロイの際に、Horizon Cloud Connector 仮想アプライアンスの root ユーザーのパスワードを設定します。デフォルトでは、このパスワードに有効期限はありません。ただし、組織のセキュリティ ポリシーによっては、root ユーザーに有効期限ポリシーを設定して root パスワードを定期的に更新することをお勧めします。手順については、[Horizon Cloud Connector の root ユーザーのパスワード有効期限ポリシーの設定](#)を参照してください。
- Connection Server が自己署名証明書を使用していて、ポッドを Horizon Cloud にペアリングした後に自己署名証明書を置き換える場合は、Horizon Cloud Connector 構成ポータルにログインし、[再構成] ワークフローを使用して新しい自己署名証明書で証明書の検証手順を再度実行する必要があります。Horizon Cloud Connector 構成ポータルにログインしたら、[再構成] をクリックしてウィザードの手順を完了し、Connection Server からの新しい自己署名証明書を使用して通信を確認することができます。

同様に、Connection Server をアップグレードすると、自己署名証明書が変更される場合があります。新しい証明書を実際に検証するには、Connection Server をアップグレードした後に、Horizon Cloud Connector の [再構成] ワークフローを実行します。

- Connection Server の IP アドレスを解決するために、`/etc/hosts` ファイルにエントリを追加した場合は、`hze-core` および `csms` サービスを再起動する必要があります。次のコマンドを使用します。

```
systemctl restart hze-core
systemctl restart csms
```

- Horizon Cloud および必要な Connection Server インスタンスで Horizon Cloud Connector 仮想アプライアンスが確実に正しく認証されるようにするには、仮想アプライアンスの時刻を NTP サーバと同期する必要があります。詳細については、[Horizon Cloud Connector 仮想アプライアンスと NTP サーバの同期](#) を参照してください。
- Horizon Cloud Connector 構成ポータルで接続の問題が発生した場合は、[VMware ナレッジベース \(KB\) の記事 79859](#) のトラブルシューティング情報を参照してください。
- Horizon Cloud Connector バージョン 2.3.x 以前 - Horizon Cloud Connector がポッドとペアリングされたときに構成ポータルで使用された Active Directory ドメイン アカウント ([Horizon 認証情報]) の認証情報が変更された場合は、[再構成] アクションを使用して、保存されている Active Directory ドメイン アカウントの詳細を新しいパスワードに変更し、ライセンス プッシュ エラーを回避する必要があります。構成ポータルで [再構成] をクリックし、手順に従ってウィザードを完了します。
- Horizon Cloud Connector 2.4.x 以降 - [Horizon 認証情報] アカウントのパスワードが変更された場合は、[Horizon Cloud Connector 2.4 以降 - Horizon Cloud Connector が Horizon Connection Server で使用する登録済みの Active Directory 認証情報を更新する](#)に記載されている手順に従って、Horizon Cloud Connector を更新し、更新された認証情報を使用できます。

廃止された旧バージョン

Horizon Cloud Connector の新しいデプロイは、バージョン N、N-1、N-2 を使用してサポートされます。N は、Horizon Cloud Connector の最新バージョンです。以前のバージョンは廃止され、使用できません。既存のデプロイは、同じバージョンにアップデートすることが期待されます。最新バージョンの数字については、[リリース ノート](#)を参照してください。

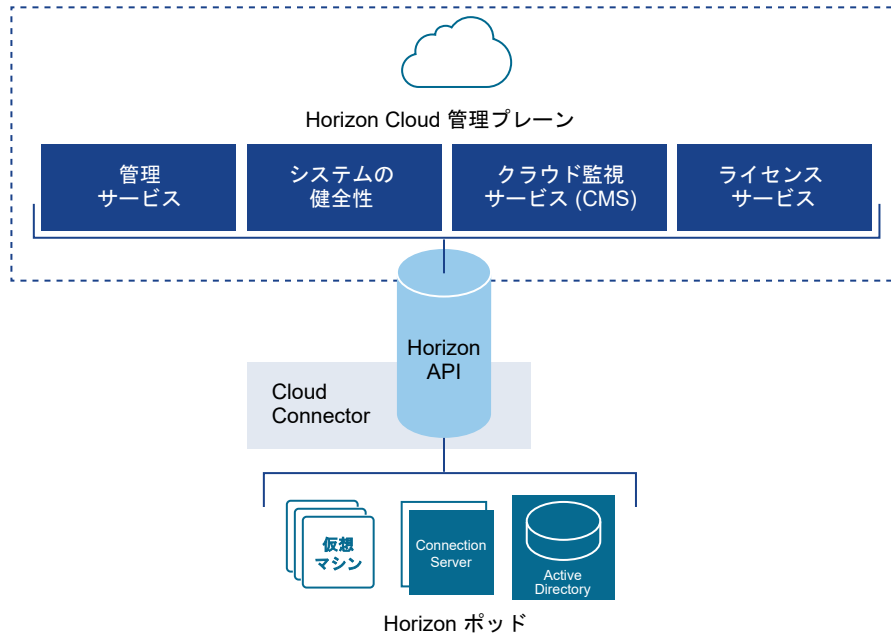
第1世代テナント - 第1世代 Horizon Cloud Service を既存の Horizon ポッドに接続してクラウド ホスト型サービスを使用する

このページは、第1世代のテナント環境にアクセスできる場合にのみ使用します。VMware ナレッジベースの記事 KB92424 で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。

重要: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、[該当記事を参照してください](#)。

既存の Horizon ポッドを第1世代 Horizon Cloud Service に接続する場合は、複数の手順を実行します。VMware Customer Connect から Horizon Cloud Connector 仮想アプライアンスをダウンロードします。次に、仮想アプライアンスをインストールしてパワーオンします。仮想アプライアンスがパワーオンされ、必要なポッド コンポーネントとサービスの健全性を確認した後、コネクタのオンボーディング ワークフローを使用して、そ

のサブスクリプション ライセンスを使用するポッド内の Connection Server とペアリングします。成功したペアリング プロセスの一部として、Horizon Cloud Connector 仮想アプライアンスは Connection Server を第1世代 Horizon Cloud Service にブリッジし、クラウド管理プレーンが Horizon サブスクリプション ライセンス、および現在クラウド接続されているポッドの他のクラウド ホスト型サービスを管理できるようにします。



ヒント: Horizon Cloud のオンボーディング プロセス全体の概要については、「第1世代テナント - Horizon Cloud のポッドのデプロイとオンボーディング」を参照してください。

この手順を使用して、既存の Horizon ポッドをクラウド管理プレーンに接続します。ポッドを Horizon Cloud Service に接続すると、そのポッドでクラウド ホスト型サービスを利用していない場合でも、そのポッドで Horizon サブスクリプション ライセンスを使用できます。Horizon サブスクリプション ライセンスでは、ポッドのライセンスをアクティブ化するために手動でライセンス キーを入力する必要はありません。ペアリングが完了すると、通常ポッドをクラウド制御プレーンとペアリングしてから 4 時間以内に、VMware はサブスクリプション ライセンスをアクティブ化します。VMware がサブスクリプション ライセンスをアクティブ化すると、ポッドの Web ベースの管理コンソールに Horizon 環境がサブスクリプション ライセンスを使用しているというメッセージが表示されます。

ライセンスと使用状況

ライセンス 使用量 カスタマー エクスペリエンス プログラム

ライセンスを編集 ⓘ 無期限ライセンスを使用する ⓘ

ライセンスキー

✔ Horizon サブスクリプション ライセンス
License Service に接続されています。
Horizon は、License Service に接続され、サブスクリプション ライセンスを使用しています。

ライセンスの有効期限 Mon Mar 01 2027 08:00:00 GMT+0800 (中国標準時)

第1世代テナント - Horizon Cloud のポッドのデプロイとオンボーディングで説明するように、Horizon ポッドを Horizon Cloud にオンボーディングするプロセスには、次の基本概念が含まれます。

- Horizon サブスクリプション ライセンスは、クラウド管理プレーン、すなわち Horizon Cloud から管理されます。
- そのため、Horizon ポッドでサブスクリプション ライセンスを使用する場合は、ポッドをそのクラウド管理プレーンに接続する必要があります。ポッドをクラウド管理プレーンに接続しないようにする場合、そのポッドでサブスクリプション ライセンスを使用することはできません。
- 既存の Horizon ポッドをクラウド管理プレーンに接続するには、Horizon Cloud Connector という名前のコネクタが必要です。クラウド管理プレーンはコネクタと通信し、コネクタはポッドの Connection Server インスタンスの1つと通信します。コネクタは、一度にポッドのインストール済みの Connection Server インスタンスの1つのみとペアリングできます。
- Horizon Cloud Connector は、クラウド管理プレーンと、それをペアリングするポッドの接続サーバ インスタンスの両方に到達する必要があるため、Horizon Cloud Connector とポッドのペアリング、および継続的な操作を成功させるために特定の [第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件](#)を満たす必要があります。ポッドでサブスクリプション ライセンスを使用する最小の使用事例でも、それらの DNS、ポート、およびプロトコルの要件を満たす必要があります。
- Horizon サブスクリプション ライセンスを取得し、クラウド管理プレーンで認証してコネクタをセットアップし、ポッドでそのサブスクリプション ライセンスを使用するための接続を確立するには、VMware Customer Connect アカウントが必要です。
- Horizon ポッドでサブスクリプション ライセンスのみを使用することも、そのポッドでクラウド ホスト型サービスを追加で使用することもできます。どのユースケースでも、サブスクリプション ライセンスが必要です。
- 最新の機能とセキュリティおよびバグ修正を取得するには、VMware Customer Connect で入手可能で、ポッドの Horizon Connection Server ソフトウェア バージョンと互換性のある最新バージョンの Horizon Cloud Connector を使用する必要があります。Horizon Cloud Connector と Horizon Connection Server の互換性マトリックスについては、[VMware 製品の相互運用性マトリックス](#)にアクセスし、[VMware Horizon Cloud Connector] と [VMware Horizon] としてリストされている2つのソリューション名の相互運用性を確認してください。

このプロセスの手順の概要は次のとおりです。

- 1 VMware Customer Connect アカウントを取得します。
- 2 そのアカウントを使用して、Horizon サブスクリプション ライセンスにサインアップします。
- 3 ライセンスにサインアップすると、その VMware Customer Connect アカウントに関連付けられているメールアドレスによる E メールが送信されます。このようこそ E メールには、[VMware Customer Connect サイト](#)内の Horizon Cloud Connector ダウンロード ページから Horizon Cloud Connector イメージをダウンロードするためのリンクが含まれます。
- 4 ようこそ Eメールのリンクを使用して、Horizon Cloud Connector イメージをダウンロードします。
- 5 固定 IP アドレスを使用して、そのアプライアンスをポッドの環境にデプロイします。仮想アプライアンスのデプロイ プロセスが完了したら、仮想アプライアンスをパワーオンします。

- 6 Horizon Cloud Connector とポッド内の Connection Server インスタンスをペアリングし、Connection Server インスタンス、Horizon Cloud Connector、およびクラウド管理プレーン間の接続を完了するためのペアリング ワークフローを開始するために使用する URL アドレスを取得します。
- 7 ペアリング ワークフローを開始する前に、`precheck.sh` スクリプトを実行してポッドのシステム コンポーネントとサービスの健全性を確認します。
- 8 以前に取得した URL アドレスを使用して、ペアリング ワークフローを開始します。Horizon Cloud からログイン画面が表示されるので、VMware Customer Connect アカウントの認証情報を使用してログインします。その時点でワークフローのユーザー インターフェイスがブラウザに表示されるので、このトピックで説明する以下の手順を完了します。

重要： このポッドを接続している Horizon Cloud 環境にすでにクラウド接続ポッドがある場合は、それらのクラウド接続ポッドすべてが同じ Active Directory ドメインのセットを認識できる必要があります。未接続のポッドを接続する手順を実行するときは、ポッドが、すでに Horizon Cloud 環境に登録されている Active Directory ドメインを認識できるようにする必要があります。

たとえば、ご使用の環境内にすでに Microsoft Azure のポッドがあり、Horizon ポッドを接続している場合は、次のことを確認する必要があります。

- 以降の手順を使用して接続している Horizon ポッドが、Microsoft Azure の既存のポッドで使用される Active Directory ドメインを認識できること（これらのドメインはすでに環境のクラウド プレーンに登録されているため）。
- Microsoft Azure の既存のクラウド接続ポッドが、Horizon ポッドの Active Directory ドメイン（以降の手順で Horizon Cloud Connector 仮想アプライアンスと Horizon ポッドの Connection Server をペアリングするために使用するドメイン）を認識できること。

前提条件

「[第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備](#)」に記載されているすべての項目を満たしていることを確認します。

Horizon ポッドと Horizon Cloud をペアリングするために Horizon Cloud Connector を使用する場合、[第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件](#)を満たしていることを確認します。

デプロイされた Horizon Cloud Connector がポッドの Connection Server の FQDN を解決するために、ネットワーク トポロジ内の DNS 構成が提供されることを確認します。デプロイされた Horizon Cloud Connector が DNS を使用して Connection Server を解決できない場合、ポッドのドメイン認証情報を入力するステップでオンボーディング ウィザードに予期しないエラーが発生します。

[Horizon Cloud Connector の既知の考慮事項](#)を確認して、これらのアイテムを認識していることを確認します。

Horizon Cloud Connector 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、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 Cloud Connector 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。第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備、Horizon Cloud Connector の既知の考慮事項、および Horizon Cloud Connector 1.6 以降のプロキシ設定の変更のプロキシ関連情報を参照してください。

手順

1 第1世代テナント - Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイする

Horizon Cloud Connector をダウンロードしてデプロイするには、ご利用の Horizon ポッドのデプロイアーキテクチャに適用されるサブトピックの手順に従ってください。

2 第1世代テナント - Horizon ポッドと仮想アプライアンスの第1世代 Horizon 制御プレーンとのペアリングの準備ができていることを確認する

Horizon ポッドを第1世代 Horizon 制御プレーン サービスにオンボーディングするこのワークフローのステップでは、`precheck.sh` 診断ツールを実行して、ポッドと Horizon Cloud Connector の両方ともペアリングプロセスの準備ができていることを確認します。最初に診断を実行し、システムコンポーネントおよび構成で見つかった障害となっている問題を修正することにより、ペアリングプロセスが成功する可能性を最大限に高めることができます。

3 第1世代テナント - Horizon Cloud Connector 構成ポータルを使用して Horizon ポッドと第1世代 Horizon Cloud のペアリングを完了する

Horizon ポッドを第1世代 Horizon Cloud にオンボーディングするワークフローのこの手順では、Horizon Cloud Connector 構成ポータルを使用して、Horizon Cloud Connector が Horizon ポッドの Connection Server とのペアリングに使用する詳細を指定します。これらの手順を正常に完了すると、ポッドが第1世代 Horizon Cloud テナント環境に接続されます。

4 Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector クラスタへのワーカー ノードの追加

Horizon Cloud Connector のサービス レベルのフォルト トレランスをサポートするには、プライマリ ノードを含んでいるクラスタにワーカー ノードを追加して、デュアル ノード クラスタを作成します。ワーカー ノードは、Horizon Cloud Connector アプリケーション サービスのレプリカを含んでいます。

結果

Horizon ポッドが Horizon Cloud に正常に接続された場合、Horizon Cloud Connector 構成ポータルに「セットアップが完了しました」というメッセージが表示されます。この時点から、この同じ構成ポータルを使用して、Horizon Cloud Connector コンポーネントの健全性ステータスの確認、Horizon Cloud Connector 仮想アプライアンスへの SSH アクセスの有効化または無効化などの管理タスク、およびその他の同様のタスクを実行します。詳細については、[Horizon ポッドと Horizon Cloud のペアリング後に Horizon Cloud Connector で実行する一般的な管理およびメンテナンス タスクのトピック](#)を参照してください。

次のステップ

現在のクラウド接続ポッドでサブスクリプション ライセンスを使用することが唯一の目標である場合、追加の手順はありません。ただし、Horizon Cloud Connector とクラウド制御プレーン間の接続を維持するために、DNS、ポート、およびプロトコルの要件が引き続き満たされていることを確認する必要があります。サブスクリプション ライセンスは Cloud 制御プレーンによって管理されるため、Horizon Cloud Connector はサブスクリプション ライセンス情報を受け取るためにポッドの Cloud 制御プレーンに引き続き到達できる必要があります。

重要： Horizon Cloud Connector をインストールすると、インターネットの送信ポート 443 でクラウド制御プレーンへの接続が確立されます。最新のサブスクリプション ライセンス情報をポッドに同期するなど、さまざまな目的でクラウド制御プレーンと通信するために、この接続は常に開いたままにする必要があります。Horizon サブスクリプション ライセンスの使用は、クラウド制御プレーン、Horizon Cloud Connector インスタンス、およびその Horizon Cloud Connector インスタンスとペアリングされたポッドの間の正常に動作する通信チェーンに依存します。通信チェーン内のリンクが動作していない場合（Horizon Cloud Connector の電源がオフになっている場合やネットワークの中断が発生した場合など）、クラウド プレーンは、このポッドとその Horizon Cloud Connector とのペアリングを期限切れとしてマークする前に、サービス定義の時間間隔に従って通信チェーンに沿って、サブスクリプション ライセンス情報の同期を試みます。このサービスで定義された期間中、クラウド プレーンと Horizon Cloud Connector およびポッドの間の通信チェーンが動作していない場合でも、ポッドのライセンスは有効なままで、エンドユーザー接続は機能します。サービスは、このサービス定義の同期の有効期限を提供して、通信チェーンを再度動作可能にするときに、ポッドのライセンス機能が引き続き適切に動作できるようにします。通信チェーンの非動作状態がシステム定義の期間全体にわたって維持され、定義された期間の終了までに正常な同期が行われない場合、クラウド プレーンはこの Horizon Cloud Connector とポッドとのペアリングを期限切れとしてマークします。その場合は、VMware のサポートに問い合わせる必要があります。詳細については、[Horizon ユニバーサル ライセンスの監視](#)を参照してください。期間全体を通じて、システム定義の期間が終了するまでの残り時間については、Horizon Universal Console のアラートと通知で通知されます。また、コンソールの監査ログには、通信チェーンの問題が示されて、修正方法を特定するのに役立ちます。

クラウドに接続されたポッドでクラウド ホスト型サービスを利用するには、管理コンソールにログインし、ポッドの Active Directory ドメインを Horizon Cloud に登録する Active Directory 登録ワークフローを完了する必要があります。このワークフローの詳細については、『Horizon Cloud 管理ガイド』の「[Horizon Cloud 環境での最初の Active Directory ドメイン登録の実行](#)」を参照してください。

第1世代テナント - Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイする

Horizon Cloud Connector をダウンロードしてデプロイするには、ご利用の Horizon ポッドのデプロイ アーキテクチャに適用されるサブトピックの手順に従ってください。

注目: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

2022年8月の時点で、Horizon Cloud Service - next-gen は一般公開され、独自の『Horizon 制御プレーン next-gen の使用』ガイドを入手できます。

次世代と第1世代のどちらの環境を使用しているかは、環境にログインし、Horizon Universal Console ラベルに表示されるブラウザの URL フィールドのパターンで確認することができます。次世代環境の場合、コンソールの URL アドレスには /hcsadmin/ のような部分が含まれます。第1世代コンソールの URL の場合は、異なるセクション (/horizonadmin/) があります。

Horizon ポッドのデプロイ アーキテクチャの背景情報については、[第1世代テナント - 第1世代 Horizon Cloud を使用した Horizon ポッドのデプロイ アーキテクチャ](#)を参照してください。

Horizon ポッドのデプロイ アーキテクチャ:	参照する Horizon Cloud Connector デプロイ手順:
<ul style="list-style-type: none"> ■ オンプレミス ポッド ■ オールイン SDDC ポッド 	第1世代テナント - オンプレミスおよびオールイン SDDC Horizon ポッド: Horizon Cloud Connector をダウンロードして、ポッドの vSphere 環境にデプロイする
連携したポッド - Microsoft Azure クラウドおよび Azure VMware Solution (AVS)	第1世代テナント - Horizon ポッド - Azure VMware Solution を使用したフェレデーション アーキテクチャ: Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイする
連携したポッド - Google Cloud Platform および Google Cloud VMware Engine (GCVE)	第1世代テナント - Horizon ポッド - Google Cloud VMware Engine を使用したフェレデーション アーキテクチャ: Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイする
連携したポッド - Amazon Web Services EC2 および VMware Cloud on AWS	第1世代テナント - Horizon ポッド - VMware Cloud on AWS を使用したフェレデーション アーキテクチャ: Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイする

第1世代テナント - オンプレミスおよびオールイン SDDC Horizon ポッド: Horizon Cloud Connector をダウンロードして、ポッドの vSphere 環境にデプロイする

次の手順に従って、Horizon Cloud Connector をダウンロードし、オンプレミスまたはオールイン SDDC アーキテクチャのクラウド環境にデプロイされた Horizon ポッドの vSphere インフラストラクチャにデプロイします。これらの手順の結果、Horizon Cloud Connector 仮想アプライアンスがデプロイされ、vSphere 環境で実行されます。

重要: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

この手順では、Horizon ポッドをオンプレミスまたはオールイン SDDC アーキテクチャのクラウド環境にデプロイした場合に、ポッドの vSphere 環境に Horizon Cloud Connector をデプロイする必要がある場合の対処方法について説明します。

注： Horizon ポッドのデプロイ アーキテクチャの背景情報については、[第1世代テナント - 第1世代 Horizon Cloud を使用した Horizon ポッドのデプロイ アーキテクチャ](#)を参照してください。

Horizon Cloud Connector 2.0 以降をダウンロードする場合、以下の手順の説明は、仮想アプライアンスのプライマリ ノードをポッドの vSphere 環境にデプロイする方法になります。

Horizon Cloud Connector 1.10 をダウンロードする場合、以下の手順の説明は、仮想アプライアンスをポッドの vSphere 環境にデプロイする方法になります。

注： 特に指定がない限り、この手順の内容は Horizon Cloud Connector のすべてのバージョンに適用されます。これらの手順では、「仮想アプライアンス」という用語を使用して、アプライアンスのプライマリ ノード (Horizon Cloud Connector 2.0 以降) または仮想アプライアンス (Horizon Cloud Connector 1.10) を指します。

重要： vSphere Client を使用して、ポッドの vSphere 環境に Horizon Cloud Connector をデプロイする必要があります。Horizon Cloud Connector を ESXi ホストに直接デプロイしないでください。

前提条件

- [第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備](#)に記載されているコネクタ関連の前提条件を満たしていることを確認します。
- Horizon ポッドと Horizon Cloud をペアリングするために Horizon Cloud Connector を使用するための [第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件](#)を満たしていることを確認します。
- Horizon Cloud 制御プレーンと通信するには、Horizon Cloud Connector 仮想アプライアンスがインターネットにアクセスできる必要があります。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 Cloud Connector アプライアンスで使用する時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。[第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備](#)、Horizon Cloud Connector の既知の考慮事項、および [Horizon Cloud Connector 1.6 以降のプロキシ設定の変更のプロキシ関連情報を参照](#)してください。
- アプライアンスをポッドにペアリングする前に、推奨されるレベルのセキュリティでアプライアンスへの SSH アクセスを有効にする場合は、SSH パブリック キーを生成します。アプライアンスのデプロイ時に SSH パブリック キーを登録する必要があります。

手順

- 1 前提条件リストに記載されているように、サブスクリプション E メールに記載されているリンクを使用して Horizon Cloud Connector アプライアンスをダウンロードします。

Horizon Cloud Connector アプライアンスは、OVA ファイルとして使用できます。このファイルには、VMware Customer Connect のメインの「[VMware Horizon Service のダウンロード](#)」にある「VMware Horizon Cloud Connector」行から移動できます。その「[VMware Horizon Service のダウンロード](#)」ページで、「VMware Horizon Cloud Connector」行の「[ダウンロードに移動](#)」というラベルのリンクをクリックして、OVA ファイルを含む Horizon Cloud Connector ページを開きます。

重要： 最新の製品修正、セキュリティ修正、および最新機能を使用するには、ダウンロードしたバージョンが一般公開された最新バージョン以降であることを確認してください。現在、バージョン 2.4.x が最新の一般公開されたバージョンです。以前に 2.4.x より前のバージョンの Horizon Cloud Connector OVA をダウンロードした場合は、customerconnect.vmware.com にログインし、ポッドのペアリングに使用する最新バージョンを取得します。

- 2 vSphere Client を使用して、Horizon Cloud Connector アプライアンスを OVF テンプレートとして Horizon ポッドにデプロイします。

OVF テンプレートのデプロイに関する一般的な情報については、[VMware vSphere のドキュメントページ](#)にある『vSphere 仮想マシン管理』ガイドを参照してください。

OVF デプロイ ウィザードには、OVF デプロイのためにホスト、データストア、ネットワークなどの一般的な選択を行うためのいくつかのステップがあります。[テンプレートのカスタマイズ] 手順では、Horizon Cloud Connector アプライアンスに固有の詳細を指定します。

- 3 ウィザードの [テンプレートのカスタマイズ] 手順で、必要な項目を完了し、お使いの環境に適した項目を指定します。

この手順での入力は、仮想アプライアンスの構成に使用されます。

- a 仮想アプライアンスの root パスワードを指定します。

注： 新しいパスワードが強力なパスワードのセキュリティ基準を満たしていることを確認します。パスワードは 8 文字以上で、少なくとも 1 つの大文字、1 つの数字、および 1 つの特殊文字を含んでいることを確認します。

重要： 既知の制限により、特殊文字を含まない root パスワードを指定しても、OVF デプロイ ウィザードは引き続き仮想アプライアンスをデプロイします。この場合、デプロイは成功しますが、デプロイ後は仮想アプライアンスのオペレーティング システムへのログインがブロックされます。仮想アプライアンスがデプロイされた後、その仮想アプライアンスに確実にアクセスできるようにするには、パスワードに少なくとも 1 つの特殊文字が含まれていることを確認します。

- b (Horizon Cloud Connector 2.0 以降) アプライアンスのプライマリ ノードをデプロイするには、[ワーカー ノード] オプションが無効になっていることを確認します。デフォルトでは、このオプションは無効になっています。

- c ccadmin アカウントで SSH パブリック キー認証を使用するには、先ほど生成した SSH パブリック キーを入力します。

詳細については、[コマンドラインインターフェイスの使用による Horizon Cloud Connector への SSH アクセスの有効化](#)を参照してください。

アプライアンスとポッドをペアリングする前に、アプライアンスへの SSH アクセスを必要としない場合は、この手順をスキップできます。アプライアンスとポッドのペアリングが完了するまで、パブリック キーの登録と SSH アクセスの有効化を遅らせることができます。

- d 仮想アプライアンスに固定 IP アドレスを指定します。

Horizon Cloud Connector 仮想アプライアンスで IPv6 を使用しないでください。IPv6 はサポートされていません。

- e [ネットワーク] セクションで [ポッド ネットワーク] および [サービス ネットワーク] フィールドはオプションです。これらのネットワークは、仮想マシン内の Kubernetes によって使用され、仮想マシンの外部からアクセスすることはできません。顧客の社内ネットワークと重複しない限り、デフォルト値にする必要があります。Kubernetes CNI のデフォルトでは、サブネット 192.168.240.0/21 は [ポッド ネットワーク] の構成に使用され、192.168.236.0/23 は [サービス ネットワーク] に使用されます。[ワーカー ノード] を構成している場合、これらの設定は適用されません。

- f 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環境では、プロキシ関連の設定を行います。

重要： 次の考慮事項を念頭に置いてください。

- Horizon Cloud Connector 仮想アプライアンスの自己署名証明書では、プロキシの SSL 設定を使用できません。
- HTTP プロキシ経由でインターネット ルートへの送信要求のみを行うには、アプライアンスからの内部要求を受信するときに、プロキシ サーバをバイパスするプロキシなしのホストを構成します。このユースケースでは、[プロキシなし] には少なくとも Horizon Cloud Connector とペアリングされるポッドに関連付けられた Connection Server と vCenter Server インスタンスの DNS サブドメインを入力します。

[プロキシなし] では、次の例のように複数の値を区切るためにカンマを使用し、空白スペースをゼロにします。この例に示すように、フィールドは IP アドレス範囲も受け入れます。

.ad-domain.example.com,10.109.*

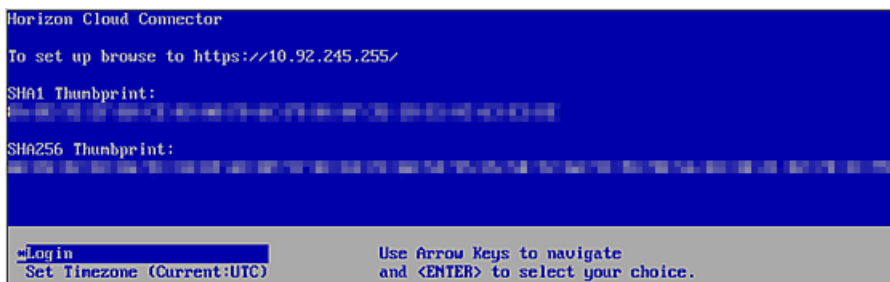
[プロキシなし] 設定を空白のままにすると、仮想アプライアンスは管理者によって提供された、または検出された Connection Server ホスト名を取得します。アプライアンスは、ポッドをクエリして Connection Server のホスト名を検出します。検出されたホストは、暗黙的なプロキシなしのホストとして構成されます。

-
- 4 vSphere Client を使用して、Horizon Cloud Connector アプライアンスをパワーオンします。

- 5 アプライアンスが完全にパワーオンされたら、vSphere Client のオプションを使用して Horizon Cloud Connector アプライアンスのコンソールを起動します。

- (Horizon Cloud Connector 2.0 以降) Kubernetes が初期化プロセスを完了するまでに最大 10 分かかります。この間、システムは青色の起動画面に「Horizon Cloud Connector (プライマリ) を構成しています...」というメッセージが表示されます。初期化が完了すると、プライマリ ノードの URL アドレスを含む青いコンソール画面が表示されます。この URL は、オンボーディング ワークフロー用としてブラウザにロードします。
- (Horizon Cloud Connector 1.10) アプライアンスの青いコンソール画面が仮想アプライアンスの URL アドレスと共に表示されるまで待機します。この URL は、オンボーディング ワークフロー用としてブラウザにロードします。

次のスクリーンショットは、アドレス `https://10.92.245.255/` を持つデプロイ済みアプライアンスの例です。



```

Horizon Cloud Connector
To set up browse to https://10.92.245.255/
SHA1 Thumbprint:
SHA256 Thumbprint:
*Login
Set Timezone (Current:UTC)
Use Arrow Keys to navigate
and <ENTER> to select your choice.
  
```

- 6 コマンド ライン インターフェイスの使用による Horizon Cloud Connector への SSH アクセスの有効化の手順を完了させます。
- 7 Horizon Cloud Connector 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 Cloud Connector 仮想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。
- 8 第1世代テナント - Horizon ポッドと仮想アプライアンスの第1世代 Horizon 制御プレーンとのペアリングの準備ができていることを確認するに進み、ポッドのオンボーディング ワークフローを続行します。

第1世代テナント - Horizon ポッド - VMware Cloud on AWS を使用したフェレデーション アーキテクチャ: Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイする

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 Cloud Connector 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、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 Cloud Connector をデプロイする必要があります。

重要: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

Horizon ポッドのデプロイ アーキテクチャの背景情報については、[第1世代テナント - 第1世代 Horizon Cloud を使用した Horizon ポッドのデプロイ アーキテクチャ](#)を参照してください。

以下は、ポッドの環境内のネイティブの Amazon EC2 インフラストラクチャに Horizon Cloud Connector をデプロイするために必要な手順の概要です。

- VMDK 形式の Horizon Cloud Connector ファイルをダウンロードします。
- Amazon EC2 に Amazon Simple Storage Service (S3) バケットを作成し、アプライアンスの VMDK ファイル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 VMDK 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 Cloud Connector 仮想マシン (VM) インスタンスを作成します。

重要： Horizon Cloud Connector をネイティブの Amazon EC2 インフラストラクチャにデプロイすると、次の Horizon Cloud サービスがデフォルトで無効になります。アプライアンスをデプロイした後、オプションで第1世代テナント - ネイティブの Amazon EC2 の Horizon Cloud Connector に対し第1世代の Horizon Cloud 制御プレーン サービスを手動で有効にすることができます。

- Cloud Monitoring Service
 - クラウド ブローカ クライアント サービス
 - イメージ ローカリティ サービス
-

前提条件

- 第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備に記載されているコネクタ関連の前提条件を満たしていることを確認します。
- Horizon ポッドと Horizon Cloud をペアリングするために Horizon Cloud Connector を使用するための第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件を満たしていることを確認します。
- Horizon Cloud Connector 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 Cloud Connector 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。第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備、Horizon Cloud Connector の既知の考慮事項、および Horizon Cloud Connector 1.6 以降のプロキシ設定の変更のプロキシ関連情報を参照してください。
- 多くの手順では、AWS 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 サブスクリプション メールに記載されているリンクを使用して、Horizon Cloud Connector ディスク イメージをダウンロードします。

注： アプライアンスの Amazon EC2 環境へのデプロイをサポートするには、バージョン 2.0 以降の Horizon Cloud Connector ディスク イメージをダウンロードする必要があります。

Horizon Cloud Connector ディスク イメージは、My VMware アカウントの認証情報を使用して my.vmware.com にログインした後、VMDK ファイルとして利用できます。VMDK ファイルをローカル システムにダウンロードします。

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。

- 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。

次のテキストは、上記のコマンドを実行した後の 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"
        }
      }
    }
  ]
}
```

- 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": "horizon-cloud-connector-2.0.0.0-18191154_OVF10-disk1.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 Cloud Connector 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 Cloud Connector 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。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 Cloud Connector 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 Cloud Connector の AMI インスタンスを起動します。

重要： 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。

重要： 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 Cloud Connector 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。

次のステップ

第 1 世代テナント - Horizon ポッドと仮想アプライアンスの第 1 世代 Horizon 制御プレーンとのペアリングの準備ができていることを確認するの手順に従って、ポッドのオンボーディング ワークフローを続行します。第 1 世代テナント - Horizon Cloud Connector 構成ポータルを使用して Horizon ポッドと第 1 世代 Horizon Cloud のペアリングを完了するに進みます。

注： デフォルトで無効になっている 1 つ以上のクラウドプレーン サービスを有効にする場合は、ポッドとクラウドプレーンのペアリングを完了する前にそれらを有効にする必要があります。第 1 世代テナント - ネイティブの Amazon EC2 の Horizon Cloud Connector に対し第 1 世代の Horizon Cloud 制御プレーン サービスを手動で有効にするを参照してください。

第 1 世代テナント - Horizon ポッド - Azure VMware Solution を使用したフェデレーション アーキテクチャ: Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイする

次の手順に従って、Azure VMware Solution (AVS) を使用したフェデレーション アーキテクチャを使用するポッド環境の Horizon Cloud Connector 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 Cloud Connector をデプロイする必要があります。

重要： この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。KB-92424 で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

Horizon ポッドのデプロイ アーキテクチャの背景情報については、第 1 世代テナント - 第 1 世代 Horizon Cloud を使用した Horizon ポッドのデプロイ アーキテクチャを参照してください。AVS 環境の操作の詳細については、<https://docs.microsoft.com/en-us/azure/azure-vmware/> にある Microsoft Azure のドキュメントを参照してください。

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 Cloud Connector をデプロイするために必要な手順の概要です。

- Horizon Cloud Connector 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 Cloud Connector 仮想マシンを作成します。

前提条件

- [第 1 世代テナント - Horizon ポッドと Horizon Cloud Connector - 第 1 世代の制御プレーン サービスにオンボーディングする準備](#)に記載されているコネクタ関連の前提条件を満たしていることを確認します。
- Horizon ポッドと Horizon Cloud をペアリングするために Horizon Cloud Connector を使用するための [第 1 世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件](#)を満たしていることを確認します。
- Horizon Cloud Connector 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 Cloud Connector 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。[第 1 世代テナント - Horizon ポッドと Horizon Cloud Connector - 第 1 世代の制御プレーン サービスにオンボーディングする準備](#)、Horizon Cloud Connector の既知の考慮事項、および Horizon Cloud Connector 1.6 以降のプロキシ設定の変更のプロキシ関連情報を参照してください。
- 必要な仮想マシンのサイジングについては、[4 章 第 1 世代の Horizon Cloud 制御プレーンを使用する VMware Horizon 8 ポッド - 要件チェックリスト - 2023 年 11 月 2 日のサービス更新に合わせて適切に更新されました](#)を参照してください。

手順

- 1 サブスクリプション E メールに記載されているリンクを使用して、Horizon Cloud Connector ディスク イメージをダウンロードします。

Horizon Cloud Connector ディスク イメージは、My VMware アカウントの認証情報を使用して my.vmware.com にログインした後、ZIP パッケージに圧縮された VHD ファイルとして取得できます。VHD ファイルをダウンロードし、ローカル システムに展開します。

重要： 最新の機能を有効にするには、バージョン 1.10 以降の Horizon Cloud Connector ディスク イメージをダウンロードします。バージョン 1.10 以降では、Horizon Cloud Connector の自動更新を除いた、すべての Horizon Cloud 機能とサービスがサポートされています。

Horizon Cloud Connector 1.9 以前とペアリングされている場合、AVS の Horizon ポッドでは、次の機能とサービスはサポートされません。

- Horizon Cloud Connector の自動更新
- Universal Broker およびマルチクラウド割り当て
- クラウド監視サーバ (CMS)
- Horizon Image Management Service

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>/HorizonCloudConnectorDiskImageName.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/horizon-cloud-connector-1.8.0.0-16488286.vhd?sv=2020-01-01&ss=bfqt&srt=sco&sp=rwldlapx&se=2020-01-01T12:00:00Z&st=2020-01-01T06:00:00Z&spr=https&sig=dUPul7414K0ah%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 Cloud Connector 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:\horizon-cloud-connector-1.9.0.0-16488286.vhd "https://azurestorage1.blob.core.windows.net/vmware/horizon-cloud-connector-1.8.0.0-16488286.vhd?sv=2020-01-01&ss=bfqt&srt=sco&sp=rwldlapx&se=2020-01-01T12:00:00Z&st=2020-01-01T06:00:00Z&spr=https&sig=dUPul7414K0ah%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 Cloud Connector 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 Cloud Connector 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、[4 章 第1世代の Horizon Cloud 制御プレーンを使用する VMware Horizon 8 ポッド - 要件チェックリスト - 2023 年 11 月 2 日のサービス更新に合わせて適切に更新されました](#)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、[第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件](#)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 Cloud Connector 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 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環境では、[Horizon Cloud Connector 1.6 以降のプロキシ設定の変更の説明](#)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 必要な証明書を構成します (Horizon Cloud Connector 仮想アプライアンスの CA 署名付き証明書の構成を参照)。
 - 8 コマンド ライン インターフェイスの使用による Horizon Cloud Connector への SSH アクセスの有効化の手順を完了させます。
 - 9 Horizon Cloud Connector 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 Cloud Connector 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。

次のステップ

第 1 世代テナント - Horizon ポッドと仮想アプライアンスの第 1 世代 Horizon 制御プレーンとのペアリングの準備ができていることを確認する手順に従って、ポッドのオンボーディング ワークフローを続行します。第 1 世代テナント - Horizon Cloud Connector 構成ポータルを使用して Horizon ポッドと第 1 世代 Horizon Cloud のペアリングを完了するに進みます。

第 1 世代テナント - Horizon 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 Connector をダウンロードしてポッドの環境にデプロイする

次の手順に従って、Google Cloud VMware Engine (GCVE) を使用したフェデレーション アーキテクチャを使用するポッド環境の Horizon Cloud Connector 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、ポッドの環境のネイティブ Google Cloud Platform (GCP) インフラストラクチャに Horizon Cloud Connector をデプロイする必要があります。

重要: この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

Horizon ポッドのデプロイ アーキテクチャの背景情報については、[第 1 世代テナント - 第 1 世代 Horizon Cloud を使用した Horizon ポッドのデプロイ アーキテクチャ](#)を参照してください。GCVE 環境の操作の詳細については、<https://cloud.google.com/vmware-engine/docs> にある Google Cloud のドキュメントを参照してください。

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 Cloud Connector をデプロイするために必要な手順の概要です。

- Horizon Cloud Connector 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 Cloud Connector 仮想マシン (VM) インスタンスを作成します。

前提条件

- [第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備](#)に記載されているコネクタ関連の前提条件を満たしていることを確認します。
- Horizon ポッドと Horizon Cloud をペアリングするために Horizon Cloud Connector を使用するための [第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件](#)を満たしていることを確認します。
- Horizon Cloud Connector 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 Cloud Connector 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。[第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備](#)、[Horizon Cloud Connector の既知の考慮事項](#)、および [Horizon Cloud Connector 1.6 以降のプロキシ設定の変更のプロキシ関連情報を参照してください](#)。
- 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 サブスクリプション メールに記載されているリンクを使用して、Horizon Cloud Connector ディスク イメージをダウンロードします。

Horizon Cloud Connector ディスク イメージは、My VMware アカウントの認証情報を使用して my.vmware.com にログインした後、.GZ パッケージに圧縮された TAR ファイルとして取得できます。TAR ファイルをローカル システムにダウンロードします。

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 1.10 以降の Horizon Cloud Connector ディスク イメージをダウンロードします。

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 Cloud Connector 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 Cloud Connector 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 Cloud Connector 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 Cloud Connector 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 Cloud Connector 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 Cloud Connector 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。

次のステップ

第1世代テナント - Horizon ポッドと仮想アプライアンスの第1世代 Horizon 制御プレーンとのペアリングの準備ができていることを確認するの順序に従って、ポッドのオンボーディング ワークフローを続行します。第1世代テナント - Horizon Cloud Connector 構成ポータルを使用して Horizon ポッドと第1世代 Horizon Cloud のペアリングを完了するに進みます。

コマンドライン インターフェイスの使用による Horizon Cloud Connector への SSH アクセスの有効化

Horizon Cloud Connector 2.0 以降では、アプライアンスとポッドをペアリングする前にプライマリ ノードとの SSH 接続を使用する場合、またはワーカー ノードへの SSH アクセスを有効にする場合に、これらの手順を使用します。Horizon Cloud Connector 1.10 以前では、これらの手順を使用して、ポッドとペアリングする前にデプロイされたアプライアンスへの SSH アクセスを有効にします。

アプライアンスとポッドをペアリングする前に Horizon Cloud Connector への SSH アクセスを必要としない場合は、アプライアンスがポッドとペアリングされてから SSH アクセスを有効にすることができます。『管理ガイド』の構成ポータルを使用して Horizon Cloud Connector アプライアンスで SSH を有効または無効にするを参照してください。

前提条件

オンプレミスまたは VMware Cloud on AWS にある Horizon ポッドの場合は、次のタスクを実行します。

- [第1世代テナント - Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイする](#)のサブトピックで説明されているように、Horizon Cloud Connector アプライアンスがポッドの環境に正常にデプロイされ、まだ Connection Server とペアリングされていないことを確認します。
- (Horizon Cloud Connector 1.9 以降) SSH アクセスのために推奨されるパブリック キー認証を使用するには、SSH パブリック キーを生成して、アプライアンスのデプロイ中にキーを登録します。[第1世代テナント - オンプレミスおよびオールイン SDDC Horizon ポッド : Horizon Cloud Connector をダウンロードして、ポッドの vSphere 環境にデプロイする](#)を参照してください。

デプロイ中にパブリック キーを登録しない場合は、このトピックの後の手順で説明するとおりに、SSH アクセスを有効にした後に、パブリック キーを適切なキー ファイルにコピーできます。

オンプレミスまたは VMware Cloud on AWS にある Horizon ポッドに対して、Horizon Cloud Connector 1.9 以降へのパブリック キー認証による SSH アクセスを有効にする

重要： Horizon Cloud Connector 1.9 以降、root ユーザー アカウントの SSH アクセスはサポートされなくなりました。セキュリティを強化するために、SSH アクセスは、パブリック キー（強く推奨）またはパスワード認証を使用した ccadmin ユーザー アカウントでのみサポートされます。

引き続き root アカウントを使用して、アプライアンスで SSH 以外の管理タスクを実行することができます。

次の手順を使用して、ccadmin ユーザーの Horizon Cloud Connector への SSH アクセスを有効にします。セキュリティのベスト プラクティスとして、アプライアンスに ccadmin ユーザーを認証するための SSH パブリック キーを構成することを強くお勧めします。

- 1 vSphere Client を使用して、デプロイされたアプライアンスのコンソールを起動し、OVA を vSphere にデプロイしたときに設定した root アカウントとパスワードを使用してアプライアンスにログインします。
- 2 ccadmin アカウントのパスワードを設定します。

```
passwd ccadmin
```

注： 新しいパスワードが強力なパスワードのセキュリティ基準を満たしていることを確認します。パスワードは 8 文字以上で、少なくとも 1 つの大文字、1 つの数字、および 1 つの特殊文字を含んでいることを確認します。

- 3 次のコマンドを実行して、SSH アクセスを有効にします。

```
/opt/vmware/bin/configure-adapter.py --sshEnable
```

- 4 次のいずれかの方法を使用して、パブリック キー認証を構成します。
 - アプライアンスのデプロイ ウィザードの [テンプレートのカスタマイズ] 手順で SSH パブリック キーを登録した場合、パブリック キー認証はすでに構成されており、追加の手順を行う必要はありません。

詳細については、[第1世代テナント - オンプレミスおよびオールイン SDDC Horizon ポッド : Horizon Cloud Connector をダウンロードして、ポッドの vSphere 環境にデプロイする](#)を参照してください。

- アプライアンスのデプロイ中に SSH パブリック キーを登録していなかった場合は、クライアント システムから次のコマンドを実行し、`<IP_appliance>` を Horizon Cloud Connector アプライアンスの IP アドレスに置き換えます。確認の画面が表示されたら、`ccadmin` のパスワードを入力します。

```
ssh-copy-id ccadmin@<IP_appliance>
```

`ssh-copy-id` コマンドは、パブリック キーを `ccadmin` ユーザーの `~/.ssh/authorized_keys` ファイルにコピーします。

注： パブリック キー認証を構成しない場合は、パスワード認証情報を使用して、SSH アクセスに `ccadmin` ユーザーを認証します。セキュリティを強化するために、SSH アクセスにはパスワード認証ではなく、パブリック キー認証を使用することを強くお勧めします。

これで、アプライアンスへの SSH アクセスが有効になります。

注： 昇格された権限を持つ `ccadmin` ユーザーとしてコマンドを実行するには、SSH セッションのコマンドに `sudo` プリフィックスを追加します。

オンプレミスまたは VMware Cloud on AWS にある Horizon ポッドの Horizon Cloud Connector 1.8 以前への SSH アクセスを有効にする

Horizon Cloud Connector 1.8 以前への SSH 接続を開くには、SSH アクセスを有効にして、`root` ユーザーとしてログインする必要があります。

- 1 vSphere Client を使用して、デプロイされたアプライアンスのコンソールを起動し、OVA を vSphere にデプロイしたときに設定した `root` アカウントとパスワードを使用してアプライアンスにログインします。
- 2 次のコマンドを実行して、SSH アクセスを有効にします。

```
/opt/vmware/bin/configure-adapter.py --sshEnable
```

これで、アプライアンスへの SSH アクセスが有効になります。

オンプレミスまたは VMware Cloud on AWS にある Horizon ポッドの Horizon Cloud Connector への SSH アクセスを無効にする

アプライアンスへの SSH アクセスを無効にする必要がある場合、次のコマンドを使用します。

```
/opt/vmware/bin/configure-adapter.py --sshDisable
```

Azure VMware Solution (AVS) にある Horizon ポッドの Horizon Cloud Connector への SSH アクセスを有効にする

- 1 Azure ポータルで、Horizon Cloud Connector 仮想マシンに移動します。[実行コマンド] アクションを開始して、[RunPowerShellScript] を選択します。
- 2 次のコマンドを実行して、SSH アクセスを有効にします。

```
/opt/vmware/bin/configure-adapter.py --sshEnable
```

これで、アプライアンスへの SSH アクセスが有効になります。

- 3 Horizon Cloud Connector 1.7 をデプロイし、SSH パブリック キー認証を使用する場合は、次の追加コマンドを実行します。

```
chmod 744 /home/ccadmin
```

Google Cloud VMware Engine (GCVE) にある Horizon ポッドの Horizon Cloud Connector への SSH アクセスを有効にする

GCVE のポッドとアプライアンスをペアリングする前に Horizon Cloud Connector への SSH アクセスを有効にするには、Horizon Cloud Connector 仮想マシン インスタンスを作成する際に、起動スクリプトに適切な行を含めます。第1世代テナント - Horizon ポッド - Google Cloud VMware Engine を使用したフェレデーションアーキテクチャ：Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイするを参照してください。

次の手順

第1世代テナント - Horizon ポッドと仮想アプライアンスの第1世代 Horizon 制御プレーンとのペアリングの準備ができていることを確認するに進みます。次に、第1世代テナント - Horizon Cloud Connector 構成ポータルを使用して Horizon ポッドと第1世代 Horizon Cloud のペアリングを完了するに進みます。ペアリングが正常に完了すると、Horizon Cloud Connector の Web ベースの構成ポータルにトグルが表示され、アプライアンスの SSH アクセスを無効にしたり、無効になっていた SSH を再度有効にしたりできます。

Horizon Cloud Connector 1.6 以降のプロキシ設定の変更

Horizon Cloud Connector OVF テンプレートのデプロイ中に HTTP プロキシを設定できます。デプロイ後にこれらのプロキシ設定を変更する場合は、`configure-webproxy.py` コマンドを使用する必要があります。

`configure-webproxy.py` コマンドは、デプロイされた Horizon Cloud Connector アプライアンスの `/opt/vmware/bin` ディレクトリにあります。

注： プロキシ設定とアプライアンスの更新については、次のガイドラインに従ってください。

- Horizon Cloud Connector 1.6 以降を新しいバージョンに手動で更新する場合は、プロキシ設定を再構成する必要があります。元のプロキシ構成は、手動でのアプライアンスの更新後に引き継がれません。
- Horizon Cloud Connector 1.6 以降が新しいバージョンに自動的に更新された場合は、自動更新によってプロキシ設定が引き継がれます。プロキシ設定を再構成する必要はありません。
- Horizon Cloud Connector 仮想アプライアンスの既存のプロキシ設定を表示するには、次のコマンドを実行します。

```
cat /opt/container-data/cc-settings/proxy.conf
```

`configure-webproxy.py` を使用するための構文

`configure-webproxy.py` でスクリプトを作成するには以下の構文を使用します。

```
configure-webproxy.py [argument1 [value1]] [argument2 [value2]] ...
```

コマンドの使用法と使用可能な引数のリストを表示するには、`configure-webproxy.py -h` または `configure-webproxy.py --help` を実行します。

configure-webproxy.py の引数

すべての引数は、configure-webproxy.py スクリプトではオプションです。

引数	説明
--proxyHost	HTTP プロキシ サーバのホスト名または IP アドレス
--proxyPort	プロキシ接続のポート番号
--noProxyFor	HTTP プロキシをバイパスするように構成されたホストまたはネットワーク範囲。複数の値を入力する場合は、コンマで区切ります。
--proxySsl	プロキシ接続に SSL を使用するかどうかを指定します。使用できる値は、true または false です。
--proxyUsername	HTTP プロキシのユーザー名
--proxyPassword	HTTP プロキシのパスワード
--implicitNonProxyHosts	ペアリングされたポッドの Connection Server と vCenter Server を、HTTP プロキシをバイパスするホストのリストに暗黙的に追加するかどうかを指定します。使用できる値は、true または false です。デフォルトは、true です。 ご使用の環境でプロキシを経由するために Connection Server および vCenter Server への内部リクエストが必要な場合、この引数を false に設定します。この場合、--noProxyFor によって明示的に指定されたホストのみがプロキシをバイパスします。

サンプル スクリプト

```
configure-webproxy.py --proxyHost PROXYEXAMPLE --proxyPort 80 --proxySsl=false
--noProxyFor ".AD-DOMAIN.EXAMPLE.COM,10.109.*"
```

このサンプル スクリプトは、次のプロキシ設定を構成します。

- PROXYEXAMPLE はプロキシ サーバです。
- プロキシ接続では、ポート 80 が使用されます。
- プロキシ接続では、SSL は使用されません。
- .AD-DOMAIN.EXAMPLE.COM および 10.109* に該当するホストはプロキシをバイパスします。
- また、ペアリングされたポッドの Connection Server と vCenter Server はデフォルトで暗黙的にプロキシをバイパスします。

Horizon Cloud Connector 仮想アプライアンスの CA 署名付き証明書の構成

セキュリティを強化するために、Horizon Cloud Connector 仮想アプライアンスのカスタム CA 署名付き証明書を構成できます。

前提条件

- 完全な証明書チェーンが PEM 形式で使用できることを確認します。
- PEM ファイルがパスフレーズではなくプライベート キーを使用して生成されていることを確認します。
- 発行された証明書に FQDN と Subject Alt Name が含まれていることを確認します。

手順

- 1 デプロイされた Horizon Cloud Connector 仮想アプライアンスへの SSH セッションを開きます。
- 2 ディレクトリ `/root/server.crt` に CA 署名付き証明書をコピーします。
- 3 ディレクトリ `/root/server.key` に CA 署名キーをコピーします。
- 4 既存の証明書をバックアップします。

- (Horizon Cloud Connector バージョン 1.4 以降) 次のコマンドを使用します。

```
cp /opt/container-data/certs/hze-nginx/server.crt /opt/container-data/certs/hze-nginx/server.crt.orig
```

- (Horizon Cloud Connector バージョン 1.3 以前) 次のコマンドを使用します。

```
cp /etc/nginx/ssl/server.crt /etc/nginx/ssl/server.crt.orig
```

- 5 既存のキーをバックアップします。

- (Horizon Cloud Connector バージョン 1.4 以降) 次のコマンドを使用します。

```
cp /opt/container-data/certs/hze-nginx/server.key /opt/container-data/certs/hze-nginx/server.key.orig
```

- (Horizon Cloud Connector バージョン 1.3 以前) 次のコマンドを使用します。

```
cp /etc/nginx/ssl/server.key /etc/nginx/ssl/server.key.orig
```

- 6 既存の `nginx.conf` ファイルをコピーします。

- (Horizon Cloud Connector バージョン 1.4 以降) 次のコマンドを使用します。

```
cp /opt/container-data/conf/hze-nginx/nginx.conf /opt/container-data/conf/hze-nginx/nginx.conf.orig
```

- (Horizon Cloud Connector バージョン 1.3 以前) 次のコマンドを使用します。

```
cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.orig
```

- 7 お使いの仮想アプライアンスのバージョンに適したディレクトリに CA 証明書をコピーします。

- (Horizon Cloud Connector バージョン 1.4 以降) 次のコマンドを使用します。

```
cp /root/server.crt /opt/container-data/certs/hze-nginx/server.crt
```

- (Horizon Cloud Connector バージョン 1.3 以前) 次のコマンドを使用します。

```
cp /root/server.crt /etc/nginx/ssl/server.crt
```

- お使いの仮想アプライアンスのバージョンに適したディレクトリに CA 証明書のキー ファイルをコピーします。

- (Horizon Cloud Connector バージョン 1.4 以降) 次のコマンドを使用します。

```
cp /root/server.key /opt/container-data/certs/hze-nginx/server.key
```

- (Horizon Cloud Connector バージョン 1.3 以前) 次のコマンドを使用します。

```
cp /root/server.key /etc/nginx/ssl/server.key
```

- 証明書とキー ファイルの所有者と権限を確認します。

- (Horizon Cloud Connector バージョン 1.4 以降) 次のコマンドを使用します。

```
chown -R hze-nginx:hze-nginx /opt/container-data/certs/hze-nginx
chmod 644 /opt/container-data/certs/hze-nginx/server.crt
chmod 600 /opt/container-data/certs/hze-nginx/server.key
```

- (Horizon Cloud Connector バージョン 1.3 以前) 次のコマンドを使用します。

```
chown -R root:root /etc/nginx/ssl
chmod -R 600 /etc/nginx/ssl
```

- 証明書内の発行された FQDN が、nginx の構成ファイルにあるサーバリスン 443 ブロックのサーバ名ディレクティブと一致することを確認します。

- (Horizon Cloud Connector バージョン 1.4 以降) nginx の構成ファイルは /opt/container-data/conf/hze-nginx/nginx.conf にあります。
- (Horizon Cloud Connector バージョン 1.3 以前) nginx の構成ファイルは /etc/nginx/nginx.conf にあります。

- nginx を確認して再起動します。

- (Horizon Cloud Connector バージョン 2.0 以降) 次のコマンドを使用します。

```
kubectl rollout restart daemonset hze-nginx -n hze-system
```

- (Horizon Cloud Connector バージョン 1.4 ~ 1.10) 次のコマンドを使用します。

```
docker exec -i hze-nginx sudo nginx -t
systemctl restart hze-nginx
```

- (Horizon Cloud Connector バージョン 1.3 以前) 次のコマンドを使用します。

```
nginx -t
systemctl restart nginx
```

12 [ようこそ] 画面で SSL サンプリントを更新します。

- (Horizon Cloud Connector バージョン 2.0 以降) 次のコマンドを使用します。

```
/opt/vmware/bin/configure-welcome-screen.py
/usr/bin/killall --quiet vami_login
```

- (Horizon Cloud Connector バージョン 1.4 ~ 1.10) 次のコマンドを使用します。

```
docker exec -i hze-core sudo /opt/vmware/bin/configure-welcome-screen.py
/usr/bin/killall --quiet vami_login
```

13 新しい証明書をテストするには、Web ブラウザで Horizon Cloud Connector ユーザー インターフェイスの URL を再ロードします。**14** (オプション) 証明書が正常に動作する場合は、バックアップ ファイルを削除します。

- (Horizon Cloud Connector バージョン 1.4 以降) 次のコマンドを使用します。

```
rm /opt/container-data/certs/hze-nginx/server.crt.orig
rm /opt/container-data/certs/hze-nginx/server.key.orig
rm /opt/container-data/conf/hze-nginx/nginx.conf.orig
```

- (Horizon Cloud Connector バージョン 1.3 以前) 次のコマンドを使用します。

```
rm /etc/nginx/ssl/server.crt.orig
rm /etc/nginx/ssl/server.key.orig
rm /etc/nginx/nginx.conf.orig
```

15 ルート ディレクトリにコピーした CA 証明書とキー ファイルを削除します。

次のコマンドを使用します。

```
rm /root/server.crt
```

```
rm /root/server.key
```

Horizon Cloud Connector 仮想アプライアンスと NTP サーバの同期

Horizon Cloud Connector 仮想アプライアンスがクラウド制御プレーンおよび必要な Connection Server インスタンスで正しく認証されるようにするには、仮想アプライアンスのクロックを NTP (Network Time Protocol) サーバと同期する必要があります。ホスト自身が NTP サーバと適切に同期していることを最初に確認した後、Horizon Cloud Connector 仮想アプライアンスのクロックを仮想アプライアンスが存在する物理 ESXi ホストのクロックと同期します。

手順

- ◆ (推奨される方法) Horizon Cloud Connector 仮想アプライアンスを、仮想アプライアンスが存在する物理 ESXi ホストと同期します。

- ESXi ホストのクロックが NTP サーバと適切に同期していることを確認します。

詳細については、[VMware vSphere のドキュメント](#)を参照してください。

- vSphere Client を使用して Horizon Cloud Connector 仮想アプライアンスの [設定の編集] ウィンドウを開き、[ホストとの時刻の同期] オプションを有効にします。

詳細な手順については、[VMware vSphere のドキュメント](#)を参照してください。

注: Horizon Cloud Connector 1.5 以降では、[ホストとの時刻の同期] がデフォルトで有効になっています。

- ◆ (代替方法) Horizon Cloud Connector 仮想アプライアンスを物理 ESXi ホストと同期できない場合は、仮想アプライアンスを NTP サーバと直接同期できます。

注: 時刻同期に推奨される方法は、仮想アプライアンスを物理 ESXi ホストと同期することです。推奨される方法を実行できない場合にのみ、次の手順を実行します。

- Horizon Cloud Connector 仮想アプライアンスへの SSH 接続を開き、root ユーザーとしてログインします。
- vi などのテキスト エディタを使用して、編集する `timesyncd.conf` ファイルを開きます。

```
vi /etc/systemd/timesyncd.conf
```

- 次の例のように、[Time] セクションを編集します。 `ntpAddress` を、使用する NTP サーバのドメイン名に置き換えます。

```
[Time]
#FallbackNTP=time1.google.com time2.google.com time3.google.com time4.google.com
NTP=ntpAddress
```

変更を `timesyncd.conf` ファイルに保存し、テキスト エディタを終了します。

- 仮想アプライアンスのネットワーク サービスを再起動します。

```
systemctl restart systemd-networkd
```

- 仮想アプライアンスの `timesync` サービスを再起動します。

```
systemctl restart systemd-timesyncd
```

- 仮想アプライアンスのクロックが、指定された NTP サーバと同期していることを確認します。

[ベーシック機能] プロファイルを持つ Horizon Cloud Connector 1.8 または 1.9 : Horizon Cloud サービスを手動で有効にする

Horizon Cloud Connector 1.8 または 1.9 をデプロイし、デプロイ ウィザードで [ベーシック機能] プロファイルを選択した場合は、Horizon サブスクリプション ライセンス サービスのみが有効になります。Horizon Cloud Connector が提供する追加のクラウドベース サービスを有効にするには、この記事で説明する手順を実行します。コマンドは、Horizon Cloud Connector アプライアンスで SSH セッションを使用して実行します。

Horizon Cloud Connector 1.8 または 1.9 アプライアンスをデプロイして [ベーシック機能] プロファイルを選択すると、次のコンポーネントがデプロイされたアプライアンスでデフォルトで無効になります。この手順を使用して、これらのコンポーネントの1つ以上を手動で有効にすることができます。各コンポーネントでは、特定のクラウドブレイク サービスを使用できます。

Connection Server 監視サービス (CSMS)

このコンポーネントでは、Horizon ポッドで Cloud Monitoring Service (CMS) を使用できます。Horizon Cloud Connector が [ベーシック機能] プロファイルでデプロイされたときに CMS を使用する場合、以下の手順を実行して、このコンポーネントを有効にする必要があります。CMS については、[Cloud Monitoring Service の統合された可視性とインサイトの概要](#)のページを参照してください。

クラウド ブローカ クライアント サービス (CBCS)

このコンポーネントでは、Horizon ポッドで Universal Broker を使用できます。Universal Broker を使用し、Horizon ポッドのリソースに基づいてマルチクラウド割り当てを構成する場合は、このコンポーネントを有効にする必要があります。Universal Broker については、[Universal Broker のシステム アーキテクチャとコンポーネント](#)のページを参照してください。

イメージ ローカリティ サービス (ILS)

このコンポーネントでは、Horizon ポッドで Horizon Image Management Service を使用できます。Horizon Image Management Service を使用して Horizon ポッドからシステム イメージを追跡および管理する場合は、このイメージ ローカリティ サービスを有効にする必要があります。Horizon Image Management Service については、[クラウドからの Horizon イメージの管理](#)のページを参照してください。

重要： 次のガイドラインに従います。

- アプライアンスのデプロイ時に Horizon Cloud Connector 1.8 または 1.9 をデプロイし、[ベーシック機能] プロファイルを選択した場合にのみ、これらの手順を使用してサービスを有効にします。
- 他のバージョンの Horizon Cloud Connector には、これらの手動による有効化手順を実行しないでください。これらの手順は、その他のバージョンには適用されません。
- [フル機能] プロファイルでバージョン 1.8 または 1.9 をデプロイした場合は、これらの手動による有効化手順を実行しないでください。このシナリオでは、Horizon ポッドでの使用がサポートされているクラウド管理サービスは、デフォルトですでに有効で、実行されています。
- サービスを有効にした後は、手動で無効にしないでください。サービスを無効にすると、予期しない結果が生じる可能性があります。
- Horizon Cloud Connector で CSMS サービスを無効のままにする場合、sync failed メッセージが表示されないようにするには、ポッドのペアリングを完了する前にテナント アカウントの CMS をオフに切り替える必要があります。[Horizon Cloud Connector で CSMS サービスを無効にしておく場合に、同期失敗メッセージが表示されないようにする方法](#)を参照してください。

手順

- 1 デプロイされている Horizon Cloud Connector 1.8 または 1.9 アプライアンスに移動し、有効にする追加のサービスに必要なリソース キャパシティを構成します。

有効にする追加サービス	最小リソース
Connection Server 監視サービス (CSMS)	合計 7 個の vCPU、8 GB のメモリ (RAM)、40 GB のデータストア
クラウド ブローカ クライアント サービス (CBCS)	合計 6 個の vCPU、8 GB のメモリ (RAM)、40 GB のデータストア
イメージ ローカリティ サービス (ILS)	合計 6 個の vCPU、7.5 GB のメモリ (RAM)、40 GB のデータストア
2 個以上	合計 8 個の vCPU、8 GB のメモリ (RAM)、40 GB のデータストア

2 使用する各サービスを有効にして起動します。

- a Horizon Cloud Connector アプライアンスで SSH (Secure Shell) セッションを開き、root ユーザーとしてログインします。
- b 有効にする各サービスに対応するコマンドを実行します。

サービス	コマンド
Connection Server 監視サービス (Cloud Monitoring Service に必要)	systemctl enable csms systemctl restart csms
クラウド ブローカ クライアント サービス	systemctl enable cbcs systemctl restart cbcs
イメージ ローカリティ サービス	systemctl enable ils systemctl restart ils

次のステップ

Connection Server 監視サービス (CSMS) を有効にした場合は、テナントの Cloud Monitoring Service 設定でサービスを同期するようにし、CSMS によって送信される監視データを受信するようになる必要もあります。

- 1 ブラウザで、テナント ログイン認証情報を使用して、cloud.horizon.vmware.com の Horizon Universal Console にログインし、[はじめに] ページに移動して、ページの [全般的なセットアップ] セクションを展開し、[Cloud Monitoring Service] 行で [編集] をクリックします。
- 2 [Cloud Monitoring Service] トグルの現在の状態に応じて、次のいずれかの手順を実行します。

トグルがオフになっている場合は、オンに切り替えます。

トグルがすでにオンになっている場合は、まずトグルをオフにして、数分待ちます。その後、トグルをオンに戻します。この組み合わせにより、サービスは、新しく有効化された CSMS からのデータの受信を開始します。

第1世代テナント - ネイティブの Amazon EC2 の Horizon Cloud Connector に対し第1世代の Horizon Cloud 制御プレーン サービスを手動で有効にする

ネイティブの Amazon EC2 インフラストラクチャに Horizon Cloud Connector をデプロイすると、サブスクリプション ライセンス サービスのみが有効な状態になります。Horizon Cloud Connector で提供される追加の

クラウドベース サービスを有効にするには、以下の手順にあるように、Horizon Cloud Connector アプライアンスで SSH セッションを使用します。

重要：

- これらのサービスを 1 つ以上有効にする場合は、Horizon ポッドを第 1 世代 Horizon Cloud とペアリングする前に有効化を実行します。[Horizon ポッドと仮想アプライアンスのペアリングの準備ができていることを確認する](#)を参照してください。
- Horizon Cloud Connector で CSMS サービスを無効のままにする場合、sync failed メッセージが表示されないようにするには、ポッドのペアリングを完了する前にテナント アカウントの CMS をオフに切り替える必要があります。[Horizon Cloud Connector で CSMS サービスを無効にしておく場合に、同期失敗メッセージが表示されないようにする方法](#)を参照してください。

オプションで、Horizon Cloud Connector の次のサービスを 1 つ以上有効にすることができます。

Connection Server 監視サービス (CSMS)

このコンポーネントでは、Horizon ポッドで Cloud Monitoring Service (CMS) を使用できます。この Horizon Cloud Connector デプロイとそのペアの Horizon ポッドで CMS を使用できるようにするには、以下の手順を使用して、このコンポーネントを有効にする必要があります。CMS については、[Cloud Monitoring Service の統合された可視性とインサイトの概要](#)のページを参照してください。

クラウド ブローカ クライアント サービス (CBCS)

このコンポーネントでは、Horizon ポッドで Universal Broker を使用できます。Universal Broker を使用し、Horizon ポッドのリソースに基づいてマルチクラウド割り当てを構成する場合は、このコンポーネントを有効にする必要があります。Universal Broker については、[Universal Broker のシステム アーキテクチャとコンポーネント](#)のページを参照してください。

イメージ ローカリティ サービス (ILS)

このコンポーネントでは、Horizon ポッドで Horizon Image Management Service を使用できます。Horizon Image Management Service を使用して Horizon ポッドからシステム イメージを追跡および管理する場合は、このコンポーネントを有効にする必要があります。Horizon Image Management Service については、[クラウドからの Horizon イメージの管理](#)のページを参照してください。

注： 現在のリリースでは、Horizon 環境での Horizon Image Management Service (IMS) の使用は、オンプレミス環境でのみサポートされています。オンプレミス以外の Horizon 環境での IMS の使用は現在サポートされていません。したがって、次の手順を使用して、フェデレーション デプロイのネイティブ Amazon EC2 にデプロイされた Horizon Cloud Connector でイメージ ローカリティ サービス コンポーネントを有効にできますが、現在、そのフェデレーション デプロイ タイプでは、対応する機能の実際の使用はサポートされていません。

前提条件

デプロイされている Horizon Cloud Connector 仮想マシンのバージョンが [4 章 第 1 世代の Horizon Cloud 制御プレーンを使用する VMware Horizon 8 ポッド - 要件チェックリスト - 2023 年 11 月 2 日のサービス更新](#)に合わせて適切に更新されましたに記載されているリソース要件を満たしていることを確認します。

手順

- 1 ポッドの環境内の Amazon EC2 インフラストラクチャのデプロイされた Horizon Cloud Connector アプライアンスに移動します。
- 2 使用する各サービスの有効化手順を実行します。
 - a Horizon Cloud Connector アプライアンスで SSH (Secure Shell) セッションを開き、root ユーザーとしてログインします。
 - b `/opt/container-data/conf/container-info` ファイルのバックアップを作成します。

```
cp /opt/container-data/conf/container-info /opt/container-data/conf/container-info-backup
```

- c `/opt/container-data/conf/container-info` ファイルを編集のために開きます。

```
vi /opt/container-data/conf/container-info
```

- d 有効にする各サービス (クラウド ブローカ クライアント サービス (CBCS)、Connection Server 監視サービス (CSMS)、イメージ ローカリティ サービス (ILS)) の "enabled" フラグを "n" から "y" に更新します。

```
{
  "name": "cbcs",
  "namespace": "cbcs-system",
  "buildNumber": "1593-b1b5139",
  "enabled": "y",
  "firstboot": "y",
  "profile": "all",
  "imgUrl": "hcs-docker-local.artifactory.eng.vmware.com/hcs-broker/dev/websocket-
client:1593-b1b5139"
},

{
  "name": "csms",
  "namespace": "cms-system",
  "buildNumber": "ultron-10",
  "enabled": "y",
  "firstboot": "y",
  "profile": "all",
  "imgUrl": "eucsupp-docker-local.artifactory.eng.vmware.com/cloudmonitoring/
csms:ultron-10"
},

{
  "name": "ils",
  "namespace": "ils-system",
  "buildNumber": "9",
  "enabled": "y",
  "firstboot": "y",
  "profile": "all",
  "imgUrl": "hcs-docker-local.artifactory.eng.vmware.com/image-locality-service/
ils-k8-1/image-locality-service:9"
}
```

- e ファイルを保存します。
- f Horizon Cloud Connector で有効化する各サービスに適切なコマンドを実行します。

次のコマンドを実行して、クラウド ブローカ クライアント サービスを有効にします。

```
kubectl apply -f /opt/vmware/docker-container/cbcs/charts/cbcs-component.yaml
```

次のコマンドを実行して、Cloud Monitoring Service を有効にします。

```
kubectl apply -f /opt/vmware/docker-container/csms/charts/csms-component.yaml
```

次のコマンドを実行して、イメージ ローカリティ サービスを有効にします。

```
kubectl apply -f /opt/vmware/docker-container/ils/charts/ils-component.yaml
```


次のステップ

Connection Server 監視サービス (CSMS) を有効にした場合は、テナントの Cloud Monitoring Service 設定でサービスを同期するようにし、ポッドが Horizon Cloud Connector とペアリングされた後に CSMS によって送信される監視データを受信するようにする必要があります。

- 1 ブラウザで、テナント ログイン認証情報を使用して、cloud.horizon.vmware.com の Horizon Universal Console にログインし、[はじめに] ページに移動して、ページの [全般的なセットアップ] セクションを展開し、[Cloud Monitoring Service] 行で [編集] をクリックします。
- 2 [Cloud Monitoring Service] トグルの現在の状態に応じて、次のいずれかの手順を実行します。

トグルがオフになっている場合は、オンに切り替えます。

トグルがすでにオンになっている場合は、まずトグルをオフにして、数分待ちます。その後、トグルをオンに戻します。この組み合わせにより、サービスは、CSMS からのデータの受信を開始します。

Horizon Cloud Connector で CSMS サービスを無効にしておく場合に、同期失敗メッセージが表示されないようにする方法

このページでは、Horizon Cloud Connector で CSMS サービスを無効にしておく場合のベスト プラクティスについて説明します。クラウド プレーン内のすべてのテナントが作成されると、CMS が最初にデフォルトで有効になり、明示的にオフに切り替えない限り、そのままになります。CSMS サービスがポッドの Horizon Cloud Connector 内で無効な状態で、テナント アカウントで Cloud Monitoring Service (CMS) 設定がオンに切り替えられると、そのポッドに対して `sync failed` エラーが報告されます。

Horizon Cloud Connector で CSMS を無効のままにする場合、ベスト プラクティスとして Horizon Universal Console にログインし、ポッドを Horizon Cloud Connector とペアリングする前にテナント アカウントの CMS 設定をオフに切り替えます。Cloud Monitoring Service (CMS) は各テナントに提供されるクラウドプレーンサービスの1つで、CSMS サービスは、クラウド プレーンの CMS と通信するために Horizon Cloud Connector 内で実行されるマイクロサービスです。バージョン 1.9 で基本プロファイルの使用を選択した場合など、Horizon Cloud Connector アプライアンスの一部のデプロイでは、CSMS サービスがデフォルトで無効になります。このようなデプロイでは、クラウドプレーンの Cloud Monitoring Service の機能を利用できる場合、オプションで CSMS サービスを有効にできます。

ただし、テナントで CMS トグルが有効になっているときに CSMS サービスが Horizon Cloud Connector で実行されていない場合は、そのポッドに対して `sync failed` エラーが報告されます。CSMS マイクロサービスを無効のままにする場合、この `sync failed` メッセージが表示されないようにするには、ポッドを Horizon Cloud Connector とペアリングする前にテナント アカウントの Cloud Monitoring Service をオフに切り替える必要があります。

テナント アカウントの Cloud Monitoring Service をオフに切り替えるには、Horizon Universal Console (cloud.horizon.vmware.com) にログインします。テナントにまだポッドがない場合は、ログイン直後にコンソールの [はじめに] ページが表示されます。CMS トグルは、[全般的なセットアップ] メニューの [Cloud Monitoring Service] 行にあります。[全般的なセットアップ] を展開して、[Cloud Monitoring Service] 行内の [編集] をクリックし、Cloud Monitoring Service をオフに切り替えます。オフに切り替えた後、CSMS マイクロサービスが Horizon Cloud Connector で実行されないままポッドのペアリングを続行し、同時に `sync failed` メッセージが表示されないようにすることができます。

第1世代テナント - Horizon ポッドと仮想アプライアンスの第1世代 Horizon 制御プレーンとのペアリングの準備ができていることを確認する

Horizon ポッドを第1世代 Horizon 制御プレーン サービスにオンボーディングするこのワークフローのステップでは、`precheck.sh` 診断ツールを実行して、ポッドと Horizon Cloud Connector の両方ともペアリング プロセスの準備ができていることを確認します。最初に診断を実行し、システム コンポーネントおよび構成で見つかった障害となっている問題を修正することにより、ペアリング プロセスが成功する可能性を最大限に高めることができます。

注： `precheck.sh` 診断ツールは Horizon Cloud Connector 1.6 以降でのみ使用できます。Horizon Cloud Connector 1.5 以前のバージョンをダウンロードしてデプロイした場合は、次の手順を無視して直接第1世代テナント - Horizon Cloud Connector 構成ポータルを使用して Horizon ポッドと第1世代 Horizon Cloud のペアリングを完了するに進みます。

`precheck.sh` 診断ツールは、制御プレーンと Horizon ポッドを正常にペアリングするために必要なサービスとコンポーネントの健全性を検証します。さらに、ツールは以下を確認します。

- 証明書とプロキシ設定に関連する構成が正しいこと。
- 制御プレーンおよび Horizon Connection Server との Horizon Cloud Connector の接続を確立できません。
- Horizon Cloud Connector に SSL 関連の問題があるかどうか。

前提条件

次の項目を確認します。

- 第1世代テナント - Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイするの手順が完了しました。コマンドライン インターフェイスの使用による Horizon Cloud Connector への SSH アクセスの有効化を行う手順、およびクラウドホスト型サービスのいずれかを有効にする場合は、これらのサービスを手動で有効にする手順も含まれます。
- Horizon Cloud Connector 仮想アプライアンスがパワーオンされていること。

手順

- 1 デプロイされた Horizon Cloud Connector 仮想アプライアンスへの SSH セッションを開きます。
- 2 次のコマンドを使用して診断ツールを実行します。`CS-FQDN` をポッドの Connection Server の完全修飾ドメイン名 (FQDN) に置き換えます。

```
sudo /opt/vmware/bin/precheck.sh CS-FQDN
```

診断ツールは、正常なペアリング プロセスを妨げる問題を検出すると、次の情報をレポートします。

- 問題のあるコンポーネントまたはサービスの名前
- 問題のあるコンポーネントまたはサービスのステータス
- 関連するエラー メッセージと詳細

- コンポーネントまたはサービスを健全で準備が完了した状態に復元するために推奨される修正手順（該当する場合）

注： 診断ツールは、予想される状態として、常に次のいずれかまたは両方を出力の一部として報告します。オンボーディング ワークフローのこの段階では、どちらの状態も正常で予想されるものです。どちらもペアリングプロセスをブロックしません。

- ```
Component/Service Name: "Cloud Broker Client Service"
Status: "NOT_INITIALIZED"
Message: Service is not initialized.
```

この状況は、制御プレーンの Universal Broker サービスに関連しています。このサービスは、[マルチクラウド割り当てのための Horizon Universal Broker のセットアップの説明](#)に従って有効化されるまで、NOT\_INITIALIZED 状態を維持します。Universal Broker が NOT\_INITIALIZED 状態のままでも、Horizon ポッドを正常にペアリングすることができます。したがって、この状態はブロックの問題を表すものではなく、無視してもかまいません。

- ```
Component/Service Name: "Connector Client Service"
Status: "FAIL"
Message: Connector service is initialized post on-boarding.
```

初期化プロセスには制御プレーンへの接続が必要であるため、ペアリング プロセスの完了後に Horizon Cloud Connector クライアント サービスが初期化されます。そのため、オンボーディング ワークフローのこの段階では FAIL 状態が予想されます。ペアリング プロセスが成功すると、Horizon Cloud Connector クライアント サービスが初期化され、FAIL 状態がクリアされます。

- 3 診断ツールがペアリング プロセスを妨げる問題を報告した場合は、影響を受けるコンポーネントまたはサービスを調査し、推奨される修復手順を実行します。すでに説明したように、「Cloud Broker Client Service」および「Connector Client Service」のエラー状態は、ブロックの問題ではないため無視してかまいません。

必要に応じて、手順 2 と 3 を繰り返して診断ツールを再度実行し、ペアリング プロセスを妨げるブロックの問題がツールから報告されなくなるまで問題に対してトラブルシューティングを行います。これで、Horizon ポッドと Horizon Cloud Connector をペアリングするプロセスの準備が整いました。

注： 診断ツールによって報告されたブロックの問題を最初にクリアせずにペアリング プロセスを試行すると、ペアリング プロセスが失敗する場合があります。

- 4 [第1世代テナント - Horizon Cloud Connector 構成ポータル](#)を使用して Horizon ポッドと第1世代 Horizon Cloud のペアリングを完了するの順に従って、ポッドのオンボーディング ワークフローを続行します。

第1世代テナント - Horizon Cloud Connector 構成ポータルを使用して Horizon ポッドと第1世代 Horizon Cloud のペアリングを完了する

Horizon ポッドを第1世代 Horizon Cloud にオンボーディングするワークフローのこの手順では、Horizon Cloud Connector 構成ポータルを使用して、Horizon Cloud Connector が Horizon ポッドの Connection

Server とのペアリングに使用する詳細を指定します。これらの手順を正常に完了すると、ポッドが第 1 世代 Horizon Cloud テナント環境に接続されます。

重要: この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

注目: Horizon サブスクリプション ライセンスとその他のクラウド ホスト型サービスがポッドに対して適切に機能するようにするには、1 つの Horizon Cloud Connector アプライアンスのみをポッドとペアリングする必要があります。複数のアプライアンスと 1 つのポッドのペアリングは、アプライアンスの更新やトラブルシューティングの手順など、特別な状況でのみ許可されています。

ペアリング プロセスでの Horizon ポッド、第 1 世代 Horizon Cloud、および Horizon Cloud Connector の相互の関係を示す図については、「[第 1 世代テナント - 第 1 世代 Horizon Cloud Service を既存の Horizon ポッドに接続してクラウド ホスト型サービスを使用する](#)」に示されている図を参照してください。

注: Horizon Cloud Connector 構成ポータルで接続の問題が発生した場合は、[VMware ナレッジベースの記事 KB79859](#) のトラブルシューティング情報を参照してください。

前提条件

必要な準備の手順を完了していることを確認します。

- [第 1 世代テナント - Horizon Cloud Connector をダウンロードしてポッドの環境にデプロイする](#) の下の該当するサブトピックの手順を完了していることを確認します。
- [第 1 世代テナント - Horizon ポッドと仮想アプライアンスの第 1 世代 Horizon 制御プレーンとのペアリングの準備ができていることを確認する](#) の手順を完了していることを確認します。

また、次のことも確認します。

- プライマリ ノード (Horizon Cloud Connector 2.0 以降) または仮想アプライアンス (Horizon Cloud Connector 1.10 以前) がパワーオンされていること。
- ブラウザベースの Horizon Cloud Connector 構成ポータルを表示するための URL があること。URL は仮想アプライアンスの IP アドレス ([https://IP-address/](#) など) に基づいています。ここで、*IP-address* にはアプライアンスの IP アドレスが入ります。あるいは、DNS サーバで完全修飾ドメイン名 (FQDN) を Horizon Cloud Connector 仮想アプライアンスの IP アドレスにマッピングした場合、構成ポータルの URL はその FQDN になります。

[第 1 世代テナント - Horizon ポッドと Horizon Cloud Connector - 第 1 世代の制御プレーン サービスにオンボーディングする準備](#)に記載されているすべての項目を満たしていることを確認します。特に以下について確認します。

- Horizon ポッドと Horizon Cloud をペアリングするために Horizon Cloud Connector を使用する場合、[第 1 世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件](#)を満たしていること。

- ネットワーク トポロジ内の DNS 構成で、デプロイされた Horizon Cloud Connector がポッドの Connection Server の FQDN を解決できること。デプロイされた Horizon Cloud Connector が DNS を使用して Connection Server を解決できない場合、ポッドのドメイン認証情報を入力するステップでオンボーディング ウィザードに予期しないエラーが発生します。
- Horizon Cloud Connector 仮想アプライアンスが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し、ブラウザベースの構成ポータルを表示していること。ご使用の環境で、デプロイされたアプライアンスにプロキシ サーバとプロキシ構成を使用する必要がある場合、環境に必要なプロキシ設定を使用してデプロイ済みの Horizon Cloud Connector アプライアンスを構成したことを確認します。[第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備](#)、[Horizon Cloud Connector の既知の考慮事項](#)、および [Horizon Cloud Connector 1.6 以降のプロキシ設定の変更のプロキシ関連情報を参照してください](#)。
- ポッドをペアリングする Horizon Cloud のユーザー アカウントに関連付けられている My VMware アカウントの認証情報があること。[第1世代テナント - 第1世代 Horizon Cloud Service を既存の Horizon ポッドに接続してクラウド ホスト型サービスを使用する](#)で説明するように、クラウド管理プレーンに対して認証してコネクタをセットアップし、Horizon サブスクリプション サービスでそのライセンスを使用するための接続を確立するには、My VMware アカウントが必要です。
- ウィザードの最初のセットアップ手順では、次の情報を指定します。
 - Horizon Connection Server の FQDN
 - Active Directory ドメインの NETBIOS 名
 - そのドメインの Active Directory ユーザーのアカウント名。ユーザー名の SAM タイプを入力します。UPN (ユーザー プリンシパル名) は入力しないでください。このユーザー アカウントは、[Horizon Cloud 制御プレーンを使用した Horizon ポッド - 要件チェックリストの Horizon ポッドおよび Horizon Cloud Connector 要件セクション](#)に記載されている要件を満たしている必要があります。

注： ベスト プラクティスは、パスワードが変更されないサービス アカウントを使用することです。Horizon Cloud Connector は、サブスクリプション ライセンス情報を送信するなど、時間の経過とともにこれらの認証情報を使用して Horizon Connection Server と通信します。Horizon Cloud Connector バージョン 2.4 以降では、組織でこのアカウントのパスワードのローテーションが必要な場合は、「[Horizon Cloud Connector 2.4 以降 - Horizon Cloud Connector が Horizon Connection Server で使用する登録済みの Active Directory 認証情報を更新する](#)」の手順を使用して認証情報を更新できます。

手順

- 1 Web ベースの構成ポータルを起動するための URL を取得します。
 - (オンプレミスまたは VMware Cloud on AWS の Horizon ポッド)アプライアンスの青いコンソール画面から URL を取得します。

```

Horizon Cloud Connector
To set up browse to https://10.92.245.255/
SHA1 Thumbprint:
-----
SHA256 Thumbprint:
-----
Login
Set Timezone (Current:UTC)
Use Arrow Keys to navigate
and <ENTER> to select your choice.

```

- (Azure VMware Solution の Horizon ポッド) URL を取得するには、Azure ポータルのアプライアンス仮想マシンの [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 アドレスまたは FQDN をメモします。https://IP-address または https://FQDN/ のように URL を構成します。
- 2 ブラウザを使用して、前の手順で取得した URL に移動します。

重要： このステップでは、Horizon Cloud Connector が Horizon Cloud に接続してログイン画面を表示します。これはクラウド制御プレーンで My VMware アカウントの認証情報を認証するために使用されます。この接続は、ポート 443 を使用する送信 HTTPS です。ログイン画面が表示されない場合は、[第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件を満たしていることを確認](#)します。

Horizon Cloud Connector 構成ポータルにログインするためのログイン画面が表示されます。

- 3 ログイン画面で、My VMware アカウントの認証情報を入力し、[ログイン] をクリックします。

次のスクリーンショットは、[ログイン] をクリックする前に入力された認証情報を使用したログイン画面の例です。



サービス条件のメッセージが表示された場合は、[承認] をクリックして続行します。

構成ポータルには、ポッドのオンボーディングウィザードの最初の手順が表示されます。次のスクリーンショットは、フィールドの入力を完了する前のこの手順の例を示します。

Cloud Connector のバージョン : 2.2.0.0-19569899 ログのダウンロード ログアウト

セットアップ 1/3: Horizon ポッドに接続

Horizon Connection Server

* Horizon Connection Server に接続:

Horizon Connection Server 証明書

サムプリント (SHA-1):

件名:

発行者:

有効期間開始日:

有効期間終了日:

Horizon 認証情報

*ドメイン:

*ユーザー名:

*パスワード:

注： この時点で、システムは Horizon Cloud Connector 環境が正しく構成されていないかどうかを検出します。正しく構成されていない場合、構成を修正するために必要なクリーンアップ タスクを実行するように求めるメッセージが表示されます。

- 4 [Horizon Connection Server に接続] フィールドに、Horizon Cloud Connector とペアリングするポッドの Connection Server インスタンスの FQDN を入力します。

フィールドに入力すると、[接続] ボタンが表示されます。

* Horizon Connection Server に接続: 接続 リセット

- 5 FQDN を入力したら、[接続] をクリックします。

* Horizon Connection Server に接続: 接続

Horizon Cloud Connector は、指定された Connection Server と通信し、その証明書情報を取得しようとします。このプロセスには数分かかることがあります。通信が確立されると、ページには取得した証明書情報が表示されます。

Connection Server に有効なルート CA 証明書がない場合、証明書を自動的に検証できないことを示す警告メッセージが表示されます。チェック ボックスをクリックして、有効であることを確認する必要があります。次のスクリーンショットは、この状況の例です。



このメッセージが表示された場合は、表示された証明書情報が正確であることを確認し、チェック ボックスをクリックして次の手順に進みます。

注： Connection Server に有効なルート CA 証明書がある場合、ウィザードが自動的に情報を検証し、次の手順に進むことができます。

次のスクリーンショットは、チェック ボックスをクリックした後の画面を示します。



- 6 認証情報セクションで、この Connection Server に関連付けられている Active Directory ドメイン名を入力します。
- 7 ドメイン名の後に、そのドメインの Active Directory ユーザーのアカウント名の SAM タイプと、それに関連するパスワードを入力し、[接続] をクリックします。
 - ドメイン名の部分を除いて、ユーザー名の SAM タイプを入力します。UPN (ユーザー プリンシパル名) は入力しないでください。ユーザー インターフェイス フィールドが UPN 形式を受け入れて、拒否に失敗する場合でも、ここで UPN フォームを入力すると、以降のオンボーディング タスクが失敗します。
 - この管理者アカウントには、ポッドの root アクセス権を持つ Horizon 管理者ロールが事前に定義されている必要があります。管理者アカウントの要件の詳細については、[第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備](#)を参照してください。

次のスクリーンショットは、画面のこの領域を示しています。

Horizon 認証情報

*ドメイン: ⓘ

*ユーザー名: ⓘ

*パスワード: ⓘ

[接続](#)

注： この時点で、システムは、指定した Connection Server インスタンスがすでに Horizon Cloud Connector の別のインスタンスとペアリングされているかどうかを検出します。この場合、ページには、既存のペアリングを削除し、この Connection Server と新しい Horizon Cloud Connector インスタンスとのペアリングを実行する [新規インストール] アクションを実行するかを尋ねるメッセージが表示されます。新しい Horizon Cloud Connector インスタンスが既存のインスタンスよりも新しいバージョンである場合は、[Horizon Cloud Connector 仮想アプライアンスの手動更新](#)で説明されているように、既存のアプライアンス構成を新しい Horizon Cloud Connector インスタンスにコピーする [アップグレード] アクションを実行するオプションもあります。

メッセージの適切なアクション ボタンをクリックして、次の手順を使用してポッドのペアリングを続行します。

ウィザードの手順 2 が表示されます。

- 8 このウィザードの手順では、ポッドの詳細を指定します。

次のスクリーンショットは、この手順が完了した例です。

Cloud Connector のバージョン : 2.2.0.0-19569899 [ログのダウンロード](#) [ログアウト](#)

セットアップ 2/3: Horizon ポッドの構成

詳細

*名前: ⓘ

*データセンターの場所: ⓘ [新規](#) [編集](#)

詳細: ⓘ

[戻る](#) [保存](#)

これらの詳細は、ペアリングされた Connection Server インスタンスと Horizon Cloud Connector を Horizon Cloud テナント環境に関連付けるためにクラウド管理プレーンで使用されます。たとえば、指定した名前、場所、および説明が管理コンソールに表示されるため、制御プレーンに接続されている他のポッドからこのポッドを識別できます。

オプション	説明
名前	Horizon Cloud テナント環境でこのポッドを識別するためのわかりやすい名前を入力します。
データセンターの場所	<p>このポッドを使用する既存の場所を選択するか、[新規] をクリックして新しい場所を指定します。クラウドベースの管理コンソールでは、ポッドは指定した場所に従ってグループ化されて表示されます。</p> <p>[市区町村名] テキスト ボックスに、市区町村の名前を入力します。システムは自動的にバックエンドの地理参照テーブルにある、入力した文字に一致する世界の市区町村名表示するので、そのリストから市区町村を選択できます。</p> <p>注： システムのオートコンプリート リストから市区町村を選択する必要があります。現在、既知の問題により、ロケーション名はローカライズされていません。</p>
説明	オプション：このポッドの説明を入力します。

9 [保存] をクリックして、次のウィザード手順に進みます。

ウィザードの構成手順が表示されます。システムは、指定した Connection Server インスタンスへの接続をチェックし、最後の構成手順を完了します。次のスクリーンショットは、この手順の例です。



ポッドが Horizon Cloud 制御プレーンに正常に接続されたことをシステムが判断すると、正常な完了を示す画面に、構成後の管理タスクのためのいくつかのガイダンス テキストとアクション ボタンが表示されます。この画面には、アクティブ化されたクラウド ホスト型サービスの健全性ステータスも表示されます。灰色のダッシュアイコンは、サービスが非アクティブになっているため、健全性ステータスが表示されないことを示しています。

次のスクリーンショットは、正常に完了したことを示す画面の例です。

Cloud Connector のバージョン : 2.3.0.0-19616917

[ログのダウンロード](#) [ログアウト](#)

VMware Horizon Cloud Connector のセットアップ

[vCenter Server とネットワークの詳細の設定](#) [SNMP の構成](#) [SSH の構成](#) [再構成](#) [接続解除](#)

セットアップが完了しました。

Horizon Cloud Connector は正常に展開されました。

ポッド名: cs-crqzr
 ポッドの状態: 監視対象
 VMware Cloud がデプロイされました。 全般 ⓘ

Horizon サブスクリプション ライセンスのアクティベーションとライセンス期間の情報は、1 時間以内に Horizon Console の [製品のライセンスと使用状況] タブに表示されます。ライセンス情報が 4 時間以内に表示されない場合は、VMware のサポートにお問い合わせください。

次の手順:

- Horizon Cloud (cloud.horizon.vmware.com) にログインします
- 追加の My VMware ユーザーに Horizon Cloud Service 管理プレーンへの管理者権限を付与します
- ユーザーを管理しやすくするために Active Directory ドメインを登録します。管理者の追加、権限の付与、またはユーザーへの割り当てを行います

Horizon Cloud Connector の構成ステータス

ステータス	構成
✔	vCenter Server とネットワーク
⊖	SNMP - 80001adc01c0a8f38730263971 ⓘ
⊖	SSH

Cloud Connector の健全性 ✔

最新の更新 - 下午5:55:19 ⓘ

ステータス	コンポーネント	バージョン
⊖	Cloud Broker Client Service	
✔	Cloud Proxy Service	2.1
✔	Connection Server Monitoring Service	1.10.0-528(5413eab)
✔	Connection Server Proxy Service	2.0
✔	Connector Client Service	1.1
⊖	Edge Device	2.0
✔	Image Locality Service	1.0.0
✔	Keybox Service	2.1
⊖	View InfraModule	2.0
✔	vCenter Connectivity	2.0

注： 非アクティブの状態で常に表示されるコンポーネントが表示される場合があります。これらのコンポーネントは、今後のサービス リリースで使用される予定です。

Connection Server が vSphere インフラストラクチャに配置されている場合、[Horizon Cloud Connector vCenter Server の詳細] ウィンドウが自動的に表示される

Horizon Cloud Connector とそのペアリングされている Connection Server が、VMware SDDC または オンプレミスの vSphere インフラストラクチャにインストールされている場合、[Horizon Cloud Connector vCenter Server の詳細] ウィンドウが構成画面の前で自動的に開きます。

Horizon Cloud Connector と Connection Server がパブリック クラウド インフラストラクチャにネイティブでインストールされている場合（フェデレーション デプロイ タイプの場合など）、この機能は適用されません。

入力された値は、Horizon Cloud Connector 仮想アプライアンスの自動更新をサポートするためのものです。

このウィンドウを閉じるには、『管理ガイド』の [Horizon Cloud Connector 仮想アプライアンスの自動更新](#) の記事の説明に従って vCenter Server とネットワークの詳細を入力する必要があります。自動更新機能はポッドごとに有効にできるオプション機能ですが、これらの詳細の構成は必須です。

必須の情報を入力せずに [Horizon Cloud Connector vCenter Server の詳細] ウィンドウを閉じる場合、[vCenter Server とネットワークの詳細の設定] ボタンをクリックして詳細を入力するまで、警告メッセージが継続して表示されます。

次のスクリーンショットは、最初に表示されるウィンドウの例を示しています。

結果

この時点で、ペアリングのワークフローが完了します。ポッドをクラウド制御プレーンとペアリングしてから通常 30 分以内に、VMware はサブスクリプション ライセンスをアクティブ化します。VMware がサブスクリプション ライセンスをアクティブ化すると、ポッドの Web ベースの管理コンソールにポッドがサブスクリプション タイプのライセンスを使用していることを示すメッセージが表示されます。次のスクリーンショットは、図のサンプルです。

注目: 4 時間経過しても、ポッドの Web ベースの管理コンソールのライセンス領域に「ライセンス サービスに接続されませんでした」というメッセージが表示されない場合は、VMware の担当者にお問い合わせください。



次のステップ

この時点から、ポッドは Horizon Cloud と正常にペアリングされます。通常この時点から実行される Horizon Cloud Connector の管理およびメンテナンス タスクの詳細については、『管理ガイド』の [Horizon ポッドと Horizon Cloud のペアリング後に Horizon Cloud Connector で実行する一般的な管理およびメンテナンス タスクのトピック](#) を参照してください。

(Horizon Cloud Connector 2.0 以降) サービス レベルのフォルト トレランスをサポートするには、ワーカー ノードをデプロイします。 [Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector クラスタへのワーカー ノードの追加](#) を参照してください。

Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector クラスタへのワーカー ノードの追加

Horizon Cloud Connector のサービス レベルのフォルト トレランスをサポートするには、プライマリ ノードを含んでいるクラスタにワーカー ノードを追加して、デュアル ノード クラスタを作成します。ワーカー ノードは、Horizon Cloud Connector アプリケーション サービスのレプリカを含んでいます。

ワーカー ノードをクラスタに追加するには、まず vSphere Client を使用して、ワーカー ノードをポッドの vSphere 環境にデプロイします。次に、コマンドを実行して、プライマリ ノードを含んでいるクラスタにワーカー ノードを参加させます。

Horizon Cloud Connector のノード、クラスタ、およびフォルト トレランス機能の概要については、[Horizon Cloud Connector クラスタ、ノードレベルの高可用性、およびサービス レベルのフォルト トレランス](#)を参照してください。

注： このリリースでは、次のタイプのポッドとペアリングされたアプライアンスでのみ、デュアル ノード クラスタ、ノード レベルの高可用性、およびサービス レベルのフォルト トレランスがサポートされます。

- オンプレミスにデプロイされた Horizon ポッド
- オールイン SDDC アーキテクチャの VMware Cloud on AWS にデプロイされた Horizon ポッド

他のすべての環境にデプロイされた Horizon ポッドは、プライマリ ノードのみで構成される単一ノード クラスタをサポートし、ノード レベルの高可用性およびサービス レベルのフォルト トレランスはサポートしません。

前提条件

次の前提条件のタスクを完了したことを確認します。

- ポッドの vSphere 環境に Horizon Cloud Connector をダウンロードしてデプロイするの記載通りに、クラスタのプライマリ ノードをデプロイし、Horizon Cloud Connector を Horizon ポッドとペアリングします。
- Horizon Cloud と Horizon Cloud Connector 仮想アプライアンスとの間での継続的な運用のための、DNS、ポート、およびプロトコル要件を満たしていることを確認します。

手順

- 1 ワーカー ノードをデプロイするには、ポッドの vSphere 環境に Horizon Cloud Connector をダウンロードしてデプロイするの記載通りに、Horizon Cloud Connector アプライアンスを OVF テンプレートとしてデプロイする一般的な手順を実行します。次のオプションを確実に構成してください。
 - [テンプレートのカスタマイズ] ウィザード ページで、[ワーカー ノード] オプションを有効にします。デフォルトでは、[ワーカー ノード] オプションは無効になっており、プライマリ ノードのデプロイになります。
 - ワーカー ノードの ccadmin ユーザーに対する SSH パブリック キーを構成します。この手順の後半で必要なコマンドを実行するには、ワーカー ノードへの SSH アクセスを有効にする必要があります。
- 2 デプロイが完了したら、vSphere Client を使用してワーカー ノード仮想マシンをパワーオンします。青いコンソール画面で、Horizon Cloud Connector 構成ポータルを起動するためのノードの URL を書き留めます。
- 3 ccadmin アカウントのワーカー ノードへの SSH アクセスを有効にします。[コマンドライン インターフェイスの使用による Horizon Cloud Connector への SSH アクセスの有効化](#)を参照してください。
- 4 クラスタ内のプライマリ ノードへの SSH セッションを開き、次のコマンドを実行します。ここでの `<WORKER_IP>` は、先ほど取得したワーカー ノードの IP アドレスです。

```
/opt/vmware/sbin/primary-cluster-config.sh -as <WORKER_IP>
```

- 5 ワーカー ノードへの接続を続行するかを確認するプロンプトが表示されたら、**yes** と入力します。

- 6 中断されることなくコマンドを実行できるようにします。コマンド出力の最後で、次の例のような行を探します。ここでの `<PRIMARY_IP>` は、プライマリ ノード仮想マシンの IP アドレスです。

```
Please run the following command on worker node to join the cluster:  
/opt/vmware/sbin/worker-cluster-config.sh -a <PRIMARY_IP> <TOKEN 1> <TOKEN 2>
```

この cluster-join コマンドを書き留めます。

- 7 ワーカー ノードへの SSH セッションを開き、前の手順で取得した cluster-join コマンドを実行します。

```
/opt/vmware/sbin/worker-cluster-config.sh -a <PRIMARY_IP> <TOKEN 1> <TOKEN 2>
```

- 8 ワーカー ノードをクラスタに参加させた後、プライマリ ノード仮想マシンで次のコマンドを実行して、新しいクラスタ メンバーシップを確認します。

```
kubectl get nodes -o wide
```

コマンドによって返される出力で、プライマリ ノードとワーカー ノードの両方が、IP アドレスで識別された、クラスタの登録済みメンバーとして表示されていることを確認します。

第 1 世代 Horizon Cloud on Microsoft Azure のデプロイ - 主な特性

6

このドキュメント ページでは、第 1 世代 Horizon Cloud on Microsoft Azure のデプロイの主な特性について説明します。これらの環境は、Horizon Cloud ポッドとも呼ばれます。

重要: この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

簡単な紹介

Horizon Cloud ポッドは、Horizon Cloud ポッド マネージャ テクノロジーに基づいています。このポッド マネージャ テクノロジーは Microsoft Azure サブスクリプションでのみ実行され、VMware SDDC を必要としません。

Horizon Cloud on Microsoft Azure 環境は、Horizon Connection Server ソフトウェア コンポーネントを含む他の Horizon 環境タイプとは異なります。

以下も参照してください。

- [第 1 世代テナント - Horizon Cloud のポッドのデプロイとオンボーディング](#): テナント アカウントが新しく作成されたときの操作の概要、最初のポッドをデプロイする前の Day-0 タスク、ポッドをオンボーディングする Day-1 タスクについて説明します。
- [第 1 世代テナント - 事前検証のための簡素化された Horizon Cloud Service on Microsoft Azure ポッド環境の使用開始の図](#)。

デプロイ

第 1 世代 Horizon Cloud on Microsoft Azure をデプロイするときは、自動化されたポッド デプロイ ウィザードを使用してポッド マネージャ ベースのポッドをデプロイします。Microsoft Azure でクラウド キャパシティのサブスクリプションを取得し、そのサブスクリプション情報を用いてクラウド キャパシティを Horizon Cloud テナントとペアリングさせる必要があります。

このウィザードでは、必要な VMware ソフトウェア コンポーネントを Microsoft Azure クラウド サブスクリプションにデプロイして、環境を作成します。

デプロイした VMware ソフトウェアがポッドというエンティティを作成し、適切に構成します。このエンティティが制御プレーンとペアリングされます。

このポッドがデプロイされたら、制御プレーンを使用して VDI デスクトップと RDSH をプロビジョニングして、デスクトップとリモート アプリケーションへのアクセスをエンド ユーザーに付与します。

Microsoft Azure に Horizon Cloud によってデプロイされたポッドには、Microsoft Azure クラウド内に物理的な配置場所があります。ポッド デプロイ ウィザードで、Microsoft Azure サブスクリプションで使用可能なリージョンに基づいてポッドの配置場所を選択します。選択したリージョンでポッドが使用する既存の仮想ネットワーク (VNet) も選択します。ポッドで外部ゲートウェイ構成をデプロイするオプションがあります。このオプションでは、その外部ゲートウェイのリソースをポッドと同じ VNet にデプロイするか、ポッドの VNet とピアリングされる別の VNet にデプロイします。

注： ポッドの VNet (およびその構成オプションを使用する場合は外部ゲートウェイ VNet) を使用して、Microsoft Azure 環境を事前に構成します。ポッドと外部ゲートウェイの構成に必要なサブネットを事前に作成するか、デプロイ中にポッド デプロイヤーによってサブネットを作成することができます。事前にサブネットを作成しない場合は、ポッド デプロイヤーが環境内で必要な仮想マシンとリソースをデプロイすると同時にサブネットを作成します。ポッド デプロイヤーによって必要なサブネットを作成するよう選択した場合、デプロイ ウィザードを開始する前に、ポッドのサブネットに使用する IP アドレス空間を把握しておく必要があります。サブネットを事前に作成することを選択した場合は、デプロイ プロセスを開始する前にサブネットが特定の要件を満たしていることを確認する必要があります。事前にサブネットを作成するときの要件の詳細については、[第 1 世代テナント - ポッドのデプロイの前に、Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成する](#)および[第 1 世代テナント - Microsoft Azure で Horizon Cloud ポッド用に既存のサブネットを使用する場合を参照してください](#)。

複数のポッドを Microsoft Azure にデプロイし、同じ管理コンソールですべてのポッドを一元管理できます。最初のポッドの後にデプロイするポッドは、最初のポッドと同じ VNet を再利用することも、別の VNet を使用することもできます。また、各ポッドは別の Microsoft Azure リージョンに配置することもできます。この場合は、各リージョンの VNet を使用します。

重要： Microsoft Azure では、このポッドはテナントではありません。このポッドの特性は、テナントを定義する特性や、ユーザーがテナントに対して期待する特性とまったく同じものにはなり得ません。たとえば、テナントが Active Directory ドメインに対して 1 対 1 でマッピングされていて、他のテナントから分離されている場合でも、同じ Horizon Cloud 顧客アカウント レコードを使用して展開されている Microsoft Azure 内のすべての Horizon Cloud ポッドは同じ Active Directory サーバにアクセスできる必要があるとともに、DNS 構成でこれらのすべての Active Directory ドメインを解決する必要があります。

マルチ テナント状態を実行するには、複数の Horizon Cloud 顧客アカウント レコードを設定します。Horizon Cloud Service を使用するために VMware で登録を行ったときに作成され、VMware Customer Connect 認証情報に関連付けられる Horizon Cloud 顧客アカウント レコードは、よりテナントに近いものになります。Horizon Cloud 顧客アカウント レコードは、他の Horizon Cloud 顧客アカウント レコードから分離されます。1 つの顧客アカウント レコードは複数のポッドにマッピングされます。また、誰かが管理コンソールにログインするためにその顧客アカウント レコードに関連付けられたいずれかのアカウント認証情報を使用するときに、その顧客アカウント レコードにマッピングされているすべてのポッドがコンソールで反映されます。

ポッドのデプロイ プロセスで、一連のリソース グループが Microsoft Azure キャパシティに自動的に作成されます。リソース グループは、環境が必要として作成する次のような資産の整理に使用します。

- ポッド マネージャ インスタンスの仮想マシン。
- Unified Access Gateway インスタンスとそのロード バランサの仮想マシン

- ポッドの VNet とは別の VNet に外部ゲートウェイ構成をデプロイする場合の、その構成のコネクタ仮想マシンの仮想マシン
- RDSH 対応ゴールド イメージの仮想マシン
- VDI デスクトップ ゴールド イメージの仮想マシン
- ゴールド イメージから作成された割り当て可能な（公開済み、シールド済み）イメージの仮想マシン
- RDSH デスクトップとリモート アプリケーションを提供する RDSH ファームの仮想マシン
- VDI デスクトップの仮想マシン
- ネットワーク インターフェイス、IP アドレス、ディスク、キー コンテナ、Microsoft Azure Database for PostgreSQL サーバ リソースなど、サポートされている操作のために仮想マシンおよび環境で必要となる追加のアセット、およびそれらに関連するさまざまなアイテム。ポッドのデプロイ プロセスは、デプロイ ウィザードで指定する値を使用して、必要な仮想サブネットを作成することもできます。

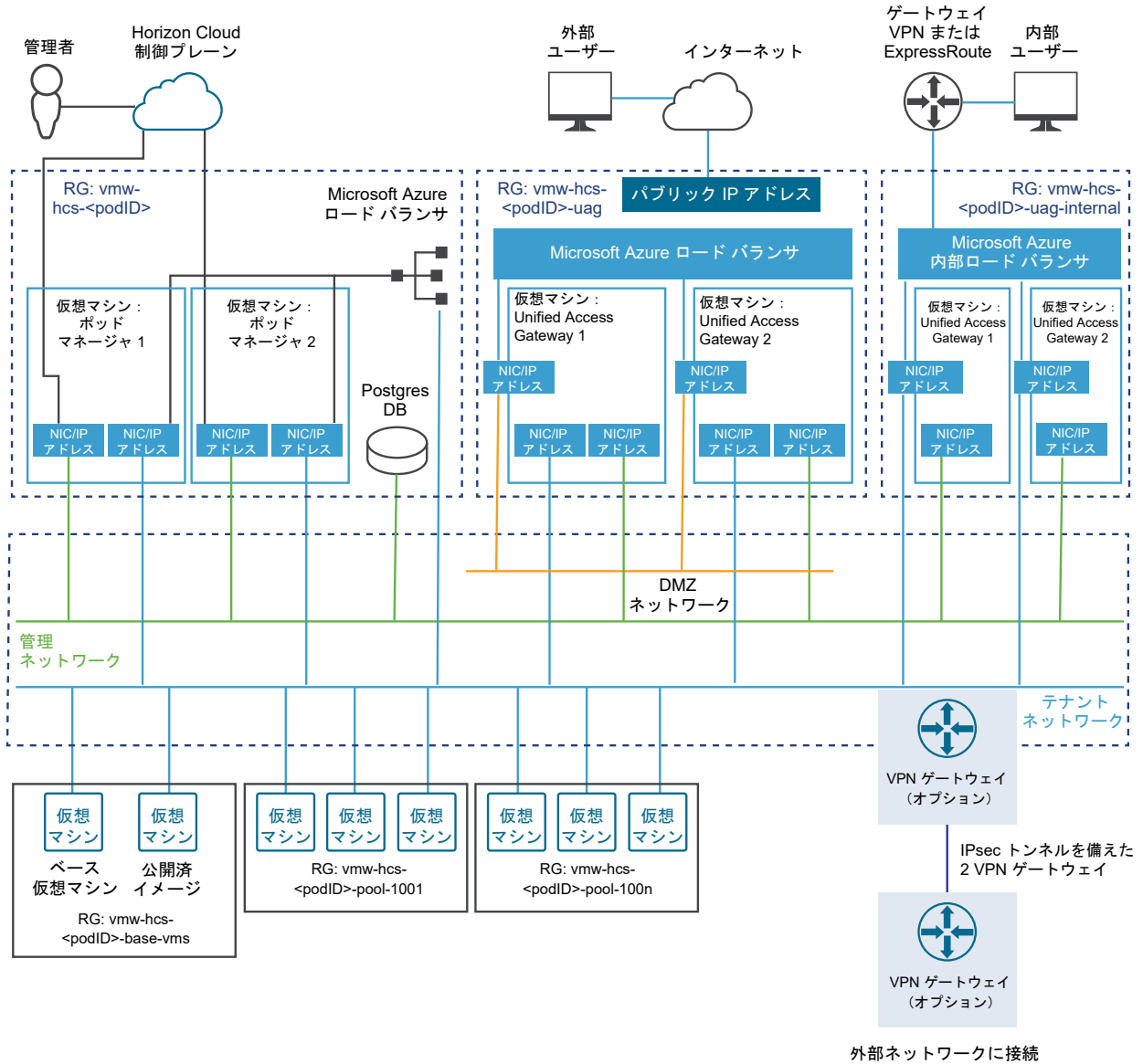
次の図は、外部と内部の両方のタイプのゲートウェイ構成があり、外部ゲートウェイがポッド自身と同じ VNet に存在するデプロイされたポッドを示しています。この図では、RG はリソース グループを意味します。

外部ゲートウェイ構成の Unified Access Gateway インスタンスは、非武装地帯 (DMZ) ネットワーク上に NIC があります。外部ゲートウェイ構成を使用すると、インターネットや企業ネットワーク外部のエンド ユーザーは、その構成を介してポッドがプロビジョニングされた仮想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。内部ゲートウェイ構成を使用すると、イントラネットや企業ネットワーク内部のエンド ユーザーは、そのゲートウェイを介してポッドがプロビジョニングされた仮想デスクトップおよびアプリケーションとの間で信頼された接続を確立できます。

ポッド デプロイヤーは、両方の構成を事前に使用してポッドをデプロイするオプションを提供します。または、ポッドを1つのゲートウェイ構成のみでデプロイするか、まったく構成せずにデプロイし、デプロイされたポッドを後で編集して、選択されていないゲートウェイ構成を追加できます。どちらのタイプも使用せずに最初にポッドをデプロイして、後で追加することもできます。

システムは、高可用性でポッドをデプロイします。デフォルトでは、2 台のポッド マネージャ仮想マシンがあります。

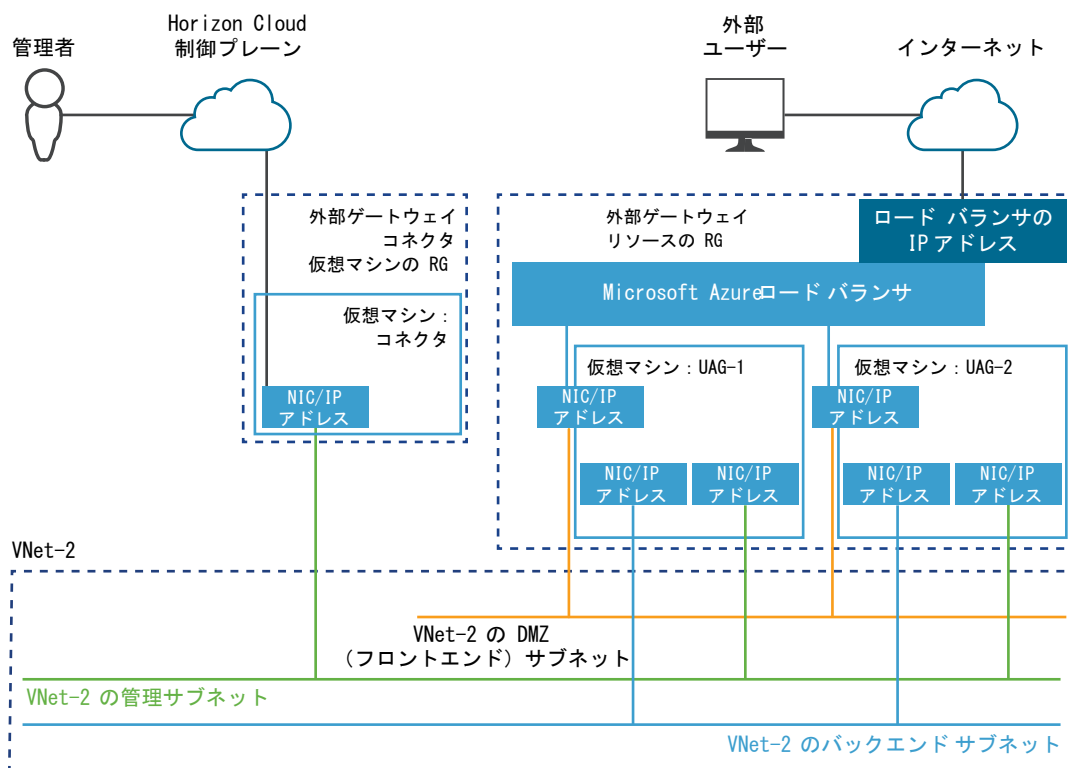
図 6-1. ポッドが外部および内部ゲートウェイの両方で構成された Horizon クラウド ポッド アーキテクチャの図 (外部ゲートウェイはポッドと同じ VNet にデプロイされた; 外部ゲートウェイ仮想マシンに 3 つの NIC、内部ゲートウェイ仮想マシンに 2 つの NIC がある; 外部ゲートウェイのロード バランサに対してパブリック IP アドレスが有効)



次の図は、外部ゲートウェイをポッドの VNet とは別の専用の VNet に配置するオプションを選択したときにデプロイされるリソースを示しています。2つの VNet をピアリングする必要があります。この図は、ポッドで使用されるものとは異なる Microsoft Azure サブスクリプションを使用して外部ゲートウェイのリソースをデプロイするオプションを選択した場合にも適用されます。VNet は複数のサブスクリプションにまたがることはできないため、外部ゲートウェイを専用のサブスクリプションにデプロイすることは、外部ゲートウェイを専用の VNet に配置するように選択することの一部です。

ヒント: 外部ゲートウェイ構成を専用の VNet にデプロイすると、これらの Horizon Cloud ポッドを、Microsoft Azure のハブ - スポーク ネットワーク トポロジを使用する複雑な Microsoft Azure 環境にデプロイできます。

図 6-2. 外部ゲートウェイがポッドの VNet とは別の専用の VNet にデプロイされている場合の外部ゲートウェイのアーキテクチャ要素の図



Microsoft Azure の専門用語とリファレンス

VMware Horizon Cloud Service on Microsoft Azure 製品のドキュメントでは、必要に応じて VMware Horizon Cloud Service on Microsoft Azure ワークフローの説明とタスクの手順に Microsoft Azure の専門用語が使用されています。Microsoft Azure の専門用語に慣れていない場合は、以下の Microsoft Azure 製品ドキュメントに関連するリファレンスを参照してください。

注: 以下の表記に含まれる大文字と小文字の区別およびスペルは、すべて Microsoft Azure ドキュメント自身のリンク先の記事に合わせてあります。

有用な Microsoft Azure のリファレンス	説明
Microsoft Azure glossary: A dictionary of cloud terminology on the Azure platform (Microsoft Azure 用語集 : Azure プラットフォームに関するクラウド用語の辞書)	<p>この用語集には、たとえばロード バランサ、リージョン、リソース グループ、サブスクリプション、仮想マシン、仮想ネットワーク (vnet) など、Microsoft Azure クラウドのコンテキストで使用される用語が含まれています。</p> <p>注: Microsoft Azure 用語集には「サービス プリンシパル」という用語は含まれていません。サービス プリンシパルは、アプリケーション登録が Microsoft Azure で作成されるときに Microsoft Azure で自動的に作成されるリソースであるためです。Microsoft Azure サブスクリプションでアプリケーション登録を作成する理由は、Microsoft Azure キャパシティを使用するために Horizon Cloud をアプリケーションとして承認することです。アプリケーション登録とそのコンパニオン サービス プリンシパルによって、アプリケーションとして動作する Horizon Cloud クラウド サービスは Microsoft Azure サブスクリプションのリソースにアクセスできるようになります。Microsoft Azure のリソースにアクセスできるアプリケーションとサービス プリンシパルについては、以下のリファレンスを参照してください。</p>
Use portal to create an Azure Active Directory application and service principal that can access resources (ポータルを利用してリソースにアクセスできる Azure Active Directory アプリケーションとサービス プリンシパルを作成する)	<p>この記事では、Microsoft Azure クラウドのアプリケーションとサービス プリンシパルの関係について説明しています。</p>
Azure Resource Manager overview (Azure Resource Manager の概要)	<p>この記事では、Microsoft Azure のリソース、リソース グループ、およびリソース マネージャの関係について説明しています。</p>
Azure VNet	<p>この記事では、Microsoft Azure の Azure 仮想ネットワーク (VNet) サービスについて説明しています。Azure Virtual Network FAQs (Azure 仮想ネットワークに関する FAQ) も参照してください。</p>
Azure VNet Peering (Azure VNet ピアリング)	<p>この記事では、Microsoft Azure での仮想ネットワーク ピアリングについて説明しています。</p>
Azure のハブ - スポーク ネットワーク トポロジ	<p>この記事では、Microsoft Azure でのハブ - スポーク ネットワーク トポロジについて説明しています。</p>
Microsoft Azure ExpressRoute の概要	<p>この記事では、Microsoft Azure ExpressRoute について、およびオンプレミス ネットワーク、Microsoft Azure、および Horizon Cloud ポッド間の接続を確立するために Microsoft Azure ExpressRoute を使用方法について説明します。</p>
VPN ゲートウェイについて VPN ゲートウェイの計画および設計 Azure ポータルでのサイト間の接続の作成	<p>これらの記事では、Microsoft Azure で VPN を構成する方法について説明します。</p>
Azure Load Balancer の概要	<p>この記事では、ポッド用にデプロイされた Azure ロード バランサについて、すなわちポッド マネージャ仮想マシンのロード バランサとゲートウェイ構成のロード バランサについて説明します。</p>
Azure Database for PostgreSQL の概要	<p>この記事では、Microsoft Azure Database for PostgreSQL サービスについて説明します。</p>
Azure 仮想デスクトップの概要	<p>この記事では、Microsoft Azure 仮想デスクトップについて、および Microsoft Windows 10 Enterprise マルチセッションおよび拡張セキュリティ更新プログラムが適用された Microsoft Windows 7 Enterprise との関係について説明します。Horizon Cloud テナント アカウントに Microsoft Azure 仮想デスクトップを拡張する Horizon Cloud Service on Microsoft Azure の構成がある場合、Microsoft Windows 10 Enterprise マルチセッションおよび Microsoft Windows 7 Enterprise を Microsoft Azure にデプロイされたポッドで使用するためのサポートが提供されます。</p>

その他の VMware リソース

次のリソースは、サービスに関する技術的な詳細情報を提供します。

その他の VMware の技術的なリソース	説明
要件チェックリスト - 第1世代 Horizon Cloud on Microsoft Azure のデプロイ	このチェックリストを使用して、ポッドのデプロイ プロセスを開始する前に取得および構成する必要があるアセットについて確認します。
Tech Zone - ネットワーク設計 - Horizon Cloud on Microsoft Azure - 第1世代アーキテクチャ	「VMware Digital Workspace Tech Zone の Horizon Cloud on Microsoft Azure - 第1世代アーキテクチャ」のこのネットワーク設計セクションでは、これらの第1世代のデプロイのネットワーク設計について説明します。
Horizon Cloud Service on Microsoft Azure のセキュリティについての考慮事項	この記事では、環境のセキュリティ詳細に関する情報と、保存されたデータのタイプに関する情報が提供されます。
Tech Zone - VMware Horizon Cloud on Azure での電源管理	この記事では、デスクトップとリモート アプリケーションのサイズを適切に設定し、第1世代の Horizon Cloud on Microsoft Azure デプロイでワークロードを効率的に管理するのに役立つ機能について説明します。

次のトピックを参照してください。

- [第1世代テナント - 事前検証のための簡素化された Horizon Cloud Service on Microsoft Azure ポッド環境の使用開始](#)
- [第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - 概要レベルの手順](#)
- [第1世代テナント - 第1世代 Horizon Cloud ポッドを Microsoft Azure にデプロイする前の準備](#)
- [第1世代テナント - Microsoft Azure へのポッドの自動デプロイを実行するための第1世代 Horizon Universal Console の使用](#)
- [第1世代テナント - 第1世代 Horizon Cloud ポッドのデプロイまたは初めてのドメイン バインドで問題が発生した場合のトラブルシューティング](#)

第1世代テナント - 事前検証のための簡素化された Horizon Cloud Service on Microsoft Azure ポッド環境の使用開始

このページでは、第1世代 Horizon Cloud Service on Microsoft Azure 環境の簡素化された確認作業で使用するポッドの材料とステップバイステップのレシピについて説明します。

重要: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。KB-92424 で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。



簡単な紹介

このページの目的は、事前検証、ホーム ラボ、パイロット、トライアル環境など、確認目的の環境に適した、スムーズで簡素化されたポッド環境を作成するためのステップバイステップのレシピを提供することです。

そのような環境は、確認作業が終了次第削除されると想定されます。

このレシピは、単一のサブスクリプション、1つの基本的な VNet、およびローカルの PoC Active Directory 仮想マシンで使用するためのもので、その他は対象外です。

詳しくは、VMware プロフェッショナル サービスにお問い合わせください。VMware プロフェッショナル サービスは、[デリバリー スペシャリスト プログラム](#)を通じて、Horizon Cloud Service on Microsoft Azure 環境の特定のニーズに合わせた実装とオンボーディングの「設計-構築」アプローチを提供します。

簡素化された初期展開のための材料

このページに記載されているステップバイステップのレシピは、以下の最小限必要な材料を使用して、大学卒業生によって証明されました。

材料

- 業界標準のクレジットカードでバックアップされる1つの従量課金制の Azure サブスクリプション。
- そのサブスクリプション内の West US 3 Azure リージョンの場所。
- そのサブスクリプション内の、512 個のアドレス (10.0.0.0/23) 用に構成されている1つの基本的な単一 VNet。
- Active Directory の登録フローを満たすための、その VNet 上のローカル PoC Active Directory 仮想マシン。
- Azure API 呼び出しを行うために Contributor に設定したアプリケーション登録には、Azure の組み込み Horizon Cloud Service ロールを使用します。

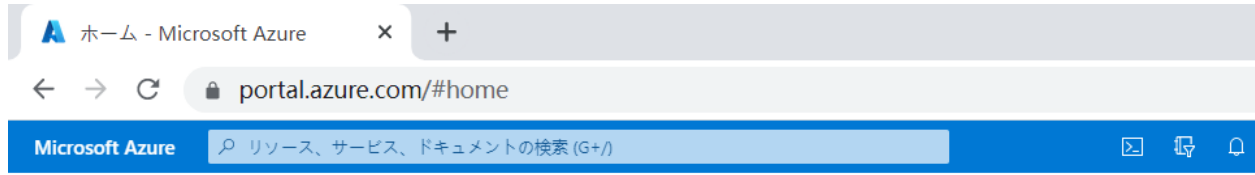
このレシピでは、West US 3 リージョンが使用されました。これは、本書の執筆時点では、West US 3 リージョンが PoC 環境の2つの目標を満たしていたためです。つまり、このリージョンは、対象の VDI エンドユーザーに地理的に最も近く、また、環境の [Azure Managed PostgreSQL] サービスおよび [仮想マシン ファミリー vCPU] の従量課金制のサブスクリプションを使用するという要件を満たしていました。

簡素化

- ゲートウェイ機能は展開されたポッドに [ポッドを編集] を使用して後から追加できるため、最初はゲートウェイ構成のトグルをオフにして展開することで、レシピを簡素化しました。
これにより、ゲートウェイ構成に必要な SSL 証明書の取得と並行して、初期展開を正常に完了できます。
- 割り当てチェックの手順を簡素化するために、Windows 11 オペレーティング システム (OS) を使用するゴールド イメージに対してシステムが必要とする仮想マシン ファミリーの割り当てチェックを省略しています。Windows 11 のゴールド イメージには、Windows 10 のイメージとは異なる仮想マシン モデルが必要です。簡素化のため、割り当てチェックでは Windows 11 の使用事例を省略しています。

Azure ポータルを使用する場合

Microsoft Azure の準備に関連するアクティビティは、Azure ポータルに依存しています。



レシピの Azure ポータルに関連する部分については、以下の点に注意してください。

- Microsoft は、時間の経過とともにインターフェイスを更新することがあります。
- Microsoft はまた、アカウント アクセスとポータルの設定に応じて、すべてのユーザーのポータル エクスペリエンスをパーソナライズします。
- Microsoft の変更に合わせて、このページのスクリーンショットと Azure ポータルに表示されるラベルと名前はできるだけ最新の状態に保つようになっています。
- このページのスクリーンショット、ラベルと名前は、Microsoft が更新をロールアウトしてポータル エクスペリエンスをパーソナライズする方法によっては、ある時点で Azure ポータルに表示されるものと完全には一致しない場合があります。

この PoC ページでは、「ペイン」という用語を使用して Azure ポータルの領域を表しています。

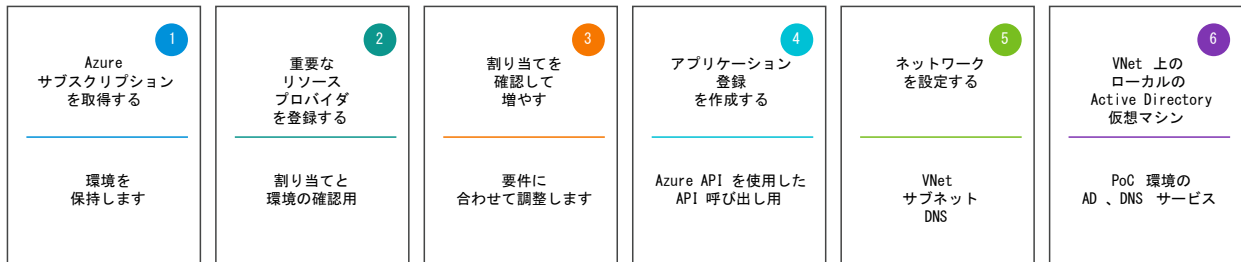
Microsoft Azure クラウドの準備



この PoC レシピの場合、[ポッドの追加] ウィザードを実行する前に、PoC の Horizon Cloud on Microsoft Azure 環境に Microsoft Azure サブスクリプションを準備する必要があります。

これらのセクションに含まれているスクリーンショットは、このページの手順を証明するために使用した従量課金制のサブスクリプションの内容を示しています。

Microsoft によって表示内容やアクセスの対象がパーソナライズされるため、実際の Azure 環境で表示される詳細は異なります。



1 Azure サブスクリプションを取得する

PoC の最初のアクティビティは、PoC 環境の Azure サブスクリプションの取得です。

定義上は、Horizon Cloud Service on Microsoft Azure 環境は、提供する Microsoft Azure サブスクリプションに存在します。

本書の執筆時点では、Microsoft は、Azure サブスクリプションの主なタイプとして、無償タイプ、従量課金タイプ、エンタープライズタイプのサブスクリプションを提供しています。

現在、従量課金タイプとエンタープライズタイプのサブスクリプションは、Horizon Cloud on Microsoft Azure 環境に必要な割り当てレベルをサポートするものです。

Microsoft は通常、無料タイプのアカウントの割り当てレベルを増やすことを許可しません。したがって、Horizon Cloud 環境をサポートするための要件を満たす無料アカウントを作成することはできません。

PoC 環境では、次のアプローチの使用を検討します。

- 1 サインアップから 30 日間 \$200 の Azure クレジットを使用できる無料の Azure アカウントにサインアップします。
- 2 その無料の Azure アカウントを従量課金アカウントにすぐに変更します。\$200 の Azure クレジットが、30 日間従量課金アカウントで使用可能になります。
- 3 Horizon ユニバーサル サブスクリプション ライセンスの 60 日間の試用版にサインアップします（まだ Horizon Cloud テナントを使用していない場合は必須）。
- 4 VMware が Horizon Cloud テナントを構成している間、Azure の準備項目 2 ~ 6 を続行します。
- 5 「Horizon Cloud へようこそ」E メールを受信したら、ログインして [ポッドの追加] ウィザードを実行します。

これにより、Horizon Cloud テナント アカウントがログインして [ポッドの追加] ウィザードを実行する準備ができ次第、Azure サブスクリプションの準備が完了します。

残りの 5 つの準備アクティビティを実行できる Azure サブスクリプションを取得したら、Azure ポータルにログインしてそれらの準備を開始できます。

残りの Microsoft Azure 準備アクティビティ (2 ~ 5) はすべて、Azure サブスクリプション内の Azure ポータルを使用して実行されます。サブスクリプションの認証情報を使用して、Azure ポータルにログインします。

2 重要なリソース プロバイダを登録する

次に、PoC ポッド環境に必要なすべての重要なリソース プロバイダを登録します。

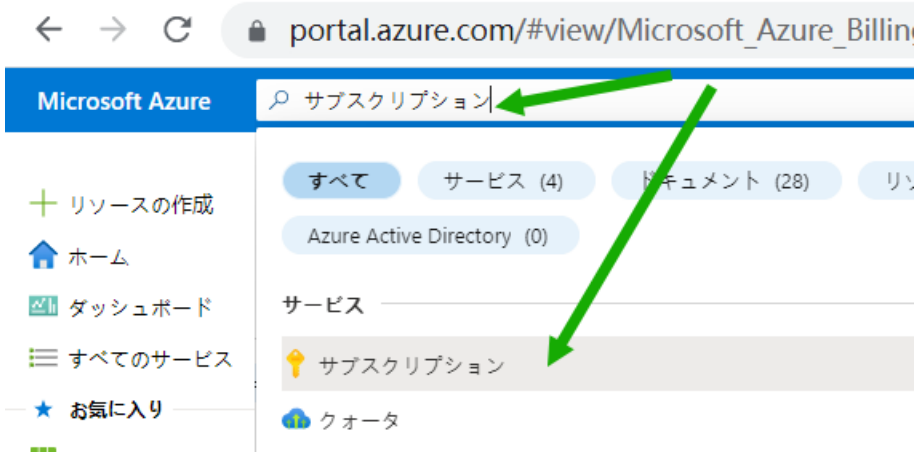
特定の Azure リージョンの場所で必要なアイテムの可用性を確認する次の PoC アクティビティの前に、Azure ポータルに正しいデータが表示されるようにするには、Microsoft.DBforPostgreSQL、Microsoft.Sql、および Microsoft.Compute リソース プロバイダが Registered 状態になっている必要があります。

[ポッドの追加] ウィザードに必要なすべての追加リソース プロバイダをここで登録することで、以降の時間を節約できます。[ポッドの追加] ウィザードの実行を開始したときに、[ポッドの追加] ウィザードに必要なものはすでに登録済みになります。

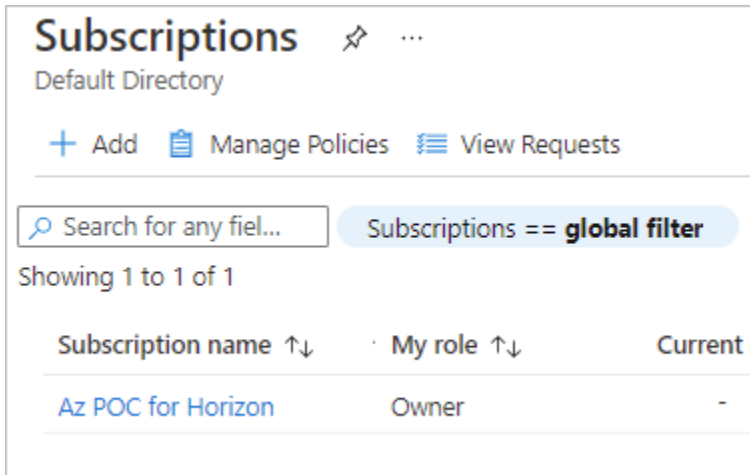
Azure ポータルでは、各リソース プロバイダが Unregistered から Registered 状態に切り替わるまでに最大で 10 分かかる場合があります。

手順

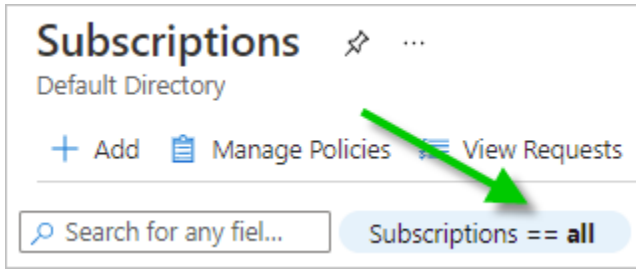
- 1 Azure の認証情報を使用して、Azure ポータル (<https://portal.azure.com>) にログインします。
- 2 ポータルの上部の検索バーで、「**subscriptions**」と入力すると、[サブスクリプション] アイコンが表示されます。[サブスクリプション] アイコンをクリックします。



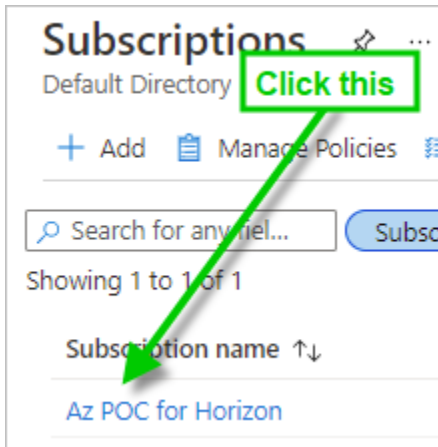
[サブスクリプション] をクリックすると、ポータルに [サブスクリプション] ペインが表示され、ログイン認証情報に関連付けられているサブスクリプションが一覧表示されます。



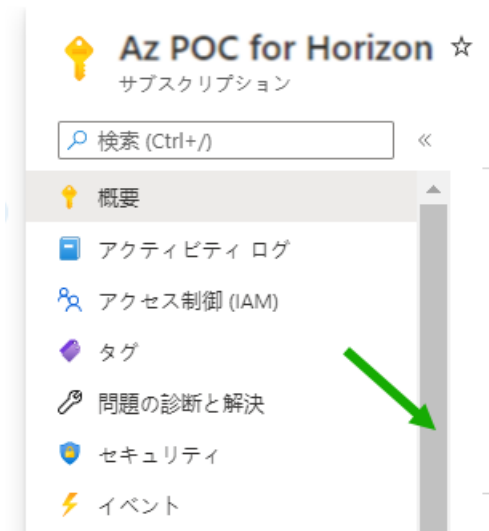
この PoC に使用するために取得したサブスクリプションの名前が表示されない場合は、[サブスクリプション == グローバル フィルタ] をクリックします。次に表示されるボックスで、[選択したサブスクリプションのみを表示] ボックスをクリアし、[適用] をクリックして、フィルタに [サブスクリプション == すべて] と表示されるようにします。



- 3 この PoC に使用するサブスクリプションをクリックします。



- 4 サブスクリプションのペインを下にスクロールして、[リソース プロバイダ] を見つけます。



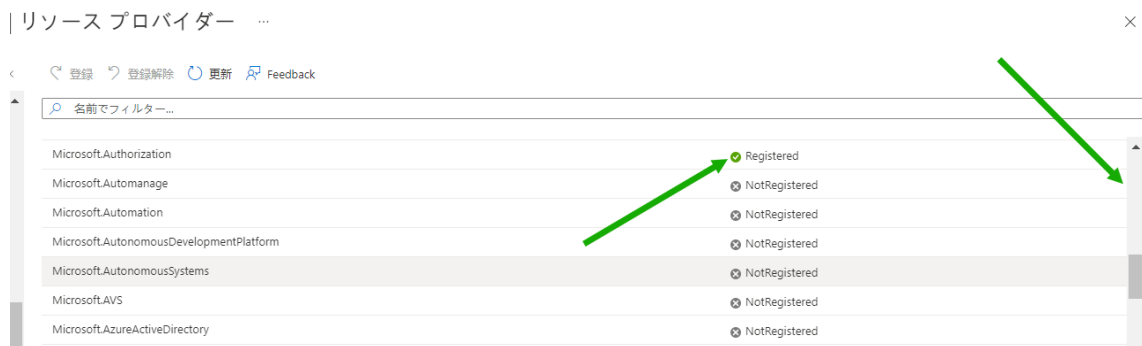


- 5 [リソース プロバイダ] ペインを開く [リソース プロバイダ] をクリックします。



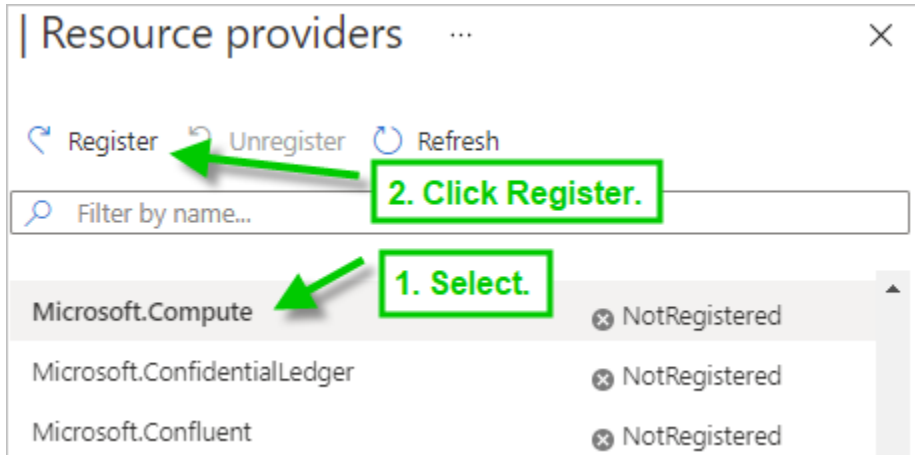
- 6 次の表の重要なリソース プロバイダのそれぞれについて、[リソース プロバイダ] ペインをスクロールし、そのリソース プロバイダの横に Registered が表示されているかどうかを確認します。

次のスクリーンショットは、Registered 状態を確認できる場所を示しています。



Microsoft Azure の標準動作により、新規の Azure サブスクリプションでは、一部のリソース プロバイダにはすでに Registered 状態が表示されます。たとえば、新しい Azure サブスクリプションには通常 Registered 状態の Microsoft.MarketplaceOrdering があります。これは、Azure は、Azure サブスクリプションを持つすべてのユーザーが Azure Marketplace を使用することを想定しているためです。

- これらの重要なリソース プロバイダの1つについて、NotRegistered の行に何かが表示された場合は、それを選択し、ペインの上部にある [登録] ボタンをクリックして Registered 状態に移行します。



[登録] をクリックすると、次のスクリーンショットに示すように、ペインに Registering が表示されます。



登録プロセスが完了しても、ポータル の [リソース プロバイダ] ペインは自動的に更新されないことに注意してください。最新の状態を表示するには、[更新] をクリックする必要があります。各リソース プロバイダごとに、状態が Registering から Registered に変更されるまでに最大 10 分かかる場合があります。

- 次の表のリソース プロバイダの確認と登録の手順を繰り返し、サブスクリプションの [リソース プロバイダ] ペインですべての状態が Registered になるようにします。

表 6-1. PoC の重要なリソース プロバイダ

リソース プロバイダ
Microsoft.Authorization
Microsoft.Compute
Microsoft.DBforPostgreSQL
microsoft.insights
Microsoft.KeyVault
Microsoft.MarketplaceOrdering
Microsoft.Network

表 6-1. PoC の重要なリソース プロバイダ (続き)

リソース プロバイダ
Microsoft.ResourceGraph
Microsoft.ResourceHealth
Microsoft.Resources
Microsoft.Security
Microsoft.Sql
Microsoft.Storage

3 可用性と割り当ての制限を確認し、必要に応じて増やす

Horizon Cloud on Microsoft Azure 環境では、環境を配置する特定の Azure リージョンの場所を決定します。低遅延を実現するため、通常は、対象となる VDI エンド ユーザーに地理的に最も近い Azure の場所に Horizon Cloud on Microsoft Azure 環境を配置します。

ただし、Microsoft はいつでも特定のリージョンの場所で特定の Azure サービスと割り当てを制限できるため、PoC 環境で使用することを検討する候補の場所の短いリストを用意することが重要です。

例として、従量課金制のサブスクリプションで France Central の [Standard Dv3 ファミリ vCPU] の可用性を確認したときに作成した次のスクリーンショットを参照してください。次のスクリーンショットは、この主要な仮想マシン ファミリが Microsoft Azure のこのリージョンでサブスクリプションに使用できない状況を示しています。

The screenshot displays a table of Azure regions with their respective availability for Standard Dv3 Family vCPUs. All regions shown (Central US, East Asia, East US, East US 2, and France Central) show 0% availability (0 of 10). A red arrow points to the 'France Central' row, and a green arrow points to the 'Microsoft.Compute' service name in the left sidebar.

Region	Availability
Central US	0% 0 of 10
East Asia	0% 0 of 10
East US	0% 0 of 10
East US 2	0% 0 of 10
France Central	0% 0 of 10

ベスト プラクティスのレシピ

- 1 短いリストにある各候補リージョンについて、Horizon Cloud on Microsoft Azure 環境に必要な Azure Database for PostgreSQL サービスと特定の仮想マシン ファミリの可用性を確認します。
- 2 これらのリージョンの1つが PostgreSQL データベースと仮想マシン ファミリの両方の可用性を満たしていることを確認したら、そのリージョンを、この PoC 環境のリージョンにします。

- 3 このリージョンの [仮想マシン ファミリ vCPU] と [合計リージョン vCPU] を十分に増やして、最初のポッド、およびゲートウェイの追加と、いくつかのゴールド イメージ、デスクトップ プール、およびマルチセッション ファームの作成という Day-2 の項目の両方に対応できるようにします。

表 6-2. そのレシピについて、サブスクリプション内の候補の場所でこれらの項目の作成が許可されていることを確認します。

項目	用途
[Azure Database for PostgreSQL] - 第 5 世代、メモリ最適化、2 個の vCore、10 GB ストレージ。	ポッド自身
[Standard Dv3 ファミリ vCPU] - 10 個の vCPU	ポッドの管理仮想マシン用に 8 個の vCPU、および 1 つの RDS ゴールド イメージ (デプロイ後に追加されるイメージ) 用に 2 個の vCPU
[Standard DSv2 ファミリ vCPU] - 4 個の vCPU	1 つの単一セッション Windows 10 ゴールド イメージ用に 2 個の vCPU、1 つの Windows 10 Enterprise マルチセッション ゴールド イメージ用に 2 個の vCPU。(これらのイメージは、システムの自動化された [Marketplace からの仮想マシンのインポート] ウィザードを使用して作成されます。)
[Standard Av2 ファミリ vCPU] - 9 個の vCPU	ポッドの外部ゲートウェイ構成 (デプロイ後に追加されたゲートウェイ) には 8 個の vCPU が必要です。次に、PoC のレシピでは、この Av2 ファミリの 1 個の vCPU の仮想マシンを Active Directory ドメインとドメイン コントローラ マシンに使用します。この見積もりでは、9 個の vCPU (8 + 1) と計算されます。
オプション: [Standard NVSv3 ファミリ vCPU] - 12 個の vCPU * (1 + デスクトップ数)	PoC で GPU 対応のゴールド イメージとデスクトップを試す場合。この NVSv3 ファミリから、ゴールド イメージ用の 12 個の vCPU に、12 個の vCPU にそのイメージに基づいて試すデスクトップの数を掛けたものを加算します。
PoC 単一セッション仮想デスクトップおよびマルチセッション ファームの仮想マシン ファミリ	ポッドによって提供される仮想デスクトップとリモート アプリケーション。Horizon Cloud on Microsoft Azure 環境では、これらにさまざまな仮想マシン ファミリを使用できます。単一セッションまたはマルチセッションの仮想インスタンスごとに、2 個以上の vCPU を推奨します。PoC レシピの場合、[Standard Dv3 ファミリ vCPU] と 20 台の単一セッション Windows デスクトップ、2 台のマルチセッション Windows デスクトップ、および 2 台のマルチセッション RDSH サーバの使用を見積もります。この見積もりでは、そのファミリから 48 個の vCPU (24 x 2 個の vCPU) と計算されます。

上記の数値は、このページの概要で説明されているように、単純な PoC レシピの数値のみを反映していることに注意してください。これらの数値は、複雑なポッド環境、大規模なデスクトップまたはリモート アプリケーション、初期デプロイのアップグレード、またはサービスの Windows 11 OS サポートのいずれかに対応するものと解釈することはできません。

可用性と割り当て制限の確認の例

最初に、Azure ポータルで、最初に選択した候補の場所に Azure Database for PostgreSQL サーバ - 単一サーバを作成することが妨げられていないかを確認します。次に、その候補に必要な [仮想マシン ファミリ vCPU] の可用性を確認します。

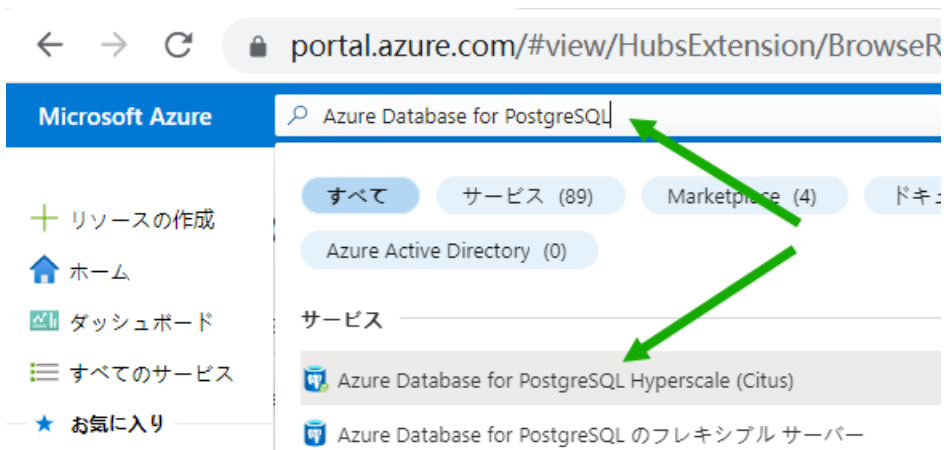
これらの手順を実行する前に、PoC アクティビティ 2 が完了し、Microsoft.DBforPostgreSQL、Microsoft.Sql、および Microsoft.Compute リソース プロバイダが Registered 状態になっていることを確認してください。

この例のスクリーンショットは、このページの手順を証明するために使用した従量課金制のサブスクリプションの内容を示しています。Microsoft によって表示内容やアクセスの対象がパーソナライズされるため、実際の表示は異なります。

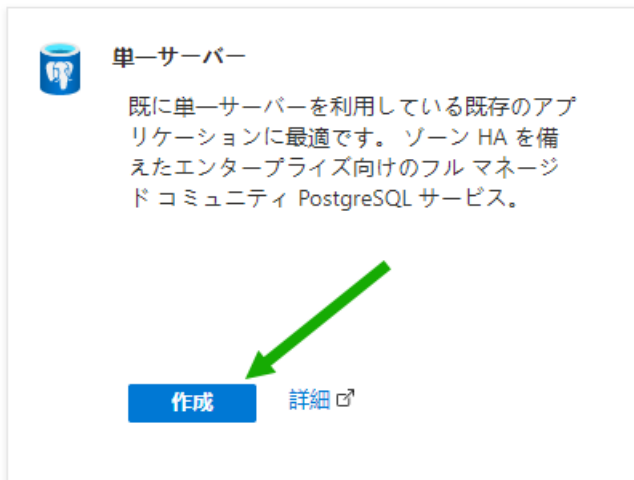
手順 1 - 最上位の候補を特定する場所で、Azure Database for PostgreSQL の作成を開始します。

Microsoft Azure が、特定のリージョンの場所に単一サーバ タイプの Azure Database for PostgreSQL インスタンスを作成することを妨げる場合は、ポッドのデプロイもブロックされます。したがって、このデータベース要件を最初に証明することをお勧めします。

- 1 Azure ポータルの上部の検索バーで、「**Azure Database for PostgreSQL servers**」と入力すると、[Azure Database for PostgreSQL サーバ] アイコンが表示されます。そのアイコンをクリックします。



- 2 ポータルの [Azure Database for PostgreSQL サーバ] ペインで、[作成] をクリックします。この手順では、Microsoft Azure が候補の場所での作成を許可するかどうかを確認できるウィザード プロセスを開始します。
- 3 [単一サーバ] オプションで、[作成] をクリックします。ポッド デプロイには、[単一サーバ] タイプを使用します。場所での可用性を確認するには、類似するものどうしを比較する必要があります。



Azure ポータルで柔軟なサーバの作成を求められた場合でも、[単一サーバの作成] のパスを選択します。

- 4 [単一サーバ] ペインで、[場所] メニューまでスクロールし、候補のリージョンの場所を選択します。

Azure ポータルに、サブスクリプションのこの場所でサービスを利用できないというメッセージが表示された場合は、場所の短いリストの次の候補を試してください。

たとえば、従量課金制のサブスクリプションでこれらの手順を実行し、(Asia Pacific) Southeast Asia を選択した日に、Currently, the service is not available in this location for your subscription. というメッセージが表示されました。



Microsoft は、リージョンごと、およびサブスクリプションごとに、サービスを利用可能にする場所を完全に制御できます。

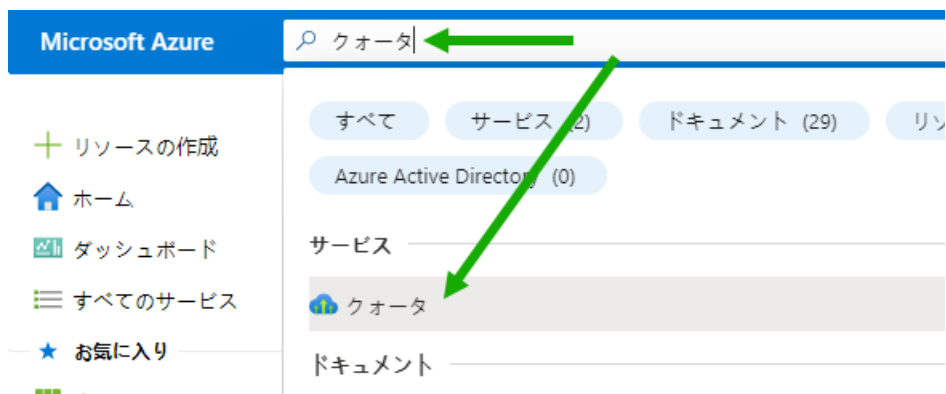
同じ日に、次の候補の (Asia Pacific) East Asia を選択したときには、メッセージが表示されませんでした。

[場所] メニューの下に選択した場所に関するメッセージが表示されない場合、その場所は、次の検証に進み、その候補の場所にある仮想マシン ファミリを検証することのできる候補です。

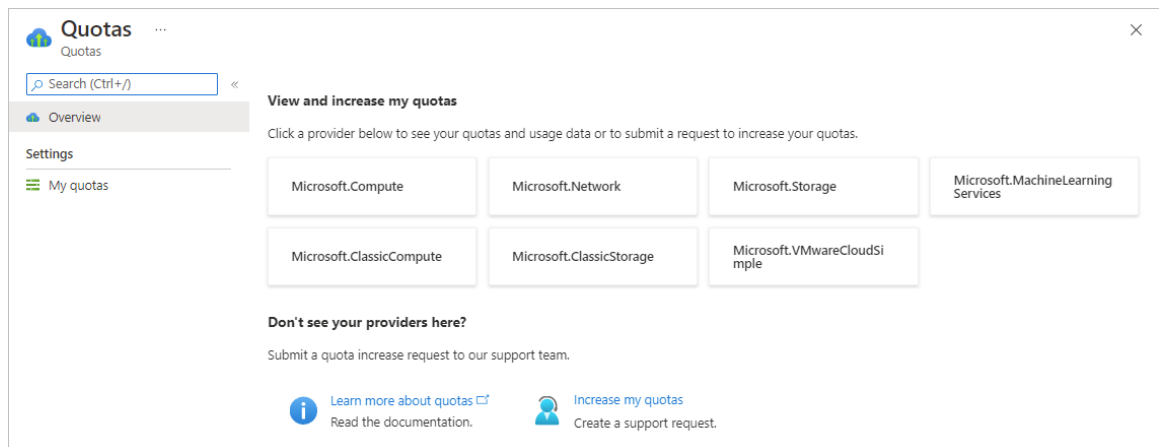
- 5 [X] をクリックして、[単一サーバ] ペインを閉じます。ポータルで、保存されていない編集を破棄できるようにします。

手順 2 - 手順 1 で特定した場所を使用して、その場所での仮想マシン ファミリ vCPU の可用性を確認します。

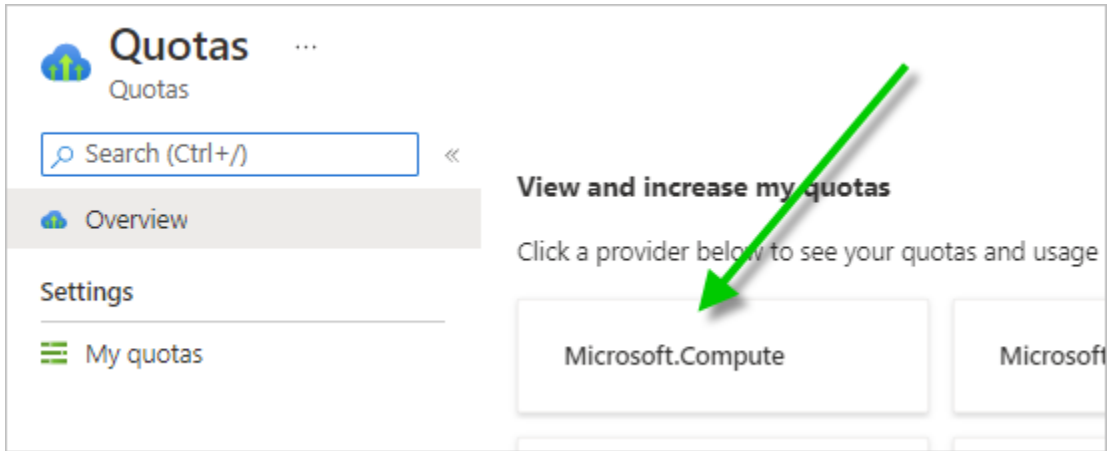
- 1 Azure ポータルの上部の検索バーで、「quota」と入力すると、[割り当て] アイコンが表示されます。[割り当て] アイコンをクリックします。



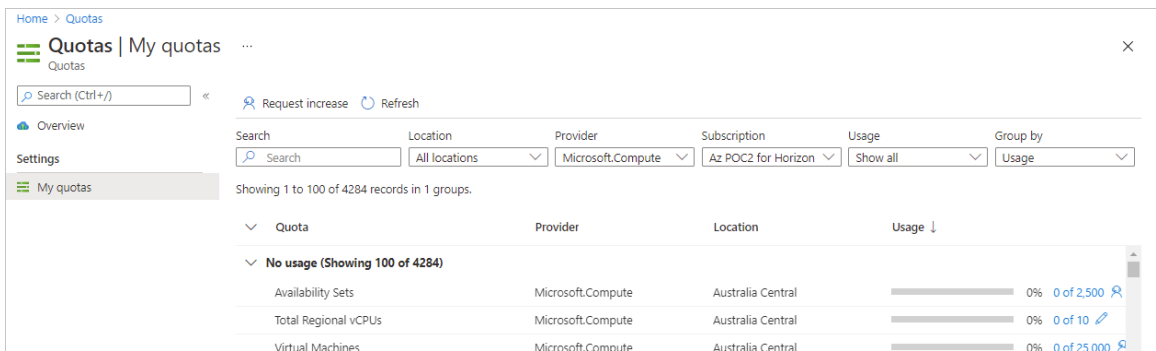
[割り当て] をクリックすると、ポータルには [割り当て] ペインが表示されます。



- 2 [Microsoft.Compute] をクリックします。

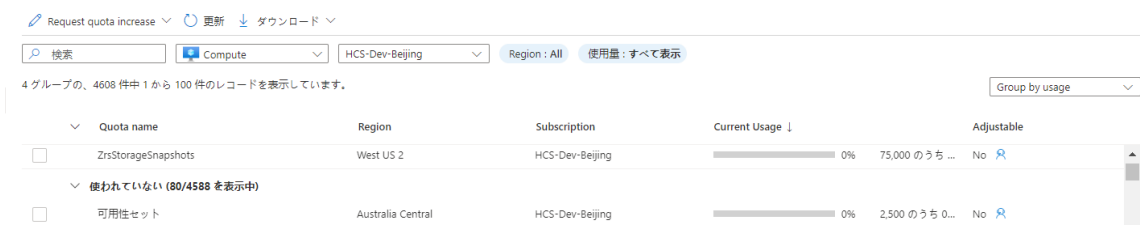


[マイ割り当て] ペインが表示され、上部にはフィルタ ボックスがあり、[プロバイダ] フィルタは [Microsoft.Compute] に設定されています。



- [場所] メニューで候補となる場所を選択し、[サブスクリプション] メニューでこの PoC に使用しているサブスクリプションが選択されていることを確認します。

次のスクリーンショットは、場所 West US 3 と PoC サブスクリプションの選択を示しています。



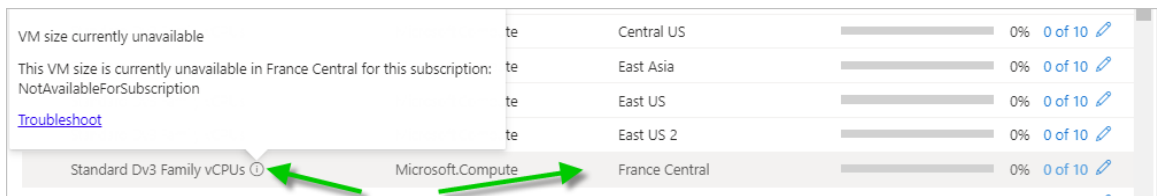
- 4 候補となる場所について、次の各ファミリの [仮想マシン ファミリ vCPU] の可用性レベルを確認し、必要に応じてそのファミリの割り当てを増やします。

表 6-3. ポッドのデプロイおよびデプロイ後の VDI 用のファミリ vCPU

仮想マシン ファミリ	必要となる使用可能な vCPU
[Standard Dv3 ファミリ vCPU]	合計 10 個の vCPU (PoC ポッド自体に 8 個の vCPU と、デプロイ後の 1 つの RDSH ゴールド イメージの作成に使用する 2 個の vCPU)
[Standard DSv2 ファミリ vCPU]	合計 4 個の vCPU (1 つの単一セッションの Windows 10 ゴールド イメージと、1 つの Windows 10 Enterprise マルチセッション ゴールド イメージのデプロイ後の作成用)
[Standard Av2 ファミリ vCPU]	合計 9 個の vCPU (ポッド上のゲートウェイに 8 個の vCPU、PoC ローカル Active Directory に 1 個の vCPU)
オプション: [Standard NVSv3 ファミリ vCPU]	ゴールド イメージ用の 12 個の vCPU と、使用するデスクトップの数 x 12 個の vCPU
PoC 単一セッション VDI デスクトップおよびマルチセッションファームに使用する仮想マシン ファミリ	PoC レシピでは、[Standard Dv3 ファミリ vCPU] と 20 台の単一セッション Windows デスクトップ、2 台のマルチセッション Windows デスクトップ、および 2 台のマルチセッション RDSH サーバの使用を計画しました。これは、その [Standard Dv3 ファミリ vCPU] から 48 個の vCPU と計算されます (24 x 2 vCPU)。

- 5 手順 3 の仮想マシン ファミリのいずれかで、仮想マシン ファミリ名の横に ① 記号 (丸で囲んだ小文字の l) が表示されている場合は、その記号をクリックします。「現在使用できない仮想マシン サイズです」というメッセージが表示された場合は、リストからその候補を削除する必要があります。その場合は、手順 1 - PostgreSQL データベースの検証を繰り返して、新しい使用可能な候補を特定し、仮想マシン ファミリでこの確認を繰り返します。

例として、従量課金制のサブスクリプションで France Central の [Standard Dv3 ファミリ vCPU] の可用性を確認したときに作成した次のスクリーンショットを参照してください。次のスクリーンショットは、この仮想マシン ファミリが Microsoft Azure のこのリージョンでサブスクリプションに使用できない状況を示しています。



Microsoft によって表示内容やアクセスの対象がパーソナライズされるため、実際の表示の詳細は異なります。

- 6 ファミリの利用可能なキャパシティが上記の表の数値よりも少ない場合は、そのリージョンでそのファミリの割り当てを増やします。

たとえばこのスクリーンショットは、サブスクリプションの West US 3 場所で現在使用されている [Standard Dv3 ファミリー vCPU] がゼロ ([使用率] 0%) であることを示しています。ただし、このスクリーンショットには、現在の割り当てで対応できる使用量が最大 10 で、非常に少ないことも示されています。PoC では、[Standard Dv3 ファミリー vCPU] からの使用量が 10 を超える必要があるため、割り当ての最大数を増やす必要があります。

Quota name	Region	Subscription	Current Usage ↓	Adjustable
ZrsStorageSnapshots	West US 2	HCS-Dev-Beijing	0%	No
可用性セット	Australia Central	HCS-Dev-Beijing	0%	No
リージョンの vCPU の合計	Australia Central	HCS-Dev-Beijing	0%	Yes

Microsoft は、個々の [仮想マシン ファミリー vCPU] の割り当ての増加を要求するいくつかの方法を提供しています。従量課金制のサブスクリプションでは、上記の画面で使用量の右側にある鉛筆アイコンをクリックしました。

Quota	Provider	Location	Usage ↓
No usage (1)			
Standard Dv3 Family vCPUs	Microsoft.Compute	West US 3	0% 0 of 10

鉛筆アイコンをクリックするとフォームが開き、選択した場所とサブスクリプション内でその仮想マシン ファミリーの vCPU の新しい最大数に割り当てを増やす要求を指定できます。

注： Microsoft 自身によって、要求を承認するか拒否するかが決定されます。要求が拒否された場合は、リンクが表示され、そこで Microsoft へのサポート リクエストを発行すると、割り当ての増加の支援を受けることができます。

- 上記の手順を使用して、単一サーバの Azure Database for PostgreSQL と [仮想マシン ファミリー vCPU] の両方の可用性要件を満たす場所を特定した後、そのリージョンの場所の [リージョン vCPU の合計] のレベルを確認して、使用可能な未使用の vCPU の数を調べます。

たとえば、次のスクリーンショットは、サブスクリプションの West US 3 場所で、[リージョン vCPU の合計] の割り当ての合計が最大 10 であることを示しています。これは、PoC レシピに必要な 71 よりもはるかに少ない値です。

Quota	Provider	Location	Usage ↓
No usage (Showing 100 of 121)			
Availability Sets	Microsoft.Compute	West US 3	0% 0 of 2,500
Total Regional vCPUs	Microsoft.Compute	West US 3	0% 0 of 10

サブスクリプションで、PoC 環境に必要な利用可能な vCPU の合計数を満たすための十分な未使用の vCPU がいないことをリージョンの [リージョン vCPU の合計] 割り当てレベルが示している場合は、[リージョン vCPU の合計] レベルも増やす必要があります。

手順 3 - 候補のリージョンのリージョン vCPU の合計を確認し、必要に応じて増やします。

これらの手順は、個々の [仮想マシン ファミリ vCPU] の割り当て制限を増やした後に実行してください。

PoC レシピに従って、目的の Azure リージョンの場所に少なくとも合計 71 個の新しい vCPU を収容する必要があります。Azure では、確認する割り当ては [リージョン vCPU の合計] です (この 71 の数には、ポッド自身、1 つの外部ゲートウェイ、ローカルの Active Directory ドメイン サーバ、および見積もられた 3 つのゴールド イメージ用の 16 個の vCPU、および約 20 台の仮想デスクトップが含まれます。この数には、GPU 対応の NV ファミリ イメージまたはデスクトップの使用は含まれません。これらを含めるには、追加の 12 個の vCPU と GPU デスクトップの数 x 12 を追加します)。

- 1 前の手順と同じ [マイ割り当て] ペインで、デプロイに使用する場所とサブスクリプションを選択し、[リージョン vCPU の合計] の行を見つけます。

例として、次のスクリーンショットは、デプロイに使用する West US 3 場所とサブスクリプションの [リージョン vCPU の合計] を示しています。

Quota	Provider	Location	Usage
No usage (Showing 100 of 121)			
Availability Sets	Microsoft.Compute	West US 3	0% 0 of 2,500
Total Regional vCPUs	Microsoft.Compute	West US 3	0% 0 of 10

- 2 [使用量] 列に表示される X of Y の数が、使用可能な (未使用の) vCPU の数が PoC に必要な数より少ないことを示している場合は、X of Y の数の右側にある鉛筆アイコンをクリックして最大数を増やします (Y の数を増やします)。

実際の数値は、独自のサブスクリプションおよび場所の最新情報を反映しているため、スクリーンショットの数とは異なります。

差分 ($Y - X = Z$) を確認して、その場所で使用可能な vCPU の数を確認します。たとえば、[使用量] に 10 of 15 と表示されている場合、差分は 5 ($15 - 10 = 5$) のみとなります。PoC に対応するには、この低い数を増やす必要があります。

まったく新しい従量課金制サブスクリプションの場合、サブスクリプションにはまだ仮想マシンがないため、最初の使用量には 0 of 10 と表示されます。ポッド、外部ゲートウェイ、Active Directory ドメイン マシン、3 つのゴールド イメージ、20 台の仮想デスクトップの見積もり数に対応するため、最大値を 71 に設定する必要があります。

サブスクリプションの鉛筆アイコンをクリックした後、[割り当ての増加を要求]で、新しい最大数に「71」と入力し、要求を送信します。

注： Microsoft 自身によって、要求を承認するか拒否するかが決定されます。要求が拒否された場合は、リンクが表示され、そこで Microsoft へのサポート リクエストを発行すると、割り当ての増加の支援を受けることができます。

サブスクリプションで West US 3 場所の [Standard Dv3 ファミリ vCPU] の可用性を確認し、割り当てを増やす具体的な例

PoC レシピでは、単一セッション仮想 Windows デスクトップ、マルチセッション Windows デスクトップ、およびマルチセッション RDSH サーバに [Standard Dv3 ファミリ vCPU] の使用を計画します。これらに加えてポッド自身に対応するために、そのファミリの割り当てが少なくとも 58 個の vCPU を持っていることを確認する必要があります（前の表のデータから合計）。

この数を確認し、必要に応じて増やすことで、仮想デスクトップの作成を開始するとき [Standard Dv3 ファミリ vCPU] が不足しないようにします。

- 1 [マイ割り当て] ペインの [検索] フィルタで、**[Standard Dv3 Family]** と入力し、[場所] を West US 3 に設定します。この検索により、サブスクリプションの West US 3 にある、[Standard Dv3 ファミリ vCPU] の使用可能な割り当てを確認できます。

Quota name	Region	Subscription	Current Usage	Adjustable
<input type="checkbox"/> ZrsStorageSnapshots	West US 2	HCS-Dev-Beijing	0% 75,000 のうち 1 を...	No
▼ 使われていない (80/4588 を表示中)				
<input type="checkbox"/> 可用性セット	Australia Central	HCS-Dev-Beijing	0% 2,500 のうち 0 を...	No
<input type="checkbox"/> リージョンの vCPU の合計	Australia Central	HCS-Dev-Beijing	0% 10 のうち 0 を使...	Yes

- 2 [使用量] 列をチェックして、使用可能な合計のうち少なくとも [58] 個が未使用で残っていることを確認します。

たとえば、[使用量] 列に [8/10] と表示されている場合、10 個のうち 8 個が使用中であり、その割り当てレベルで使用可能な vCPU が 2 個だけであることを意味します（10 - 8 = 2 個が未使用）。その場合は、割り当てを少なくとも 56 個の vCPU を増やして、[Standard Dv3 ファミリ vCPU] に必要な合計 58 個の vCPU に対応する必要があります。

次に、上記の表にある他の必要な仮想マシン ファミリについても同様の割り当てチェックを繰り返し、必要に応じて増やしました。

4 アプリケーション登録を作成する

このアプリケーション登録は、Horizon Cloud Service on Microsoft Azure 環境を可能にする重要な要素です。

Azure サブスクリプションでアプリケーションを登録すると、その API 呼び出しを使用して、そのサブスクリプションで Horizon Cloud Service on Microsoft Azure 環境を作成する機能が Horizon Cloud に提供されます。

サービスは API 呼び出しを使用して、最初にサブスクリプションでのデプロイを開始します。このサービスはまた、ゴールド イメージ、VDI デスクトップなどを作成する Day-2 の操作（すべての VDI 管理タスク）にも API 呼び出しを使用します。

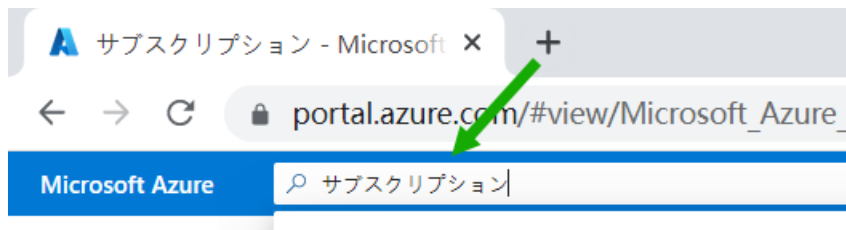
表 6-4. この手順でこれらの項目を収集し、[ポッドの追加] ウィザードを実行するときのために保存します。

[ポッドの追加] ウィザードの項目	ユーザーの値
下記の手順 2 の [サブスクリプション ID]	
下記の手順 5 の [アプリケーション (クライアント) ID]	
下記の手順 5 の [ディレクトリ (テナント) ID]	
下記の手順 6 のクライアント シークレットの [値]	

手順

- 1 Azure ポータルで、PoC で使用するために準備しているサブスクリプションの詳細に移動します。Subscriptions を検索し、結果リストに表示されたら [サブスクリプション] をクリックします。

たとえば、Azure ポータルの検索バーを使用して Subscriptions を検索します。結果リストに表示されたら、[サブスクリプション] をクリックし、特定のサブスクリプションをクリックします。



- 2 サブスクリプションの詳細から、[サブスクリプション ID] をコピーし、後で [ポッドの追加] ウィザードで参照できる場所に保存します。

次のスクリーンショットは、Az POC for Horizon という名前のサブスクリプションの [サブスクリプション ID] をコピーした場所を示しています。ここでは、値を保護するために具体的な ID を編集しました。



- 3 次に、Azure ポータルの検索バーで App registrations を検索し、結果リストに表示されたら [アプリケーション登録] をクリックします。



検索結果から [アプリケーション登録] をクリックすると、ポータルに [アプリケーション登録] ページが表示されます。

- 4 [アプリケーション登録] ページで、[新規登録] をクリックします。

アプリの登録 ...



Azure ポータルに、アプリケーション登録を作成するためのユーザー インターフェイスが表示されます。

5 ユーザー インターフェイス フォームで、次の項目を指定します。

- この登録が Horizon Cloud で使用されることを思い出させる表示名。
- このアプリケーション登録を使用できる単一のテナントの選択肢を選択します（本書の執筆時点では、この選択肢には「[この組織ディレクトリのアカウントのみ]」というラベルが付いています）。

6 オプションの項目はそのままにして、[登録] をクリックします。

新しく作成されたアプリ登録が画面に表示されます。

7 表示されたアプリケーション登録から、[アプリケーション (クライアント) ID] と [ディレクトリ (テナント) ID] をコピーし、後で [ポッドの追加] ウィザードで参照できる場所に保存します。

次のスクリーンショットは、アプリケーション登録の重要な詳細を示しています。表示名は hcs-poc1 です。ここでは、値を保護するために、具体的な [アプリケーション (クライアント) ID] と [ディレクトリ (テナント) ID] が編集されています。



8 次に、このアプリケーション登録用のクライアント シークレット キーを作成します。


a 手順 5 のアプリケーション登録画面で、[証明書またはシークレットを追加] のテキストをクリックします。

ポータルには、このアプリケーション登録の [証明書とシークレット] ペインが表示されます。

hcs-poc1 アプリケーション登録の場合、次のように表示されます。



b このペインで [新しいクライアント シークレット] をクリックします。

説明	有効期限	値 ^①
+ 新しいクライアント シークレット 		

c ポータルに [クライアント シークレットを追加] 画面が表示されます。

説明を入力し、この Horizon Cloud on Microsoft Azure PoC に対応する期間の長さに合わせて有効期限を選択します。

ここでは、12 か月（1 年）の有効期限を設定しています。ただし、このクライアント シークレットを新しい Horizon Cloud on Microsoft Azure 環境で引き続き使用する場合は、期限が切れる前に戻る必要があります。

クライアント シークレットに hcspec1 という名前を付けました。

クライアント シークレットの追加

×

説明

hcspec1

有効期限

12 か月

▼

追加

キャンセル

- d [追加] をクリックします。

[証明書とシークレット] ペインにエントリが表示されたらすぐに、[値] 列を見つけてコピーし、後で [ポッドの追加] ウィザードで参照できる場所に保存します。

重要： [値] をコピーし、後で参照可能な場所に保存するまでは、この画面を開いたままにします。このユーザー インターフェイスから移動すると、ポータルによって [値] が難読化され、値をコピーして保存するには、クライアント シークレットの作成を繰り返す必要があります。

次のスクリーンショットは、作成したクライアント シークレットを示しています。ここでは、データを保護するために具体的な値が編集されています。

+ 新しいクライアント シークレット			
説明	有効期限	値 ①	シークレット ID
hcspec1	2023/6/21	u [編集]	9 [編集] [削除]

- 9 次に、このアプリケーション登録に Azure の組み込み Contributor ロールを割り当てます。

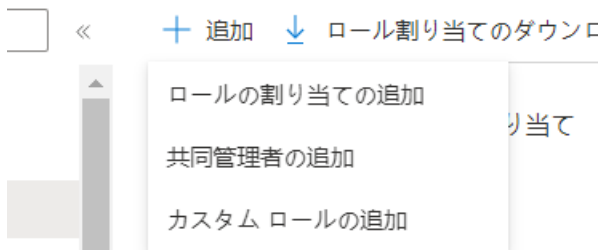
このロールの割り当てにより、サブスクリプションでの PoC 環境のために API 呼び出しを使用する機能が Horizon Cloud に提供されます。

- a 再度、サブスクリプションの詳細に戻ります (Azure ポータルの検索バーを使用して Subscriptions を検索し、表示されたら [サブスクリプション] をクリックして、[サブスクリプション] ペインでサブスクリプションをクリックします)。
- b [アクセス制御 (IAM)] をクリックします。

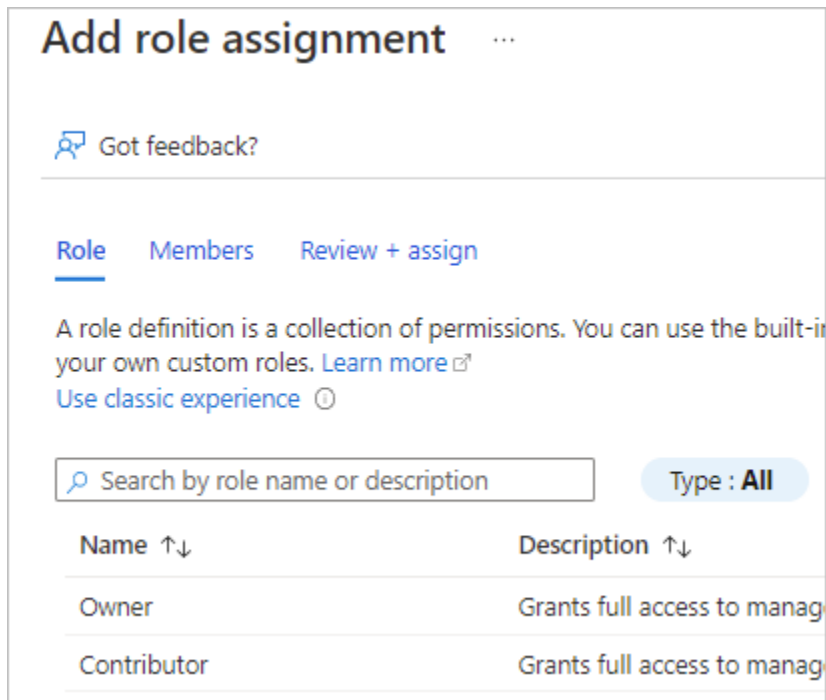


- c [アクセス制御 (IAM)] ペインで、[追加] - [ロール割り当ての追加] をクリックします。

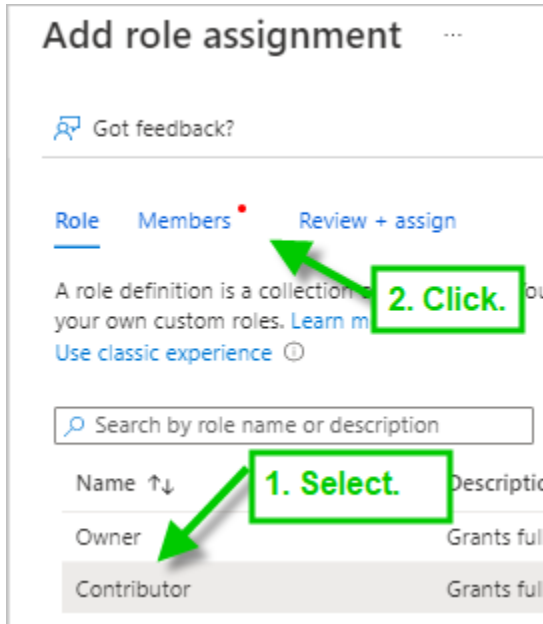
アクセス制御 (IAM) ...



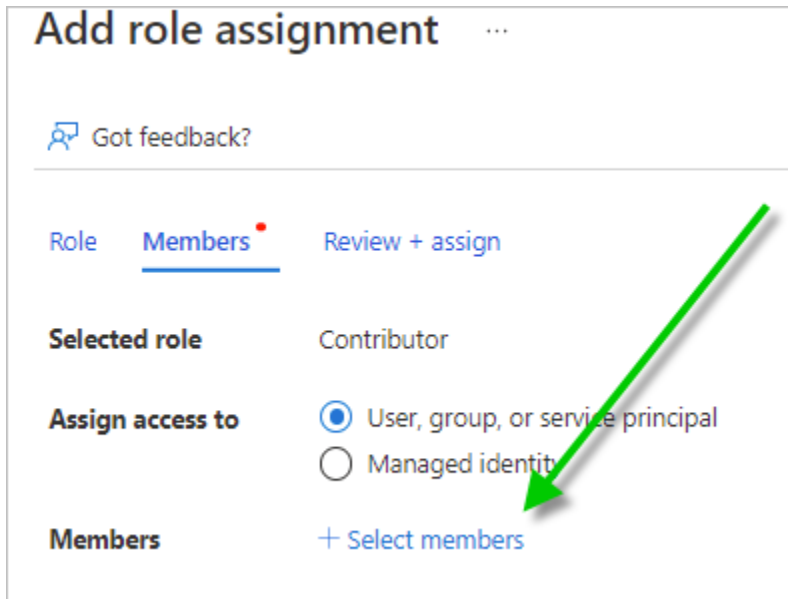
このアクションにより、[ロール割り当ての追加] ペインが表示されます。



- d この [ロール割り当ての追加] ペインで、Contributor を選択し、[メンバー] をクリックして [メンバー] タブに移動します。



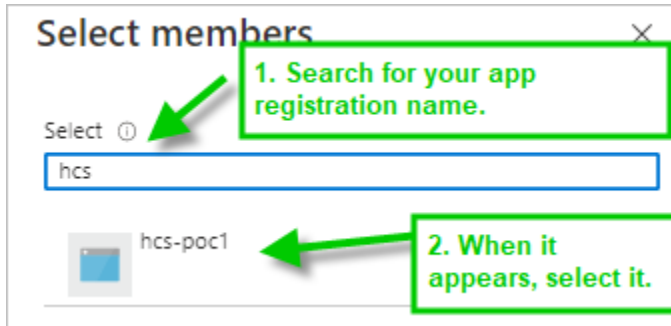
- e [メンバー] タブで、[ユーザー、グループ、またはサービス プリンシパル] を選択したまま、[メンバーを選択] をクリックします。



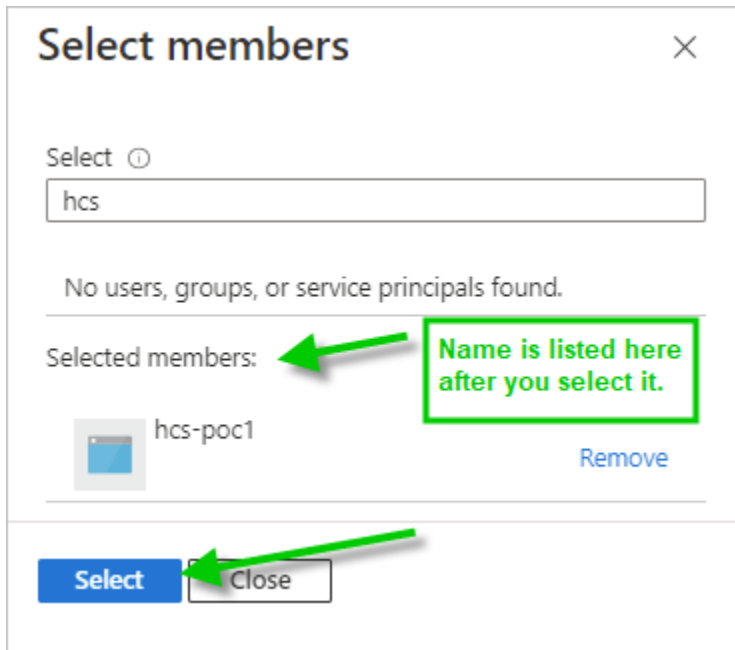
- f 選択ウィンドウで、手順 5 で作成したアプリケーション登録の名前を検索します。

手順 6 でアプリケーション登録を作成したときに、Azure はアプリケーション登録と同じ名前の関連付けられたサービス プリンシパルも作成しました。技術的には、Horizon Cloud API 呼び出しはアプリケーション登録とそれに関連付けられたサービス プリンシパルの両方を使用して、Horizon Cloud on Microsoft Azure 環境を作成および操作します。

アプリケーション登録に使用した名前「hcs-poc1」を検索します。

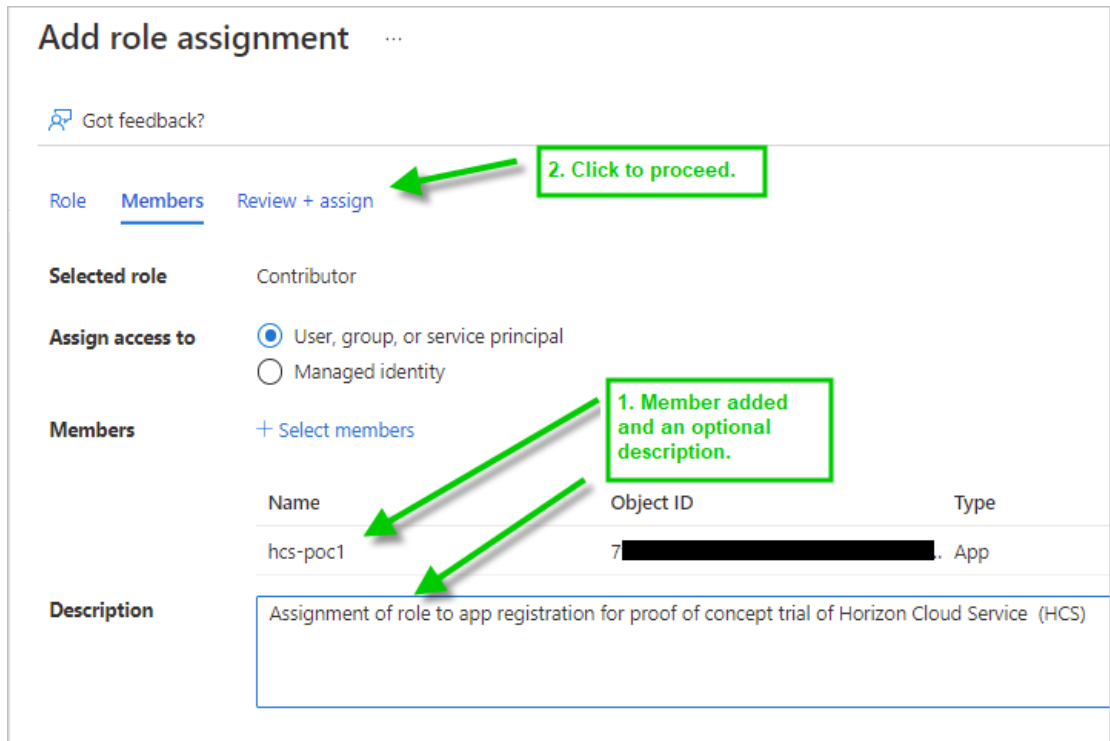


- g 名前をクリックすると、選択したメンバーとしてリストに表示されます。次に、[選択] をクリックして選択を確定します。

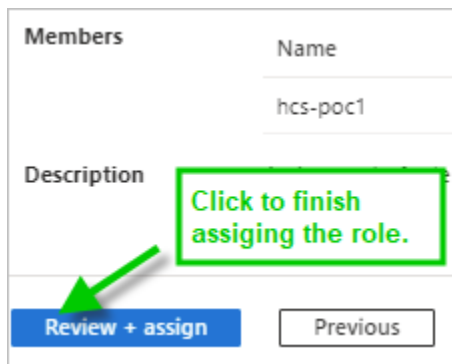


- h アプリケーション登録の名前が [メンバー] タブに追加されます。必要に応じてオプションの説明を追加し、[レビュー + 割り当て] をクリックして、[レビュー + 割り当て] タブに移動します。

次のスクリーンショットは、オブジェクト ID が編集された PoC の選択肢を示しています。



- i [レビュー + 割り当て] タブで、[レビュー + 割り当て] というラベルの付いたボタンをクリックして、これらの手順を完了します。



5 ネットワークを設定する

次に、PoC で使用する仮想ネットワーク (VNet) とサブネットを作成します。

PoC レシピでは、次のアドレス空間とサブネットを定義します。

Azure は、各サブネットから常に 5 つのアドレスを自身のために予約します。

アドレス空間	名前	目的
10.0.0.0/23	vnet-hcspoc	PoC 用に作成している VNet 全体。/23 は、VNet のアドレス空間を 512 アドレスで開始します。この CIDR を使用すると、次のサブネットを使用して、ポッド、ゲートウェイ、および PoC のゴールド イメージと仮想デスクトップに対応できます。 PoC に合わせて、より大きな空間を自由に選択してください。
10.0.0.0/29	poc-adsubnet	このサブネットにローカルの PoC Active Directory サーバ マシンを配置します。 ここでは、/29 を使用します。これは、使用できる最小の範囲であり、また、Azure が常に自身のためにすべてのサブネットから予約する 5 つのアドレスに対応しているためです。
10.0.0.32/27	hcspoc-mgmt	[ポッドの追加] ウィザードのポッド管理サブネット用。[ポッドの追加] ウィザードでは、このサブネットに少なくとも /27 が適用されます。Horizon Cloud on Microsoft Azure 環境では、環境の仮想マシンのみがこのサブネット上に配置され、他の既存マシンやデプロイ後のマシンは配置されていないことが要件です。したがって、このサブネットと次の 2 つのサブネットを個別のサブネットとして定義する必要があります。 [ポッドの追加] ウィザードでは、このサブネットに Microsoft.Sql という名前のサービス エンドポイントが構成されている必要もあります。これは、このアクティビティ  の最後のステップで追加します。
10.0.0.64/28	hcspoc-uag-ext	[ポッドの追加] ウィザードの外部ゲートウェイ サブネット用。[ポッドの追加] ウィザードでは、このサブネットに少なくとも /28 が適用されます。
10.0.1.0/25	hcspoc-vdi	[ポッドの追加] ウィザードの仮想マシン サブネット用。ここでは、/25 を使用して 128 個のアドレスを提供します。このアドレスは、ここでレシピで計画しているゴールド イメージと VDI デスクトップに使用します。

手順

- 1 Azure ポータルの上部の検索バーで、「**Virtual networks**」と入力して [仮想ネットワーク] アイコンを表示します。この [仮想ネットワーク] アイコンをクリックします。

[仮想ネットワーク] をクリックすると、ポータルに [仮想ネットワーク] ペインが表示されます。

ホーム >

仮想ネットワーク ☆ ...

VMware, Inc.

+ 作成 ⚙️ ビューの管理 ∨ 🔄 更新 ↓ CSV にエクスポート

任意のフィールドのフ...

サブスクリプション equals すべて

サブスクリプション フィルタがこの PoC のサブスクリプションに設定されていることを確認し、[作成] をクリックします。

仮想ネットワーク ☆ ...

VMware, Inc.

+ 作成 ⚙️ ビューの管理 ∨ 🔄 更新 ↓ CSV にエクスポート

任意のフィールドのフ...

サブスクリプション equals すべて

- 2 表示された [仮想ネットワークの作成] ウィザードで、[新規作成] を使用して、VNet オブジェクトを Azure に保持するためのリソース グループに名前を付けて作成します。

この例では、このリソース グループに「hcsvnet-RG」という名前を付けます。

[すべてのサービス](#) > [仮想ネットワーク](#) >

仮想ネットワークの作成 ...

基本 IP アドレス セキュリティ タグ 確認および作成

Azure Virtual Network (VNet) は、Azure のプライベート ネットワークの基本構成ブロックです。VNet を使用すると、Azure Virtual Machines (VM) など、Azure リソースの多くの種類が有効になり、相互にまたはインターネットやオンプレミスのネットワークと安全に通信できます。VNet は、独自のデータ センターで運用する従来のネットワークに似ていますが、スケーリング、可用性、分離などの Azure のインフラストラクチャの他の利点を活用できます。 [仮想ネットワークの詳細](#)

プロジェクトの詳細

サブスクリプション * ⓘ リソース グループ * ⓘ [新規作成](#)

インスタンスの詳細

名前 * 地域 *

リソース グループは、Azure のソリューションに関連するリソースを保持するコンテナです。

名前 *

OK

キャンセル

[確認および作成](#)

< 前へ

次: IP アドレス >

[Automation のテンプレートをダウンロードする](#)

- VNet の名前を入力します。リージョンに対しては、アクティビティ [3](#) を使用して確認したのと同じ Azure のリージョンの場所を選択します。これは、PoC の可用性と割り当てのニーズを満たすものです。この PoC では、VNet に vnet-hcspoc という名前を付け、サブスクリプションで West US 3 リージョンを使用することを選択しました。これは、アクティビティ [3](#) で確認し、割り当てを増やしたリージョンです。

[すべてのサービス](#) > [仮想ネットワーク](#) >

仮想ネットワークの作成 ...

基本 IP アドレス セキュリティ タグ 確認および作成

Azure Virtual Network (VNet) は、Azure のプライベート ネットワークの基本構成ブロックです。VNet を使用すると、Azure Virtual Machines (VM) など、Azure リソースの多くの種類が有効になり、相互にまたはインターネットやオンプレミスのネットワークと安全に通信できます。VNet は、独自のデータ センターで運用する従来のネットワークに似ていますが、スケーリング、可用性、分離などの Azure のインフラストラクチャの他の利点を活用できます。 [仮想ネットワークの詳細](#)

プロジェクトの詳細

サブスクリプション * ① ▼

リソース グループ * ① ▼
新規作成

インスタンスの詳細

名前 * ✓

地域 * ▼

確認および作成

< 前へ

次: IP アドレス >

[Automation のテンプレートをダウンロードする](#)

- [IP アドレス] タブに移動します。
- Azure では、[IPv4 アドレス空間] に大きな値が事前に入力されます。事前入力された値をクリックし、VNet の初期アドレス空間に使用する CIDR に変更します。

[すべてのサービス](#) > [仮想ネットワーク](#) >

仮想ネットワークの作成 ...

基本 IP アドレス セキュリティ タグ 確認および作成

CIDR 表記の 1 つまたは複数のアドレス プレフィックスとして指定された、仮想ネットワークのアドレス空間 (192.168.1.0/24)。

IPv4 アドレス空間

PoC では、512 個の IP アドレス (10.0.0.0 ~ 10.0.1.255) を提供する CIDR である、10.0.0.0/23 を使用することを選択します。本書の執筆時点では、その値の下の領域をクリックすると、Azure ポータルにアドレス範囲が表示されます。



PoC に合わせて、より大きなアドレス空間を自由に選択してください。

6 次に、この PoC に必要な 4 つのサブネットを指定します。

これらのサブネットごとに、次の手順を実行します。

a [サブネットの追加] をクリックします。



[サブネットの追加] ユーザー インターフェイスに入力します。本書の執筆時点では、次のスクリーンショットのようになります。サブネット名とそのアドレス範囲を入力し、[追加] をクリックします。

サブネットの追加 ×

サブネット名 *

サブネット アドレス範囲 * ①

(0 アドレス)

NAT ゲートウェイ

ネットワーク アドレス変換ゲートウェイを使用してインターネットへの接続を簡素化します。ロード バランサーまたはパブリック IP アドレスが仮想マシンにアタッチされていなくても、送信接続が可能です。 [詳細情報](#)

NAT ゲートウェイ

サービス エンドポイント

仮想ネットワークからサービス エンドポイントを介して特定の Azure リソースへのトラフィックを許可する、サービス エンドポイントのポリシーを作成します。 [詳細情報](#)

サービス ①

追加

キャンセル

[追加] をクリックするたびに、サブネットが [IP アドレス] タブに追加されます。

[IP アドレス] タブに 4 つのサブネットがすべて表示されるまで繰り返します。

サブネット名	サブネットのアドレス範囲
poc-adsubnet	10.0.0.0/29
hcspec-mgmt	10.0.0.32/27

サブネット名	サブネットのアドレス範囲
hcspoc-uag-ext	10.0.0.64/28
hcspoc-vdi	10.0.1.0/25

[+ サブネットの追加](#)
[🗑️ サブネットの削除](#)


<input type="checkbox"/> サブネット名	サブネット アドレス範囲
<input type="checkbox"/> poc-adsbnet	10.0.0.0/29
<input type="checkbox"/> hcspoc-mgmt	10.0.0.32/27
<input type="checkbox"/> hcspoc-uag-ext	10.0.0.64/28
<input type="checkbox"/> hcspoc-vdi	10.0.1.0/25

- 7 これでは、ウィザードには、VNet を作成するために送信するのに十分な情報があります。[レビュー + 作成] タブに移動します。

Azure は検証チェックを実行します。

[すべてのサービス](#) > [仮想ネットワーク](#) >

仮想ネットワークの作成 ...

 検証に成功しました

基本 IP アドレス セキュリティ タグ 確認および作成

基本

サブスクリプション HCS-Dev-Beijing
 リソース グループ hcspoc
 名前 hcspoc-vnet
 地域 West US 2

IP アドレス

アドレス空間 10.3.0.0/16
 サブネット default (10.3.0.0/24)

タグ

なし

セキュリティ

BastionHost 無効
 DDoS 保護プラン Basic
 ファイアウォール 無効

作成

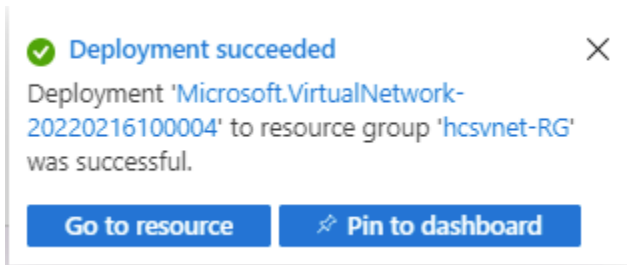
< 前へ

次へ >

[Automation のテンプレートをダウンロードする](#)

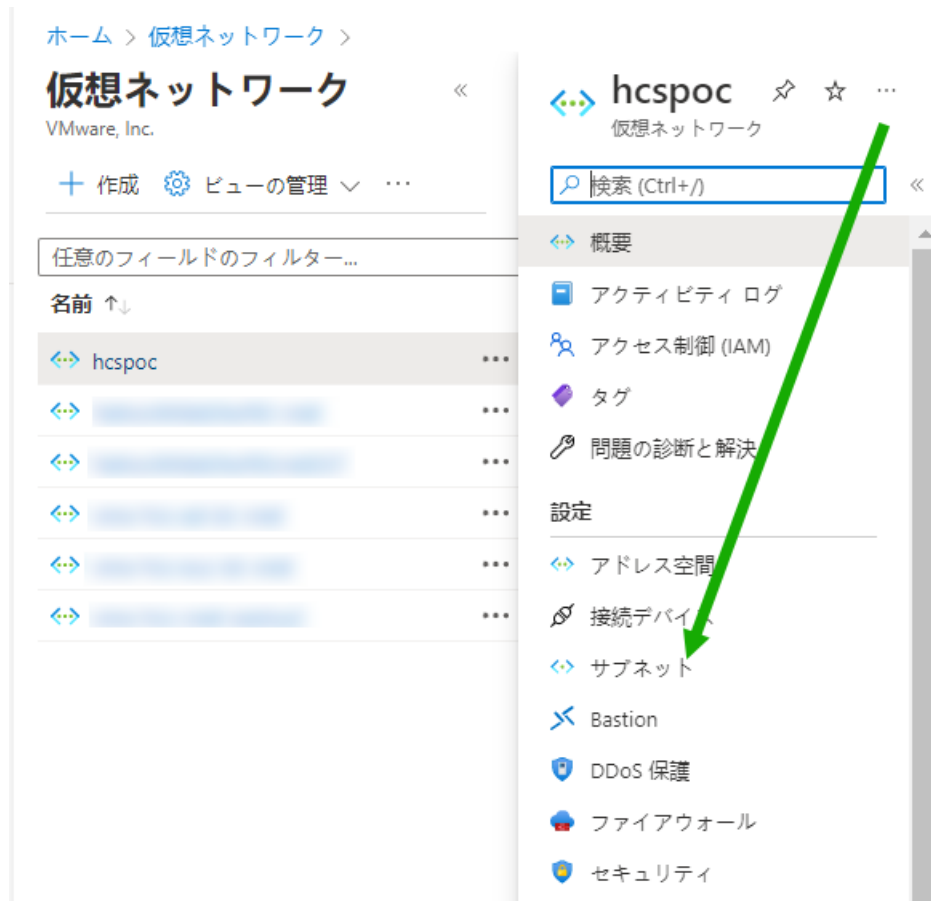
- 8 検証に成功したら、[作成] をクリックします。

Azure は、VNet とサブネットのデプロイを開始します。デプロイに成功すると、ポータルに次のような通知が表示されます。



- 9 次に、Microsoft.Sql という名前のサービス エンドポイントを、[仮想ネットワークの作成] ウィザードで作成した hcsvnet-mgmt サブネットに追加する必要があります。

- ポータルで、新しく作成した VNet（この例では vnet-hcsvnet）に移動します。
- サブネットのリストに移動します。



- hcsvnet-mgmt サブネットをクリックします。ポータルには、そのサブネットの詳細ユーザー インターフェイスが表示されます。

Microsoft.Sql という名前のサービス エンドポイントを追加します。

The screenshot shows the Azure portal interface for configuring a subnet. On the left, a list of subnets is displayed with columns for name and IP address. The 'hcspec-mgmt' subnet is selected. On the right, the configuration details for 'hcspec-mgmt' are shown, including name, address range, and various options like NAT gateway and security groups. The 'サービス' (Services) dropdown menu is highlighted with a red box, and a message below it states '0項目が選択されました' (No items selected).

名前 ↓	IP アドレス ↓
poc-adsbnet	10.2.4.0/29
AzureBastionSubnet	10.2.1.0/26
hcspec-desktop	10.2.2.0/24
hcspec-mgmt	10.2.0.0/24

hcspec-mgmt configuration details:

- 名前: hcspec-mgmt
- サブネット アドレス範囲: 10.2.0.0/24 (10.2.0.0 - 10.2.0.255 (251 + 5 個の Azure 予約アドレス))
- IPv6 アドレス空間の追加:
- NAT ゲートウェイ: なし
- ネットワーク セキュリティ グループ: なし
- ルート テーブル: なし
- サービス エンドポイント: なし
- サービス: 0項目が選択されました
- サブネットの委任: なし

d [サービス エンドポイント] メニューをクリックして、サービスのリストを取得します。

hcspec-mgmt
vmw-hcs-vnet-westus2

名前
hcspec-mgmt

サブネット アドレス範囲 * ⓘ
172.168.165.0/27

- すべて選択
- Microsoft.AzureActiveDirectory
- Microsoft.AzureCosmosDB
- Microsoft.CognitiveServices
- Microsoft.ContainerRegistry
- Microsoft.EventHub
- Microsoft.KeyVault
- Microsoft.ServiceBus
- Microsoft.Sql
- Microsoft.Storage
- Microsoft.Web

サービスのフィルター

0 項目が選択されました

- e [Microsoft.Sql] を選択し、そのユーザー インターフェイスの下部にある [保存] をクリックします。

hcspec-mgmt
×

hcspec

名前

hcspec-mgmt

サブネット アドレス範囲 * ⓘ

すべて選択

Microsoft.AzureActiveDirectory

Microsoft.AzureCosmosDB

Microsoft.CognitiveServices

Microsoft.ContainerRegistry

Microsoft.EventHub

Microsoft.KeyVault

Microsoft.ServiceBus

Microsoft.Sql

Microsoft.Storage

Microsoft.Web

サービスのフィルター

Microsoft.Sql

サービス	状態	
Microsoft.Sql	成功	

サブネットの委任

サブネットをサービスに委任 ⓘ

なし

保存

キャンセル

⑥ VNet でローカル Active Directory 仮想マシンを設定する

次に、仮想マシンを作成し、PoC で使用するローカル Active Directory ドメインおよびドメイン コントローラとして構成します。

Horizon Cloud on Microsoft Azure PoC 環境に Active Directory ドメインが必要な理由：

- 基本的に、VDI ソリューションはエンド ユーザーに仮想 Windows デスクトップを提供することを目的としています。
- 従来、IT 部門は Microsoft Active Directory を使用して、組織のユーザーと IT 部門が発行する Windows コンピュータ（デスクトップ）に関する情報を保持してきました。
- したがって、Active Directory ドメインを持つことは、Horizon Cloud on Microsoft Azure のような VDI ソリューションの重要な要素です。

PoC の VNet でローカル PoC Active Directory マシンを作成することで、このマシンは、PoC 環境が VNet での名前解決に必要とする DNS（ドメイン名サービス）も提供します。

手順

- 1 Azure ポータルの上部の検索バーで、「**Virtual machines**」と入力して [仮想マシン] アイコンを表示します。この [仮想マシン] アイコンをクリックします。

[仮想マシン] をクリックすると、ポータルに [仮想マシン] ペインが表示されます。



サブスクリプション フィルタが PoC のサブスクリプションに設定されていることを確認し、[作成] をクリックします。



- 2 [Azure 仮想マシン] を選択します。



このアクションにより、[仮想マシンの作成] ウィザードが開始されます。

次のスクリーンショットは、本書の執筆時点で確認した内容を示しています。サイド スクロール バーに表示されているように、ウィザードのユーザー インターフェイスの下部にはさらに追加の項目があります。

すべてのサービス > Virtual Machines >

仮想マシンの作成

基本 ディスク ネットワーク 管理 詳細 タグ 確認および作成

Linux または Windows を実行する仮想マシンを作成します。Azure Marketplace からイメージを選択するか、独自のカスタマイズされたイメージを使用します。[基本] タブに続いて [確認と作成] を完了させて既定のパラメーターで仮想マシンをプロビジョニングするか、それぞれのタブを確認してフルカスタマイズを行います。 [詳細情報](#)

プロジェクトの詳細

デプロイされているリソースとコストを管理するサブスクリプションを選択します。フォルダーのようなリソース グループを使用して、すべてのリソースを整理し、管理します。

サブスクリプション * ①

リソース グループ * ①
[新規作成](#)

インスタンスの詳細

仮想マシン名 * ①

地域 * ①

可用性オプション ①

セキュリティの種類 ①

イメージ * ①
[すべてのイメージを表示 | VM の世代の構成](#)

Azure スポット インスタンス ①

サイズ * ①
[すべてのサイズを表示](#)

管理者アカウント

ユーザー名 * ①

パスワード * ①

[確認および作成](#) < 前へ 次: ディスク >

3 PoC Active Directory サーバでは、必須とマークされたフィールド（ポータルでアスタリスクの付いたフィールド）に対して次の項目を選択し、オプションの項目はポータルで使用されるデフォルトのままにします。

- [サブスクリプション] - PoC 環境のサブスクリプションに設定されていることを確認します。
- [リソース グループ] - [新規作成] をクリックし、選択した名前 **POC-AD** を入力します。
- [仮想マシン名] - **POC-AD** と入力します。
- [リージョン] - PoC VNet と同じリージョンを選択します (**West-US3**)。

以下は、この時点での選択内容を示しています。次の項目セットを選択するには、下にスクロールし続ける必要があります。

[すべてのサービス](#) > [Virtual Machines](#) >

仮想マシンの作成 ...

▲ 基本オプションを変更すると、選択した内容がリセットされることがあります。仮想マシンを作成する前に、すべてのオプションを確認してください。

基本 ディスク ネットワーク 管理 詳細 タグ 確認および作成

Linux または Windows を実行する仮想マシンを作成します。Azure Marketplace からイメージを選択するか、独自のカスタマイズされたイメージを使用します。[基本] タブに続いて [確認と作成] を完了させて既定のパラメーターで仮想マシンをプロビジョニングするか、それぞれのタブを確認してフルカスタマイズを行います。 [詳細情報](#)

プロジェクトの詳細

デプロイされているリソースとコストを管理するサブスクリプションを選択します。フォルダーのようなリソース グループを使用して、すべてのリソースを整理し、管理します。

サブスクリプション * ①	HCS-Dev-Beijing
リソース グループ * ①	(新規) HCSPOC-AD 新規作成

インスタンスの詳細

仮想マシン名 * ①	POC-AD
地域 * ①	(US) East US
可用性オプション ①	インフラストラクチャ冗長は必要ありません
セキュリティの種類 ①	Standard
イメージ * ①	Windows Server 2019 Datacenter - Gen1 すべてのイメージを表示 VM の世代の構成
Azure スポット インスタンス ①	<input type="checkbox"/>
サイズ * ①	Standard_D2s_v3 - 2 vcpu 数、8 GiB のメモリ (54,75 \$/月) すべてのサイズを表示

- [イメージ] - 本書の執筆時点では、仮想マシンに [第1世代] を指定できます。これは PoC であり、比較的存在期間が短いため、低い世代の仮想マシンを使用し、[サイズ] メニューで低コストの仮想マシンサイズを選択できるようにします。

まず、[仮想マシン世代の構成] をクリックして、[第1世代] を選択できるユーザー インターフェイスを表示し、選択内容を [イメージ] フィールドに適用します。

すべてのサービス > Virtual Machines >

仮想マシンの作成

基本 オプションを変更すると、選択した内容がリセットされることがあります。仮想マシンを作成する前に、すべてのオプションを

基本 ディスク ネットワーク 管理 詳細 タグ 確認および作成

Linux または Windows を実行する仮想マシンを作成します。Azure Marketplace からイメージを選択するか、独自のカスタマイズされたイメージを使用します。(基本) タブに続いて [確認と作成] を完了させて既定のパラメーターで仮想マシンをプロビジョニングするか、それぞれのタブを確認してフル カスタマイズを行います。 [詳細情報](#)

プロジェクトの詳細

デプロイされているリソースとコストを管理するサブスクリプションを選択します。フォルダーのようなリソース グループを使用して、すべてのリソースを整理し、管理します。

サブスクリプション *

リソース グループ *

インスタンスの詳細

仮想マシン名 *

地域 *

可用性オプション

セキュリティの種類

イメージ *

Azure スポットインスタンス

VM の世代の構成

仮想マシンの世代

第1世代と第2世代のどちらの仮想マシンを作成するかは、仮想マシンの展開に使用するゲストオペレーティングシステムとブート方法に依存します。第1世代の仮想マシンは、ほとんどのゲストオペレーティングシステムをサポートしています。第2世代の仮想マシンは、ほとんどの64ビットバージョンのWindowsと、最新バージョンのLinuxおよびFreeBSDオペレーティングシステムをサポートしています。 [詳細情報](#)

VM の世代 *

第1世代

第2世代

[第1世代] を適用した後、[すべてのイメージを表示] をクリックして、ポータル の [イメージの選択] ペインに移動し、[Windows Server] タイルを見つけます。このタイルの [選択] メニューを使用して [Windows Server 2019 Datacenter - Gen1] を探します。

ホーム > Virtual Machines > 仮想マシンの作成 >

イメージの選択 ...

The screenshot displays the Azure Marketplace interface. On the left, a sidebar contains navigation options: 'その他のアイテム' (Other items) with sub-items 'マイ イメージ' (My images), '共有イメージ' (Shared images), and 'コミュニティ イメージ (プレビュー)' (Community images (preview)); 'Marketplace' with sub-items 'すべて' (All), '最近作成' (Recently created), and 'プライベート製品' (Private products); and 'カテゴリ' (Categories) with 'Compute (1605)' selected, along with 'Web (974)' and '管理ツール (955)'. The main area is titled 'Marketplace' and features a search bar with the text 'Marketplace を検索'. Below the search bar, there is a checkbox for 'Azure 特典の対象のみ' (Only Azure benefits eligible) and a notification: '1個の選択されたフィルターがある Compute 内の 1605'. The search results are displayed in a grid. The first result, 'Windows Server', is highlighted with a green border. It is a Microsoft Virtual Machine image for Windows Server. A green arrow points from the search bar to this image, and another green arrow points to the '選択' (Select) button at the bottom of the image card. The '選択' button has a dropdown arrow next to it.

次のスクリーンショットは、本書の執筆時点で確認したリストを示しています。

すべてのサービス > Virtual Machines >

仮想マシンの作成 ...

⚠ 基本オプションを変更すると、選択した

基本 ディスク ネットワーク 管

Linux または Windows を実行する仮想マシン
サイズされたイメージを使用します。[基本]
ジョニングするか、それぞれのタブを確認

プロジェクトの詳細

デプロイされているリソースとコストを管
使用して、すべてのリソースを整理し、管

サブスクリプション * ⓘ

リソースグループ * ⓘ

インスタンスの詳細

仮想マシン名 * ⓘ

地域 * ⓘ

可用性オプション ⓘ

セキュリティの種類 ⓘ

イメージ * ⓘ

Azure スポット インスタンス ⓘ

最近使用

- Windows Server 2019 Datacenter - Gen1
- Windows 10 Pro, version 21H2 - Gen2
- Windows 10 Pro (ZH-CN), version 21H2 - Gen2
- Windows Server 2019 Datacenter (zh-cn) - Gen1
- Windows Server 2019 Datacenter - Gen2

開始するための Marketplace イメージ

- Ubuntu Server 20.04 LTS - Gen2
- Ubuntu Server 18.04 LTS - Gen2
- SUSE Enterprise Linux 15 SP3 +Patching - Gen2
- Red Hat Enterprise Linux 8.2 (LVM) - Gen2
- Oracle Linux 8.5 (LVM) - Gen2
- Debian 11 "Bullseye" - Gen2
- CentOS-based 7.9 - Gen2
- Windows Server 2022 Datacenter: Azure Edition - Gen2
- Windows Server 2019 Datacenter - Gen2
- Windows Server 2016 Datacenter - Gen2

すべてのイメージを表示 | VM の世代の構成

リストから、PoC Active Directory サーバ仮想マシンに対して [Windows Server 2019 Datacenter - x64 Gen 1] を選択します。これを選択する理由は、以前別の状況でこの Windows Server 2019 Datacenter を選択して使用し、PoC の目的に十分に適していると思われるためです。

- [サイズ] - [Standard_A1_v2] を選択します。本書の執筆時点では、Microsoft Azure は、これを対象のサブスクリプションとリージョンの Gen 1 イメージで使用できるようにしています。この仮想マシン サイズを選択する理由の1つは、これが PoC であり、本書の執筆時点では、この仮想マシン サイズは、大規模なサイズよりも1か月あたりのコストが少ないためです。もう1つの理由は、以前にこのサイズを他の PoC で使用したことがあり、それらの PoC で問題なく実行できたためです。

以下は、ポータルがインスタンスの詳細として参照する前述のフィールドの選択を示しています。次の項目セットを選択するには、下にスクロールし続ける必要があります。

表示される1か月あたりのコストは、サブスクリプションタイプに対して Azure が計算する内容、選択したリージョン、および Azure によって利用可能になるものによって異なります。

すべてのサービス > Virtual Machines >

仮想マシンの作成

▲ 基本オプションを変更すると、選択した内容がリセットされることがあります。仮想マシンを作成する前に、すべてのオプションを確認してください。

プロジェクトの詳細
 デプロイされているリソースとコストを管理するサブスクリプションを選択します。フォルダーのようなリソース グループを使用して、すべてのリソースを整理し、管理します。

サブスクリプション * ⓘ

リソース グループ * ⓘ
[新規作成](#)

インスタンスの詳細

仮想マシン名 * ⓘ

地域 * ⓘ

可用性オプション ⓘ

セキュリティの種類 ⓘ

イメージ * ⓘ
[すべてのイメージを表示 | VM の世代の構成](#)

Azure スポットインスタンス ⓘ

サイズ * ⓘ
[すべてのサイズを表示](#)

管理者アカウント

ユーザー名 * ⓘ

❗ 値を空にすることはできません。

- [管理者アカウント] - 仮想マシンの作成時にサーバ オペレーティング システムにログインする管理者アカウントの情報を入力します。

画面のプロンプトに従います。Azure ポータルでは、管理者名とパスワードが遵守すべき条件について説明します。

- [受信ポート ルール] - [なし] を選択します。後で、Azure Bastion の使用を構成し、仮想マシンのシステムにログインして Active Directory ドメインを構成できるようにします。
- [ライセンス] - 適格な Windows Server ライセンスを持っている場合は、それを使用することを選択できます。この PoC では使用しないため、オフのままにしました。

次の手順に進む前に、入力したフィールドの図を次に示します。

すべてのサービス > Virtual Machines >

仮想マシンの作成

パスワード* ①

✖ 値を空にすることはできません。
✖ 値の長さは 12 ~ 123 文字にする必要があります。

パスワードの確認* ①

受信ポートの規則

パブリック インターネットからアクセスできる仮想マシン ネットワークのポートを選択します。[ネットワーク] タブで、より限定的または細かくネットワーク アクセスを指定できます。

パブリック受信ポート* ① なし
 選択したポートを許可する

受信ポートを選択

i インターネットからのすべてのトラフィックは、既定でブロックされます。受信ポートのルールは、[VM] > [ネットワーク] ページから変更できます。

ライセンス

Azure ハイブリッド特典を使用すれば、既に所有しているライセンスで最大 49% 節約できます。 [詳細情報](#)

既存の Windows Server ライセンスを使用しますか?* ①

[Azure ハイブリッド特典のコンプライアンスを確認します](#)

[確認および作成](#) [< 前へ](#) [次: ディスク >](#)

- 4 [次: ディスク >] に移動します。この [ディスク] タブで、[OS ディスク タイプ] として [標準 HDD] を選択します。本書の執筆時点では、標準 HDD のコストは Azure で最も低く、このマシンを PoC のみに使用しているため、上位レベルのディスクは必要ありません。

[OS ディスク タイプ] を変更する場合を除き、他のオプションはデフォルトのままにします。

[すべてのサービス](#) > [Virtual Machines](#) >

仮想マシンの作成

基本 **ディスク** ネットワーク 管理 詳細 タグ 確認および作成

Azure VM には、1 つのオペレーティング システム ディスクと短期的なストレージの一時的ディスクがあります。追加のデータ ディスクをアタッチできます。VM のサイズによって、使用できるストレージの種類と、許可されるデータ ディスクの数が決まります。 [詳細情報](#)

ディスクのオプション

OS ディスクの種類 * ① Standard SSD (ローカル冗長ストレージ) ▼
ワークロードにとってパフォーマンスが重要な場合は、より短い待機時間、より高い IOPS と帯域幅、およびバーストのために Premium SSD ディスクを選択してください。 [詳細情報](#)

VM と共に削除 ①

ホストでの暗号化 ①

i 選択したサブスクリプションには、ホストでの暗号化が登録されていません。 [この機能の有効化に関する詳細情報](#)

暗号化の種類 * (既定) プラットフォーム マネージド キーを使用した保存時の暗号化 ▼

Ultra Disk の互換性を有効にする ①
Ultra Disk は、選択された VM サイズ Standard_D2s_v3 の可用性ゾーン 1,2,3 でサポートされています。

データ ディスク

仮想マシンに別のデータ ディスクを追加および構成したり、既存のディスクを接続したりすることができます。この VM には、一時ディスクも付属しています。

LUN	名前	サイズ...	ディスクの種類	ホストキ...	VM と共に削除 ①
新しいディスクを作成し接続する 既存のディスクの接続					

確認および作成

< 前へ

次: ネットワーク >

5 [次: ネットワーク >] に移動します。

[ネットワーク] タブで、PoC VNet と、アクティビティ **5** で PoC Active Directory 用に準備した特定のサブネットに基づいて、次の選択を行いました。

- [仮想ネットワーク] - vnet-hcspoc を選択します。
- [サブネット] - poc-adsubnet を選択します。
- [パブリック IP アドレス] - [なし] を選択します。これは、後で仮想マシンに接続する Azure Bastion の方法を使用するためです。Azure Bastion を使用する場合、仮想マシンのパブリック IP アドレスは不要です。
- [NIC ネットワーク セキュリティ グループ] - 本書の執筆時点では、Azure ではデフォルトで [基本] が選択されていました。PoC ではこれを保持します。

- [パブリック受信ポート] - 本書の執筆時点では、Azure は、この [仮想マシンの作成] ウィザードで先ほど行った [なし] の選択を反映しています。したがって、この設定を保持します。
- [仮想マシンの削除時に NIC を削除する] - このオプションを選択します。これを選択するのは、これが PoC であり、PoC の最後に仮想マシンを削除するときに、すべての仮想マシンのアーティファクトも同時に削除するためです。

前述のリスト以外では、この [ネットワーク] タブで追加の選択を行いませんでした。

次の手順に進む前に、入力したフィールドの図を次に示します。

すべてのサービス > Virtual Machines >

仮想マシンの作成

基本 ディスク **ネットワーク** 管理 詳細 タグ 確認および作成

ネットワーク インターフェイス カード (NIC) 設定を構成して仮想マシンのネットワーク接続を定義します。セキュリティグループの規則によりポートや受信および送信接続を制御したり、既存の負荷分散ソリューションの背後に配置したりすることができます。 [詳細情報](#)

ネットワーク インターフェイス

仮想マシンの作成中に、ユーザー用にネットワーク インターフェイスが作成されます。

仮想ネットワーク * ① (新規) HCSPQC-AD-vnet
[新規作成](#)

サブネット * ① (新規) default (10.3.0.0/24)

パブリック IP ① なし
[新規作成](#)

NIC ネットワーク セキュリティ グループ ① なし Basic 詳細

パブリック受信ポート * ① なし 選択したポートを許可する

受信ポートを選択 1つ以上のポートを選択してください

i インターネットからのすべてのトラフィックは、既定でブロックされます。受信ポートのルールは、[VM] > [ネットワーク] ページから変更できます。

VM が削除されたときに NIC を削除する ①

高速ネットワーク ①

確認および作成 < 前へ 次: 管理 >

- 6 残りのタブではデフォルトを保持し、新しい選択を行わないため、[レビュー + 作成] ボタンをクリックしません。



Azure は検証チェックを実行し、検証に成功すると、確認のための最終情報を表示します。スクロールバーを使用して、作成される内容のすべての情報を確認します。

次のスクリーンショットは、現状と選択肢について表示された内容を示しています。

すべてのサービス > Virtual Machines >

仮想マシンの作成

検証に成功しました

基本 ディスク ネットワーク 管理 詳細 タグ 確認および作成

次に示すコストは見積もりであり、最終的な価格ではありません。以下を使用してください: [料金計算ツール](#) (すべての価格ニーズに対応できます)。

PRODUCT DETAILS

1 X Standard D2s v3
by Microsoft
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ
0.0750 USD/hr
[Pricing for other VM sizes](#)

TERMS

By clicking "作成", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

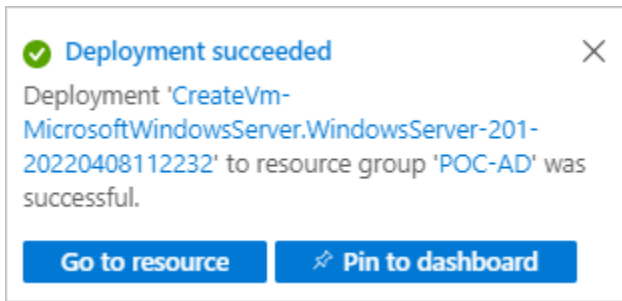
基本

サブスクリプション	HCS-Dev-Beijing
リソース グループ	(新規) HCSPOC-AD
仮想マシン名	POC-AD
地域	East US
可用性オプション	インフラストラクチャ冗長は必要ありません
セキュリティの種類	Standard
イメージ	Windows Server 2019 Datacenter - Gen1

作成 < 前へ 次へ > [Automation のテンプレートをダウンロードする](#)

7 [作成] をクリックします。

Azure は、仮想マシンと関連するすべてのアーティファクトのデプロイを開始します。デプロイに成功すると、ポータルに次のような通知が表示されます。

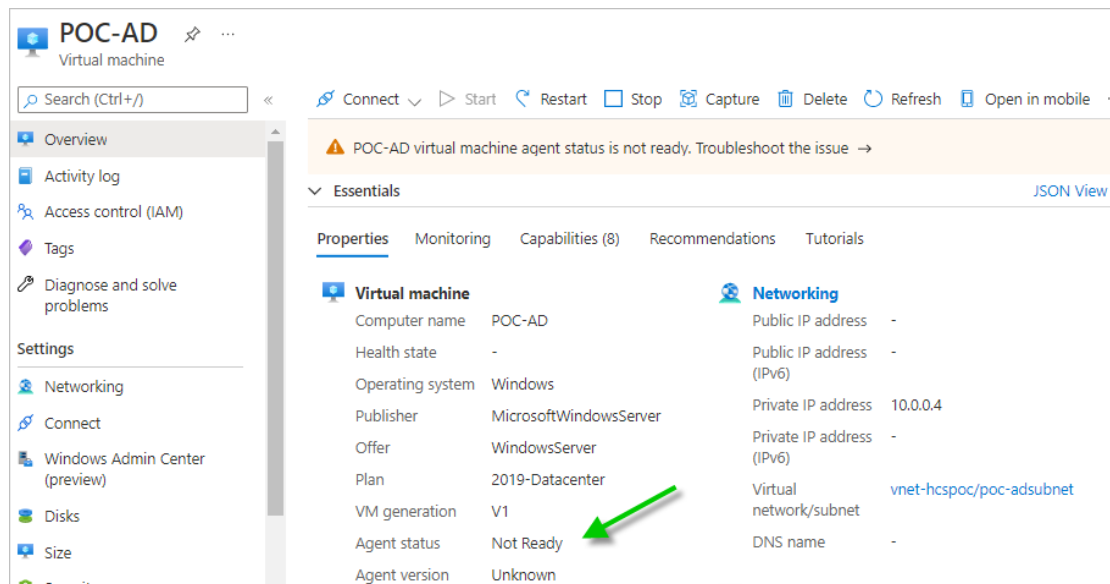


8 次に、この新しい仮想マシンにログインし、PoC Horizon Cloud on Microsoft Azure 環境の PoC Active Directory ドメインとして構成する必要があります。

- a ポータルで、新しく作成した仮想マシン（この例では POC-AD）に移動します。
- b 仮想マシンの [エージェントのステータス] に [準備完了] と表示されていることを確認します。

エージェントの準備が完了するまでは、ログインできません。このエージェントは、Azure が仮想マシンの管理に使用する Azure エージェントです。エージェントは仮想マシンのオペレーティング システムにインストールされて実行されるため、エージェントが準備完了状態になるまで数分かかる場合があります。[更新] ボタンを使用して値を更新する必要がある場合があります。

次の例では、エージェントはまだ準備ができていません。



次の例では、エージェントの準備が完了しており、仮想マシンに接続してログインできます。

接続 ▾ ▶ 開始 ↺ 再起動 □ 停止 📷 キャプチャ 🗑️ 削除 🔄 最新の情

📌 Advisor (1/1): 仮想マシンのレプリケーションを有効にして、リージョンの障害からアプリケー

▼ 基本

プロパティ 監視 機能 (8) 推奨事項 (1 個) チュートリアル

🖥️ 仮想マシン

コンピューター名	POC-AD
正常性の状態	-
オペレーティング システム	Windows (Windows Server 2019 Datacenter)
パブリッシャー	MicrosoftWindowsServer
オファー	WindowsServer
プラン	2019-Datacenter
VM の世代	V1
エージェントの状態	Ready
エージェントのバージョン	2.7.41491.1057
ホスト グループ	なし
ホスト	-
近接配置グループ	-
コロケーションの状態	該当なし
容量予約グループ	-

- 9 次に、仮想マシンに接続します。Azure Bastion 機能を使用してこの仮想マシンに接続し、必要な機能を構成します。
 - a [接続] メニューで、[Bastion] をクリックします。

🖥️ POC-AD ☆ ☆ ...
仮想マシン

🔍 検索 (Ctrl+/) << 接続 ▾ ▶ 開始 ↺ 再起

📌 概要

- 📄 アクティビティ ログ
- 👤 アクセス制御 (IAM)

RDP

SSH

Bastion

[Bastion] をクリックすると、Bastion のデプロイを選択するための画面がポータルに表示されます。次のスクリーンショットは、VNet の PoC 値に基づいた例です。

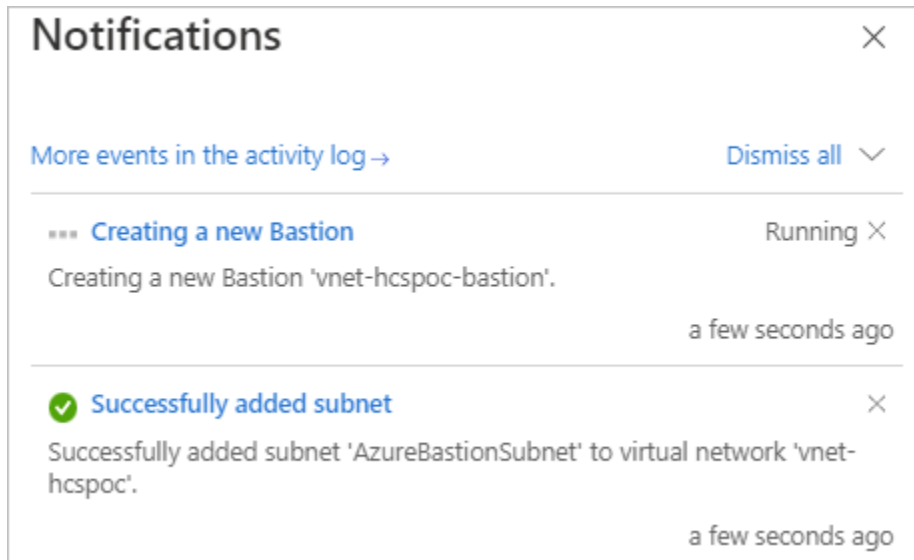


この時点から、[Bastion のデプロイ] ボタンをクリックすると、リストされた VNet とリソース (PoC の VNet と VNet のリソース グループ) に Azure Bastion が作成されます。

Bastion デプロイ プロセスでは、Azure は Bastion のサブネットを VNet に追加し、指定されたリソース グループに Bastion を作成します。

- b [Bastion のデプロイ] をクリックします。

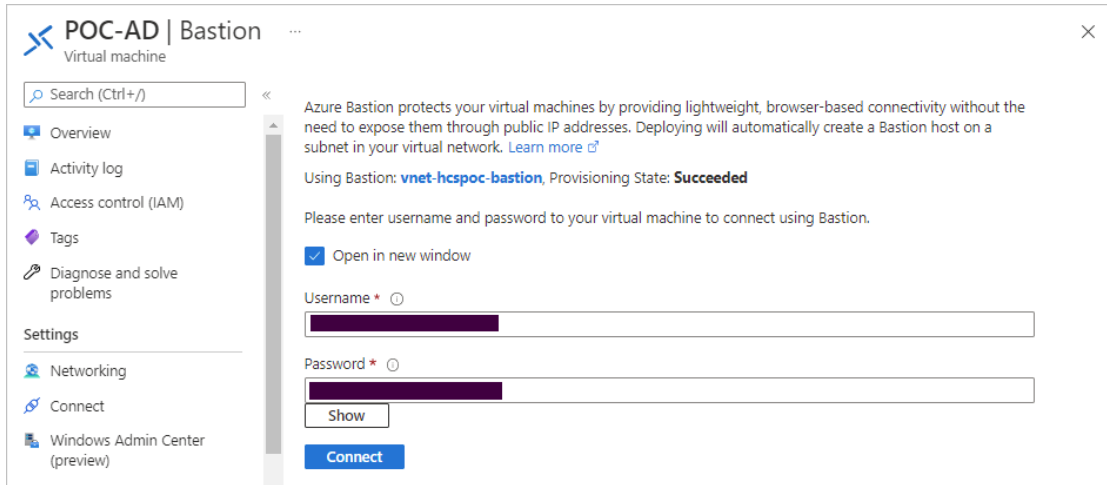
Azure は Bastion のサブネットを追加し、続いて Bastion を作成します。次のスクリーンショットは、この手順を実行したときの PoC の通知アクティビティを示しています。



Azure Bastion を使用する準備が完了すると、ポータルが表示が更新され、仮想マシンの Bastion にログインするためのユーザー インターフェイスが表示されます。

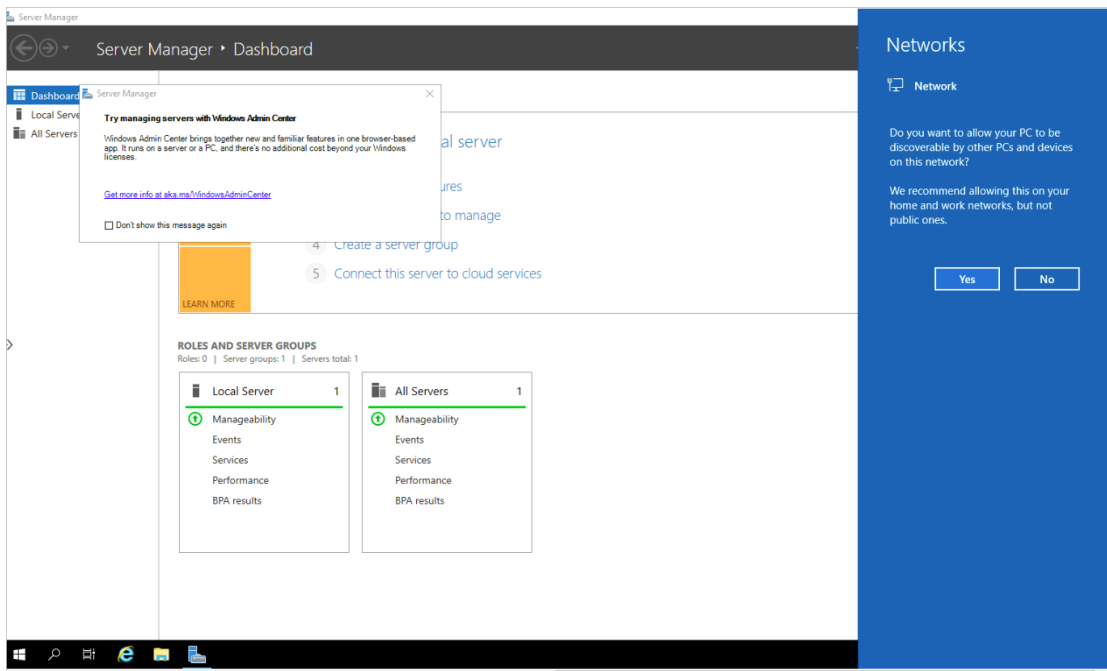
- c [仮想マシンの作成] ウィザードで仮想マシンに指定した管理者認証情報を入力し、[接続] をクリックします。

新しいウィンドウで開くためのボックスをクリアしない限り、Azure は同じブラウザ ウィンドウで接続を開始します。プライバシーのため、ここで値が編集されています。



この時点では、仮想マシンの Windows Server 2019 オペレーティング システムにログインし、スタンダード デスクトップが表示されます。

次のスクリーンショットは、この時点で PoC で確認した内容です。

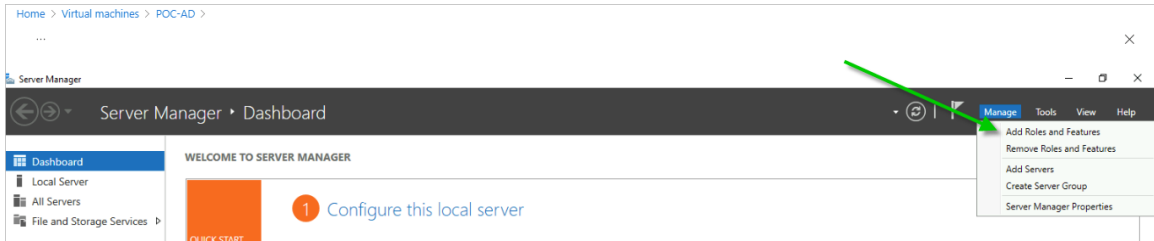


- 10 次に、この Windows Server 2019 を PoC の Active Directory ドメインおよびドメイン コントローラとして構成し、Horizon Cloud on Microsoft Azure PoC 環境に必要な管理者アカウントを追加します。

まず、[ロールと機能の追加] ウィザードを使用して、[Active Directory ドメイン サービス] ロールと必要な機能を追加します。

注： これらの手順は、Windows Server 2019 データセンターを Active Directory ドメインおよびドメイン コントローラとして構成する場合と同じです。これは、多くのインターネットの記事や Microsoft のドキュメントに記載されています。Azure クラウドに配置された仮想マシンの場合も、これらの手順に違いはありません。

- 検出可能かどうかを示す右側の青い [ネットワーク] ボックスで、[いいえ] を選択します。PoC では、この仮想マシンを検出可能にする必要はありません。
- [サーバ マネージャ - ダッシュボード] の右上の [管理] メニューで、[ロールと機能の追加] をクリックします。

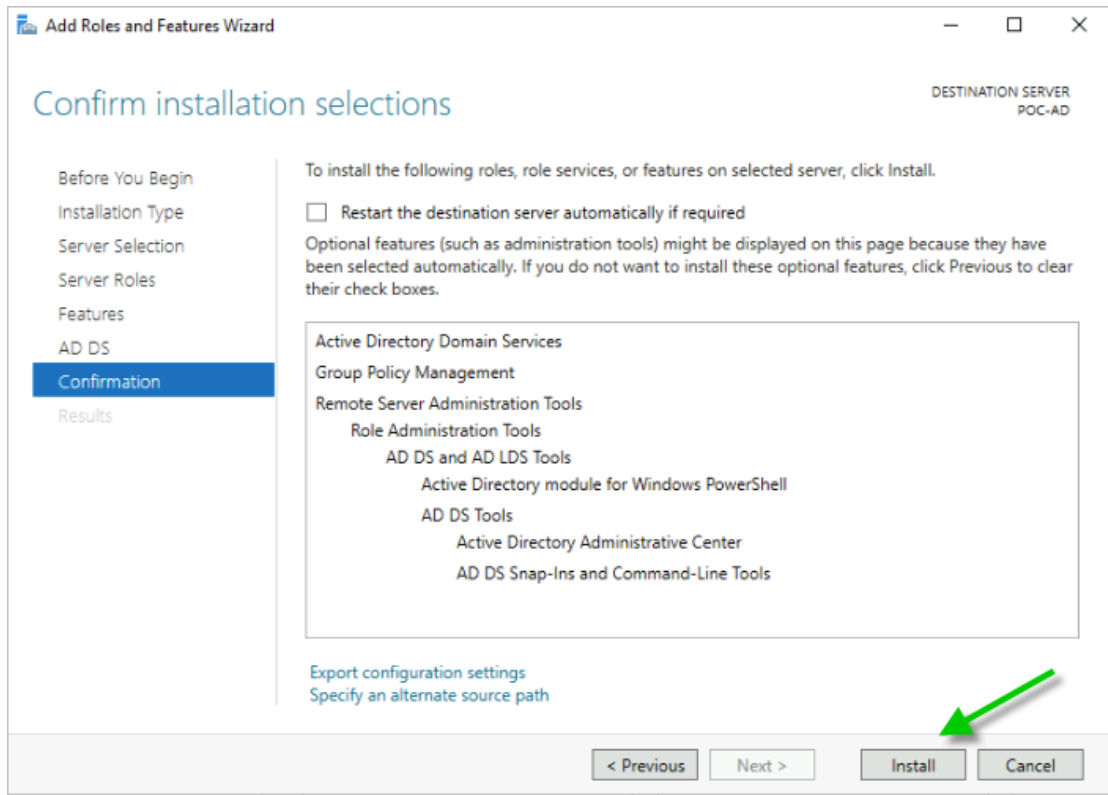


[ロールと機能の追加] ウィザードが表示されます。

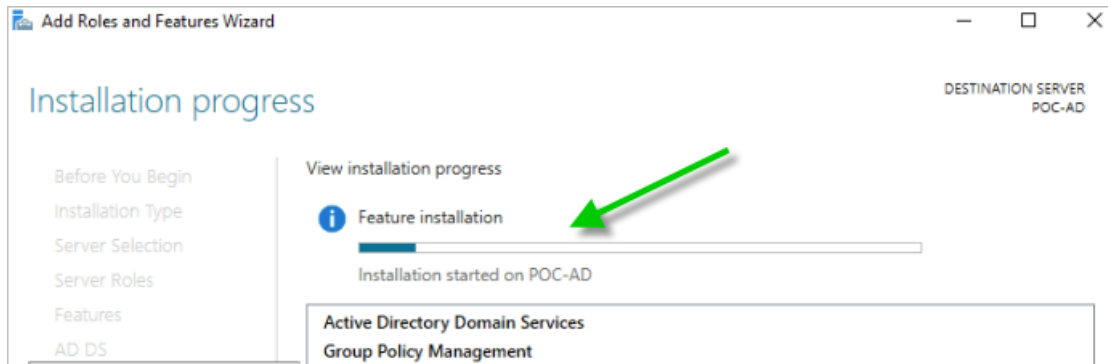
- ウィザードの指示に従い、サーバに [Active Directory ドメイン サービス] ロールとその必要な機能を構成します。
 - [ロールベースまたは機能ベースのインストール] を選択します。
 - [サーバ プールからサーバを選択する] を選択し、この手順で PoC 仮想マシンが選択されていることを確認します。ここでの名前は **POC-AD** です。
 - [Active Directory ドメイン サービス] ロールを選択します。
 - ウィザードに、必要なロール サービスまたは機能のリストのインストールに関するプロンプトが表示されたら、[機能の追加] を使用して、これらのサービスや機能も含めます。
 - ウィザードに追加機能のインストールに関する手順が表示されたら、デフォルトの選択のままにして、ウィザードの次の手順に進みます ([次へ])。
 - ウィザードの Active Directory DS の手順で、次の確認手順に進みます ([次へ])。

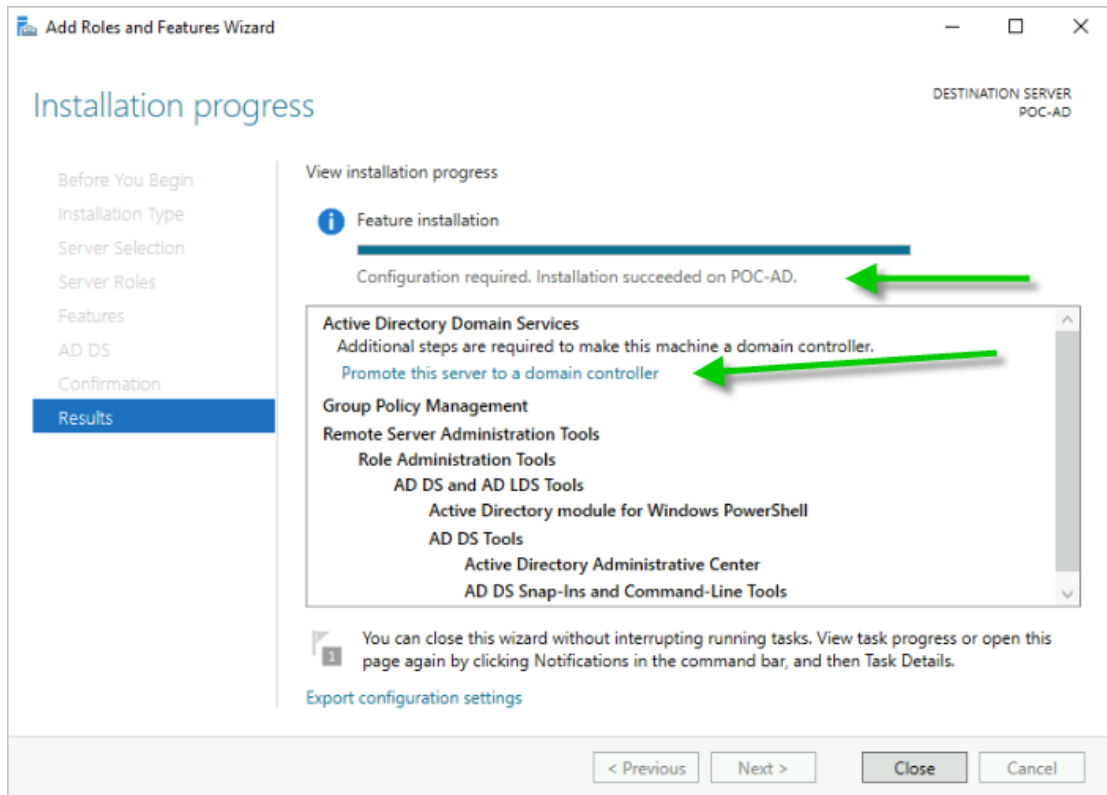
次のスクリーンショットは、ウィザードの確認手順で確認した内容を示しています。左側には、選択を実行したウィザードの手順が表示されます。

この画面では、仮想マシンへの接続を続行してインストールの実行を確認できるように、再起動に関するボックスの選択を解除します。



- [インストール] をクリックします。
 ロールのインストール アクティビティの実行が開始します。
 次のスクリーンショットは、確認した内容を示しています。





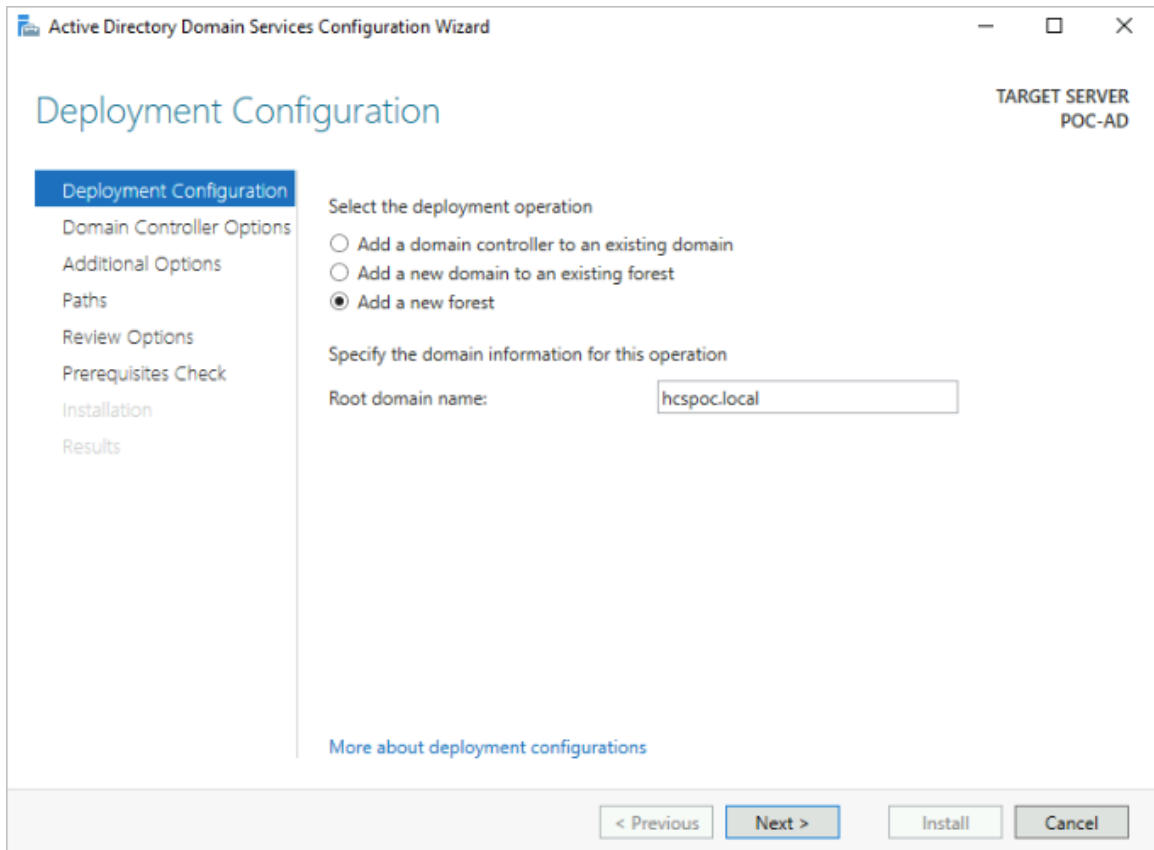
- d 次に、サーバをドメイン コントローラに昇格させます。[このサーバをドメイン コントローラに昇格させる] をクリックします。

これで、サーバをドメイン コントローラに昇格させる手順が完了します。

[ロールと機能の追加] ウィザードを閉じると、[Active Directory ドメイン サービスの構成] ウィザードが起動し、このサーバをドメイン コントローラにする値を取得します。

- a デプロイの構成で、[新しいフォレストの追加] を選択し、PoC ドメインに使用するルート ドメイン名を入力します。

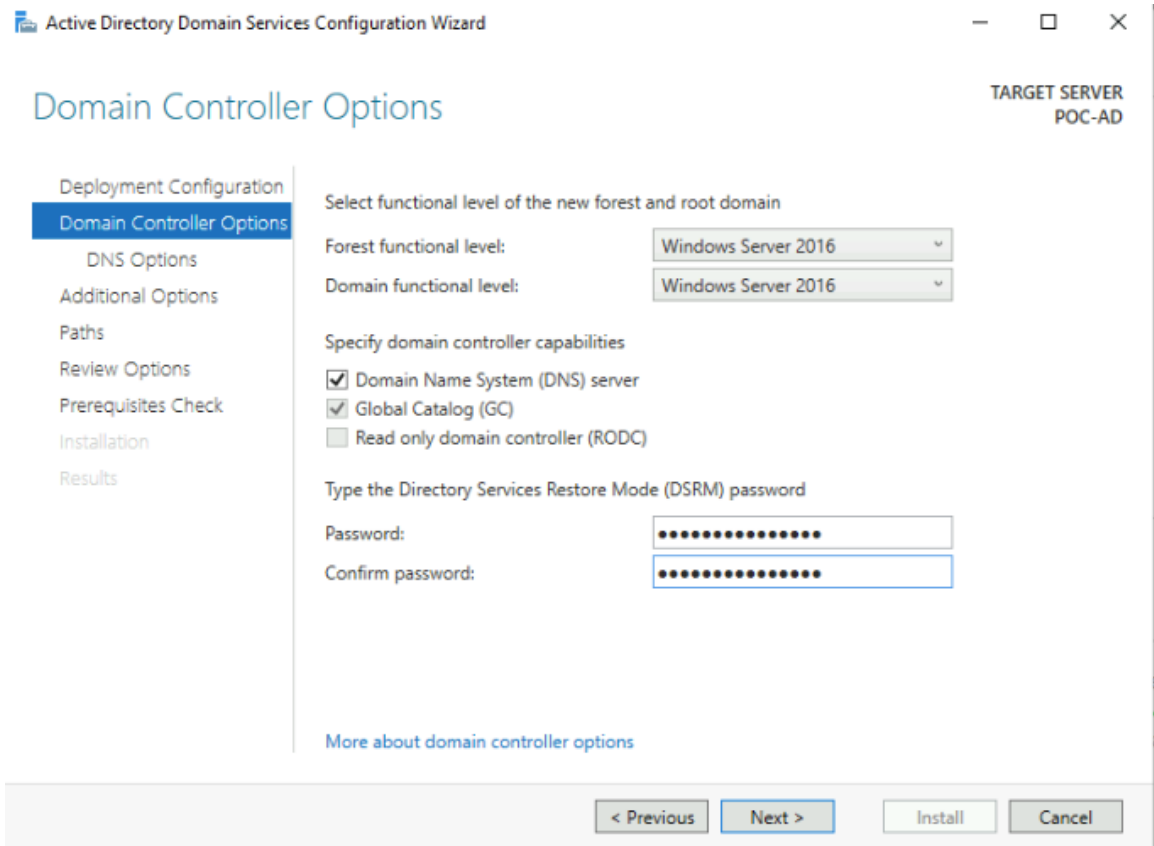
この PoC では、`hcspsc.local` を使用します。



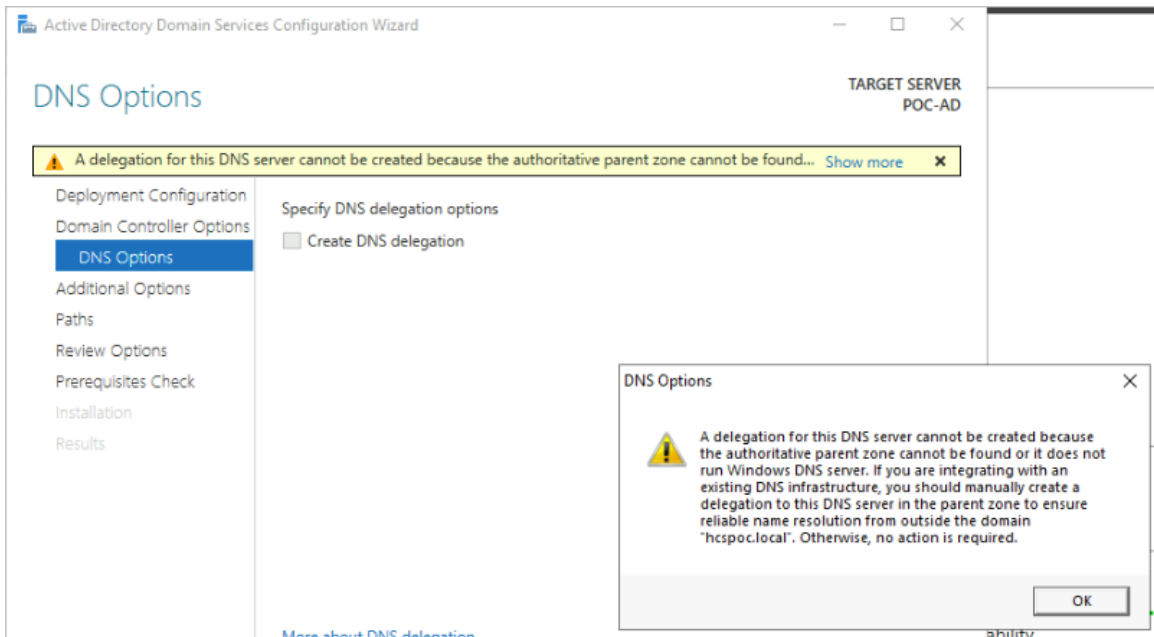
- b ウィザードの次の [ドメイン コントローラ オプション] 手順に進みます。

ここでは、フォレストおよびドメイン機能レベルに対してウィザードに表示されるデフォルトを保持し、[Domain Name System (DNS) サーバ] と [グローバル カタログ (GC)] が選択されていることを確認します (Microsoft のドキュメントによると、Microsoft は最初のドメイン コントローラにはグローバル カタログが必要であると要求しており、この場合はそれに該当します)。

また、DSRM パスワードを指定します (ウィザードで要求された場合)。



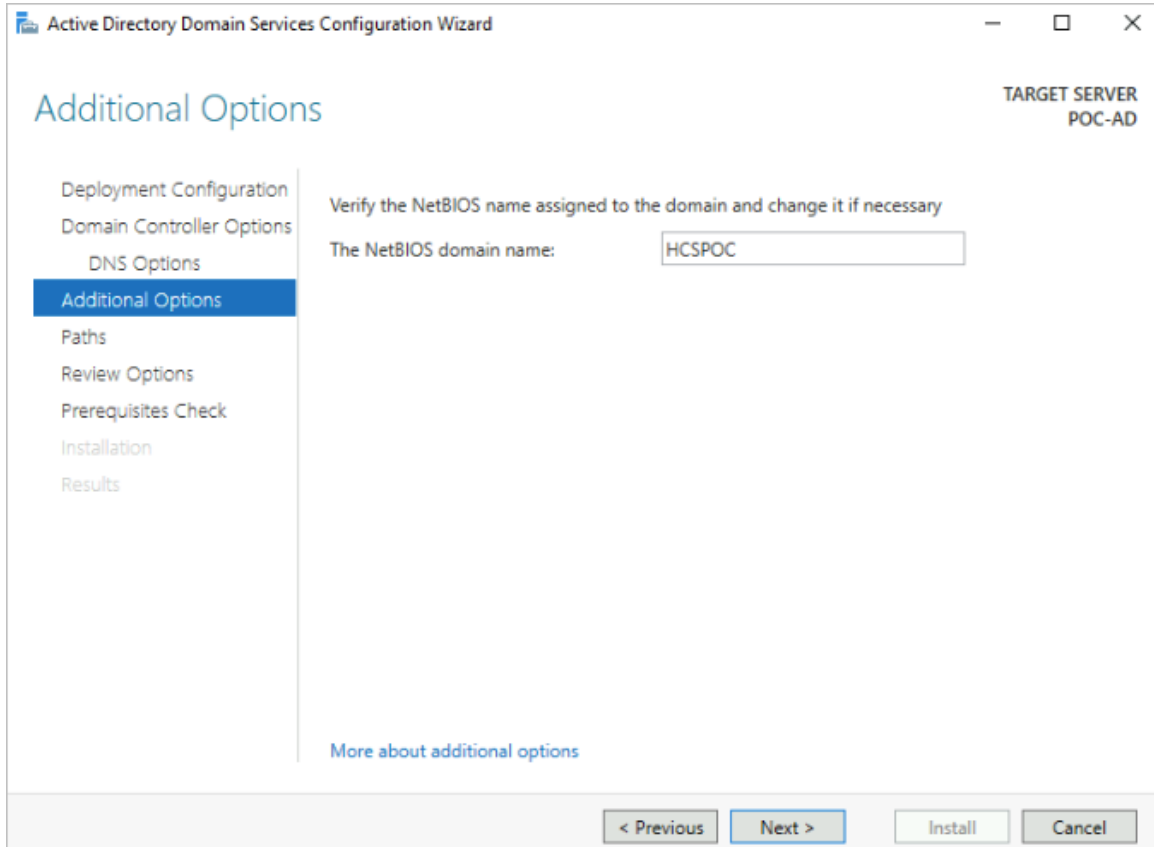
- c ウィザードの次の手順に進むと、委任を作成できない状況に関する黄色のメッセージが表示されます。詳細を表示をクリックしてメッセージ全体を読みます。



ドメイン名はわかっているため、このメッセージの理由は PoC ドメインには関係ありません。したがって、この黄色のメッセージを無視し、[次へ] をクリックして続行します。

- d 入力したドメイン名に基づいてウィザードのデフォルトの NetBIOS 名を確認し、必要に応じて変更します。

PoC ドメインでは、入力した hcspoc.local 名を基にウィザードで生成された **HCSPOC** 名をそのまま使用します。

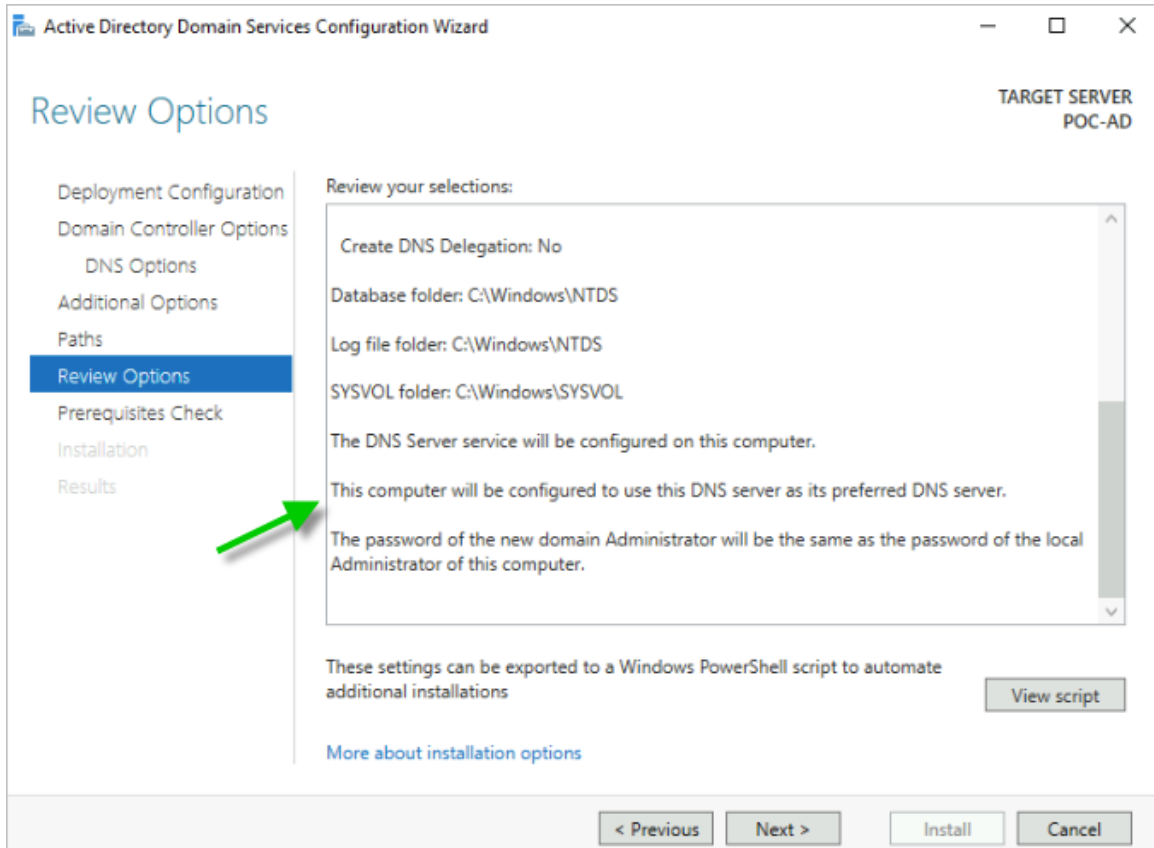


- e ウィザードの指示に従って操作を進めます。

[パス] の手順では、デフォルトを保持します。

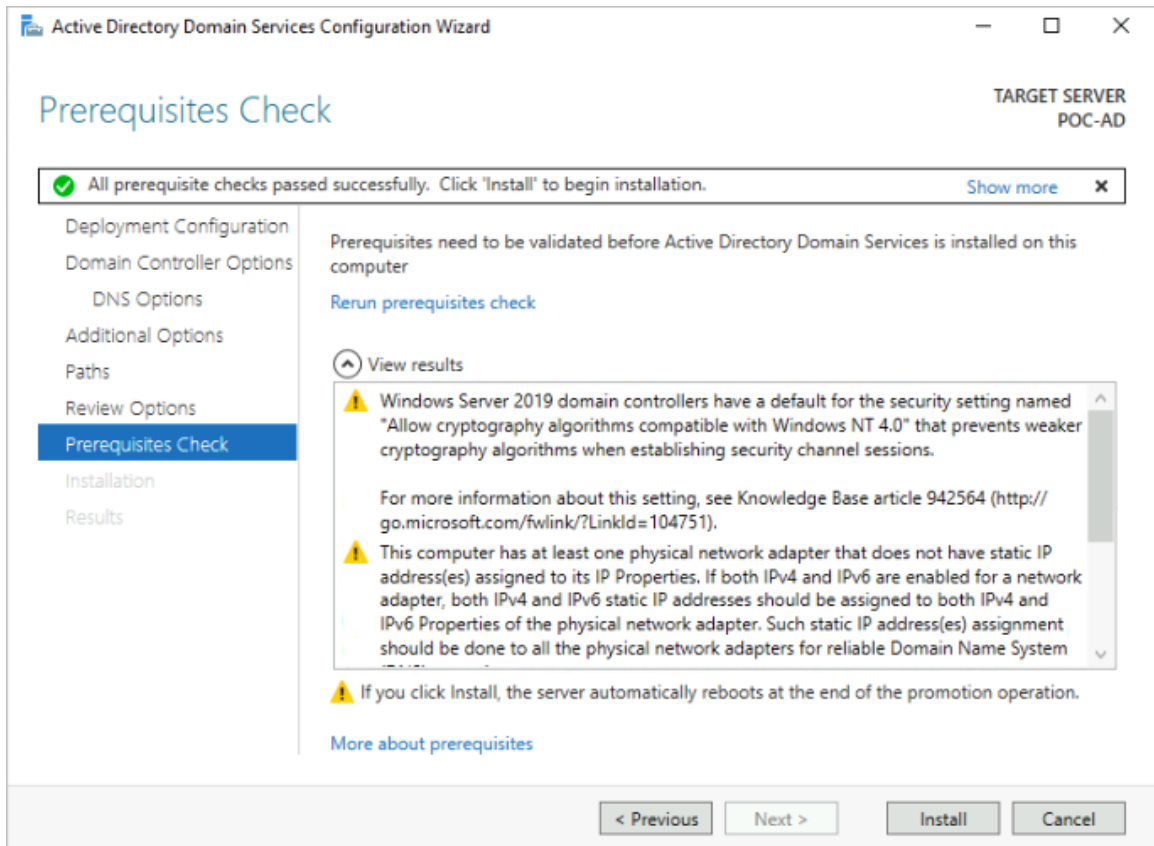
[オプションの確認] の手順で、ウィザードがこのサーバを新しいフォレストの最初の Active Directory ドメイン コントローラとして構成することを確認しました。

また、[オプションの確認] には、このコンピュータが優先 DNS サーバとして自身を使用するように構成されていることも記載されています。PoC にとって問題ないと判断しました。



- f [次へ] をクリックして、[前提条件の確認] に進みます。

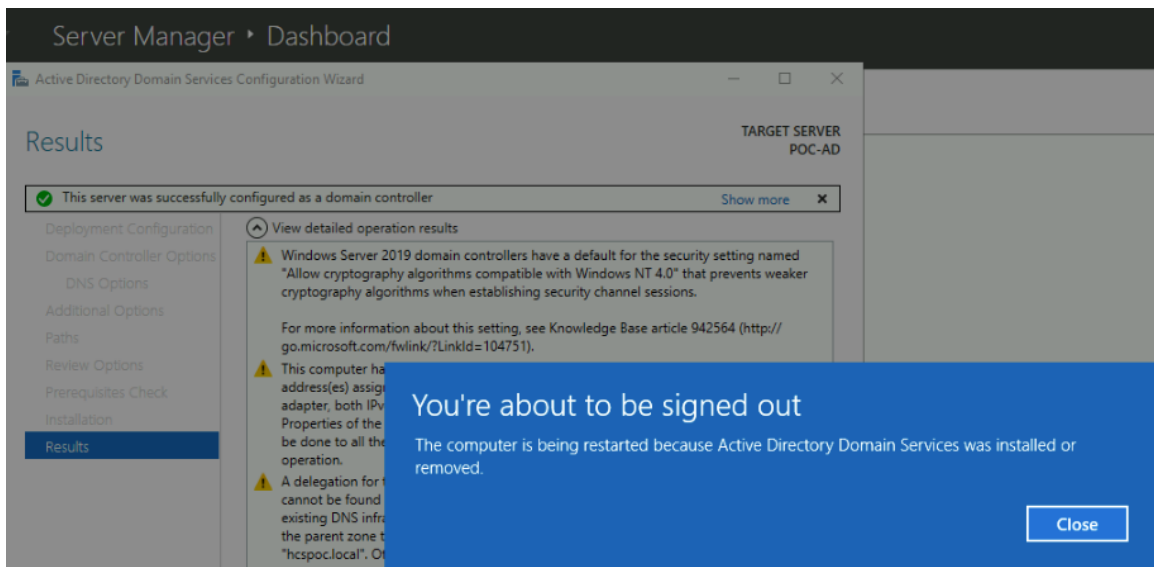
次のスクリーンショットは、表示された内容を示しています。すべての前提条件確認が正常に完了しました。すべての黄色の項目は参考情報であり、PoC では重要ではありません。



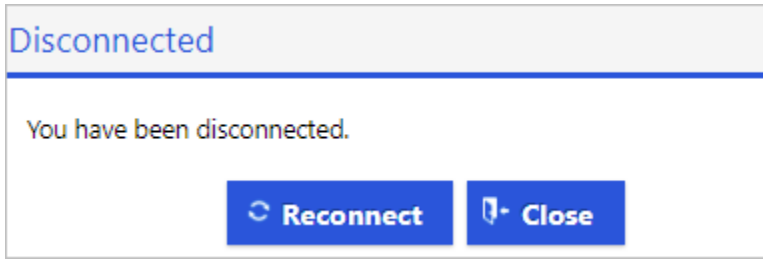
g [インストール] をクリックします。

システムがマシンの再起動が必要なポイントに達すると、[[ログアウトします]] というメッセージが表示されます。背後には、サーバが正常に構成されたことを示す結果画面が表示されます。

このメッセージの [閉じる] をクリックします。



次に、[切断されました] のメッセージで、[閉じる] を再度クリックし、マシンが起動して、Azure エージェントの準備が完了するまで Bastion 接続を閉じます。

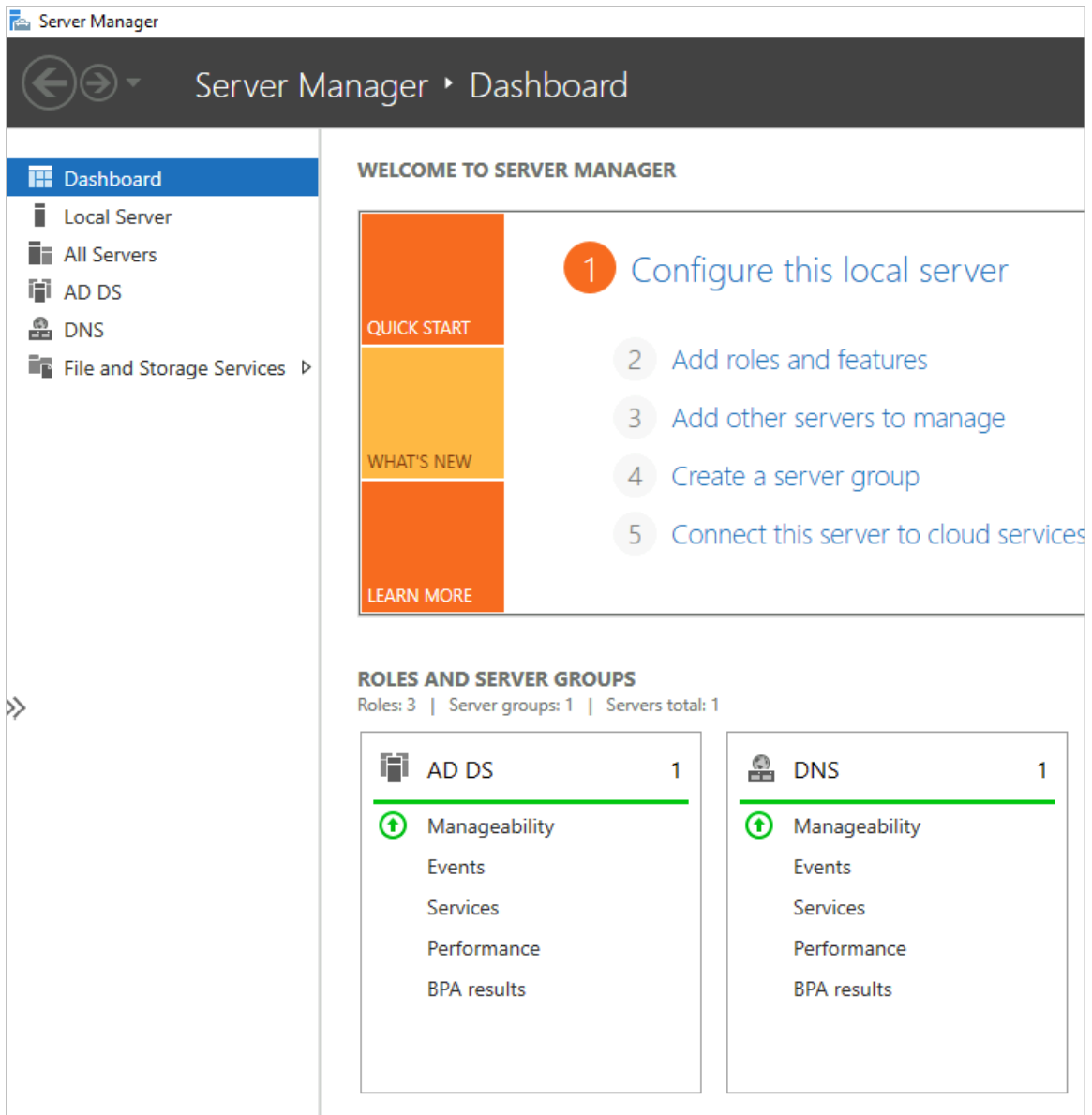


仮想マシンに再接続し、PoC が必要とする管理者アカウントを構成します

PoC Active Directory ドメイン コントローラを作成したので、PoC で使用できる 3 つのアカウントを作成する必要があります。

- a [接続] - [Bastion] を使用して仮想マシンのオペレーティング システムに再接続します。

[サーバ マネージャ - ダッシュボード] が表示されると、ダッシュボードには、構成したばかりの [Active Directory DS] および [DNS] が反映されていることがわかります。



- b 次に、ドメインに 3 つのユーザー アカウントを追加する必要があります。

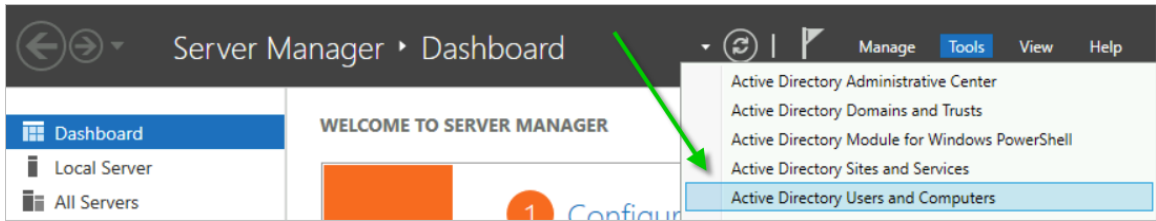
これらのユーザー アカウントは、PoC Active Directory を Horizon Cloud テナントに登録する [Horizon Cloud テナントへの PoC Active Directory の登録](#)のセクションの手順で使用されます。

簡単にするために、これは単なる PoC であるため、これらの 3 つのアカウントすべてを PoC Active Directory の標準の [Domain Admins] グループに追加します。

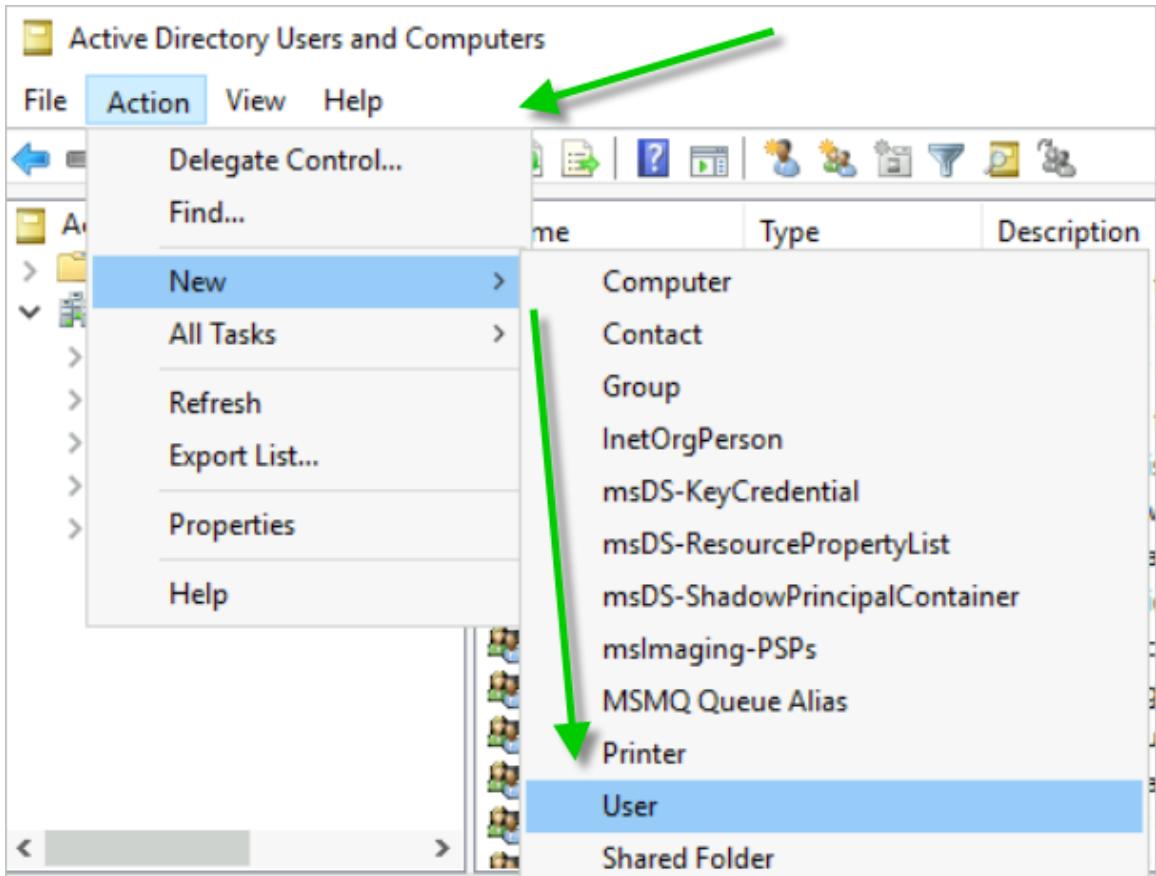
PoC では、3 つのアカウントに次の名前を付けました。

- [hcsbind1]
- [hcsbind2]
- [hcsjoin]

Active Directory ドメインへのユーザーの追加を開始するには、[サーバ マネージャ - ダッシュボード] で [ツール] - [Active Directory ユーザーとコンピュータ] をクリックします。



- c この [Active Directory ユーザーとコンピュータ] ツールで、[アクション] - [新規] - [ユーザー] をクリックします。

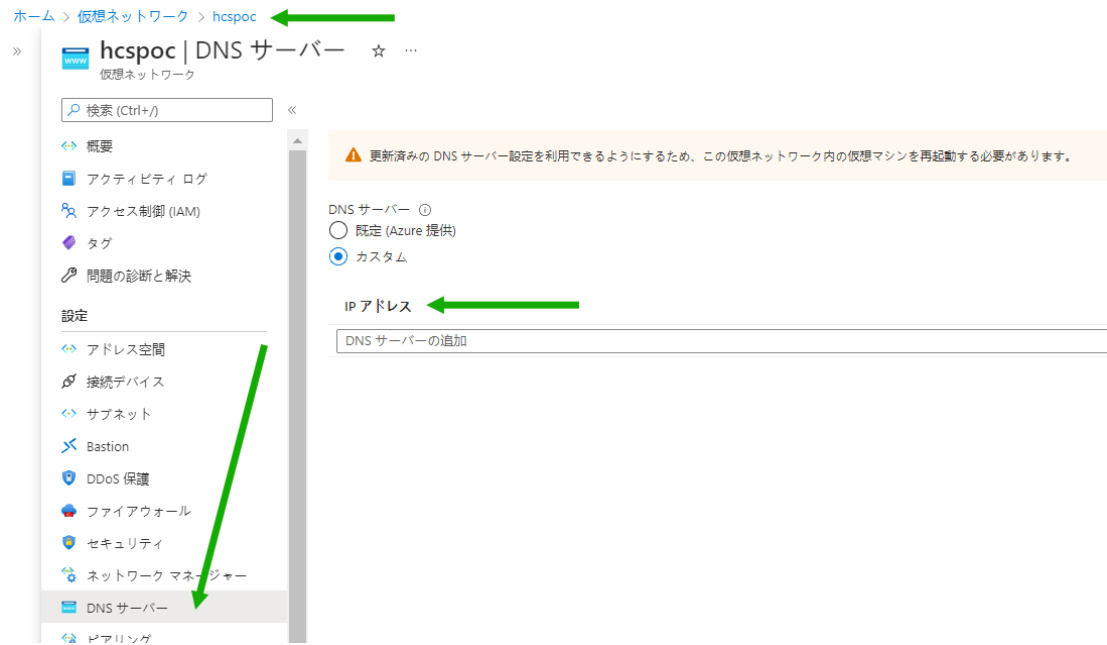


- d 最初の新しいユーザー アカウントのフィールドに入力します。
最初のユーザーに [hcsbind1] という名前を付け、[ユーザーはパスワードを変更できない] および [パスワードを無期限にする] を選択しました。
- e そのユーザーが表示されたら、[Domain Admins] グループのメンバーにします。
- f 手順 d を繰り返して、さらに 2 つのユーザーを追加します。
[hcsbind2] および [hcsjoin] という名前を付けました。
- 11 3 つのユーザー アカウントを追加したら、PoC Active Directory ドメイン仮想マシンから切断できます。
- 12 この仮想マシンは DNS サーバであるため、そのプライベート IP アドレスを VNet の DNS サーバ構成に追加する必要があります。
- a 仮想マシンの概要の詳細にある、[プライベート IP アドレス] をメモします。

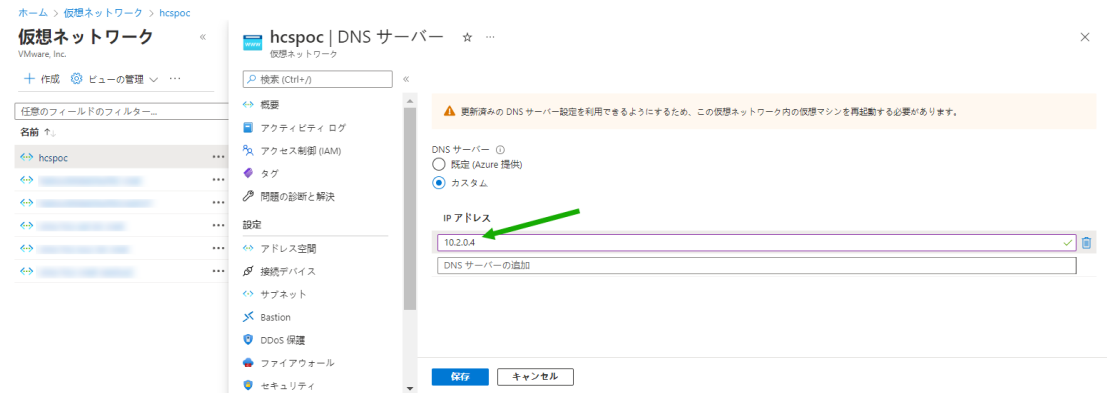
ここでの PoC 仮想マシンの場合、アドレスは 10.0.0.4 でした。



b 次に、VNet の設定とその DNS サーバ ペインに移動し、[カスタム] をクリックします。



c PoC Active Directory 仮想マシンからのプライベート IP アドレスを入力し、[保存] をクリックします。



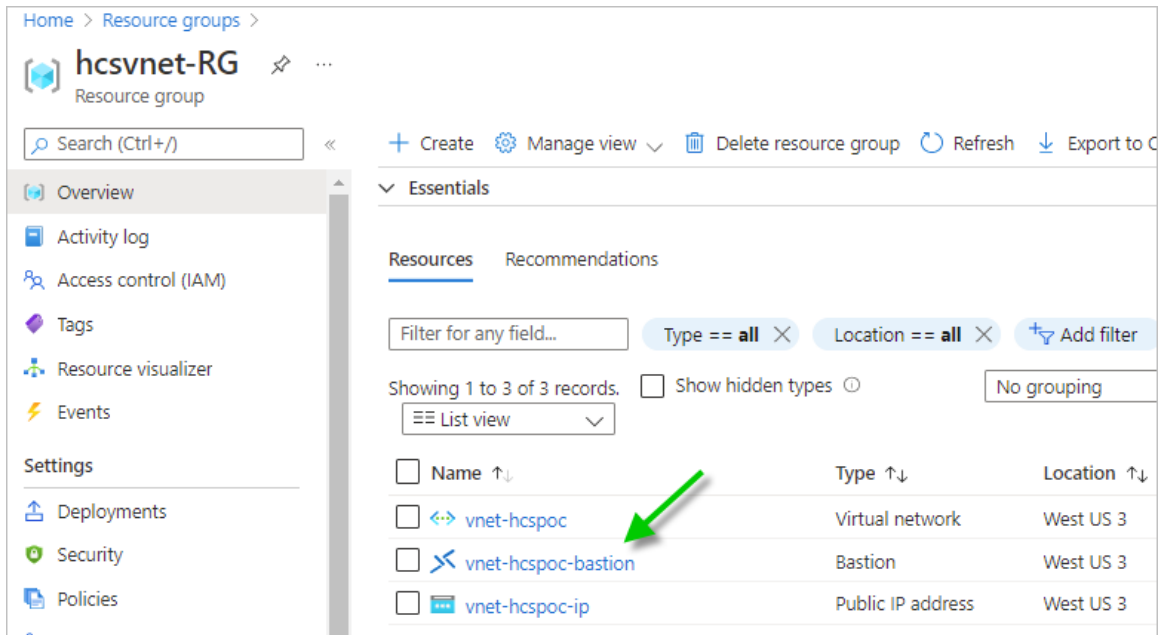
d 次に、画面上のメッセージに示されているように、PoC Active Directory 仮想マシンに移動して再起動します。

- 13 最後に、今は Active Directory 仮想マシンへの接続がなくなったので、Azure Bastion を削除して、1 時間あたりのコストが請求されないようにします。

これはオプションの手順です。Azure Bastion で発生する時間コストが気にならない場合は、それを維持することも可能です。節約のために削除することにしました。

Bastion が作成されたリソース グループに移動し、Bastion 項目を削除します。

次のスクリーンショットは、VNet のリソース グループ内の Azure Bastion が存在していた場所を示します。その Bastion をクリックして削除しました。



Azure Bastion の削除には、約 10 分かかることがあります。

Horizon Cloud テナント アカウントの取得



ログインして [ポッドの追加] ウィザードを実行する前に、クラウド テナント アカウントがすでに設定され、VMware Customer Connect アカウントに関連付けられている必要があります。

テナント アカウントを設定するための前提条件は次のとおりです。

- VMware Customer Connect アカウントまたは VMware Cloud services アカウント。
- Horizon ユニバーサル サブスクリプションなどのクラウド ホスト型サービスへのアクセスを提供するサブスクリプション。さまざまなタイプの比較については、[Horizon サブスクリプションの表](#)を参照してください。

アカウントの取得

<https://customerconnect.vmware.com> のヘッダーで [登録] アクションを使用します。

サブスクリプションの取得

クラウド ホスト型サービスへのアクセス権を提供するサブスクリプションがまだないことがわかっている場合、PoC のテナント アカウントを取得する方法の1つは、60 日間の試用版にサインアップすることです。

本書の執筆時点で、この 60 日間の評価版ライセンスに関する既知のページは <https://www.vmware.com/horizon-universal-license-trial.html> になります。

サブスクリプションがすでにあることがわかっている場合、またはサブスクリプションを持つエンタープライズアカウントに属していることがわかっている場合は、すでに設定されているクラウド テナント アカウントにアクセスできる可能性があります。

現在のステータスを確認するには、VMware ナレッジベースの記事 [KB2006985](#) の手順に従ってサービス リクエスト (SR) を発行します。現在の VMware Customer Connect のアカウント情報が必要になります。

テナントのセットアップ完了の通知

VMware がアカウントの認証情報を Horizon Cloud テナント アカウントに関連付けると、その VMware Customer Connect アカウントまたは VMware Cloud services アカウントのプロファイルにあるメールアドレスに E メールが送信されます。

その E メールを受信した場合、テナント アカウントにアクセスできることがわかります。VMware Horizon Service からの E メールがないか、迷惑メール フォルダを確認してください。

ログインと [ポッドの追加] ウィザードの実行



テナント アカウントの準備が完了したことを示す E メールがある場合は、ログインして [ポッドの追加] ウィザードを実行できま

PoC Active Directory ドメイン仮想マシンが Azure ポータルで実行されていることを確認します。前の手順の後、その仮想マシンはポッドの追加プロセスで必要となる VNet の DNS サービスを提供しています。

次の情報を収集し、以下の手順を実行するときに利用できるようにします。この情報には、前述のアクティビティで設定した内容が含まれます。

表 6-5. この手順でこれらの項目を収集し、コンソールにログインして [ポッドの追加] ウィザードを実行するときに使用します。

項目	値
name@example.com などの VMware Customer Connect アカウント。	
VMware Customer Connect アカウントのパスワード	

表 6-5. この手順でこれらの項目を収集し、コンソールにログインして [ポッドの追加] ウィザードを実行するときに使用します。 (続き)

項目	値
Azure の準備アクティビティ  からの [サブスクリプション ID]	
Azure の準備アクティビティ  からの [ディレクトリ (テナント) ID]	
Azure の準備アクティビティ  からの [アプリケーション (クライアント) ID]	
Azure の準備アクティビティ  「アプリケーション登録を作成する」からのクライアント シークレットの [値]。 以下の手順では、[サブスクリプションの管理] ユーザー インターフェイスでこれを [アプリケーション キー] として参照します。	
アクティビティ  からの VNet 名	
アクティビティ  からの mgmt サブネット名	
アクティビティ  からの vdi サブネット名	

1. VMware Customer Connect アカウントの認証情報を使用して Horizon Universal Console にログインします。

- 1 VMware Customer Connect または VMware Cloud services の認証情報を使用して Horizon Universal Console にログインします。

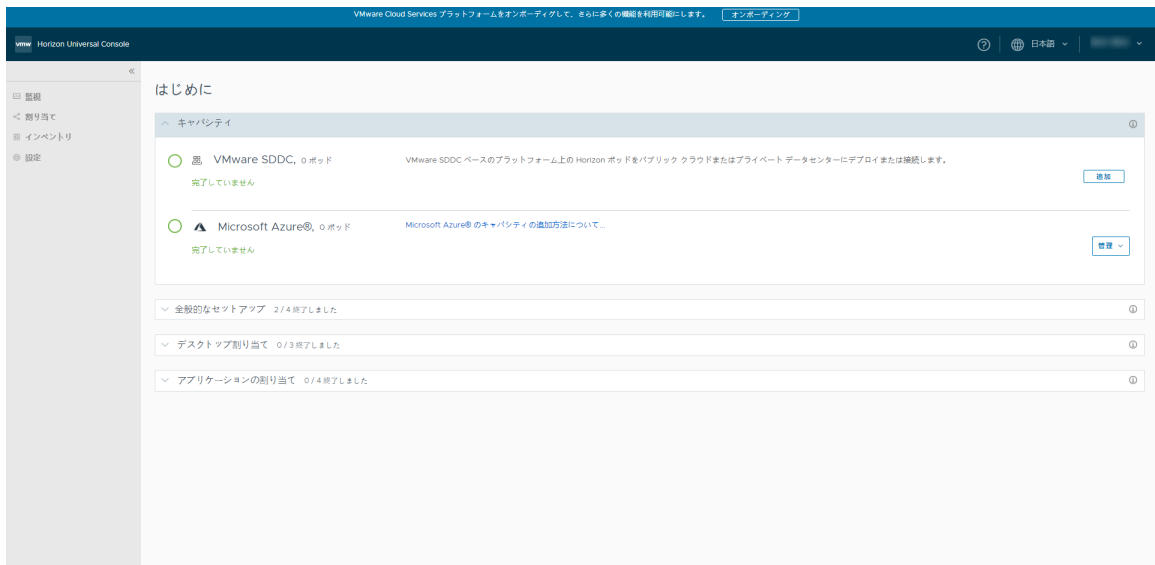
ブラウザで、<https://cloud.horizon.vmware.com> に移動します。

ログイン画面は、<https://console.cloud.vmware.com> の VMware Cloud Services ログイン ユーザー インターフェイスに自動的にリダイレクトされます。

画面上のプロンプトに従って、VMware Cloud services または VMware Customer Connect の認証情報を使用してログインします。



利用規約に同意すると、メイン コンソールに [はじめに] ページが表示されます。



このページは、すべての新しいテナントの開始点です。

ポッド環境を追加するまで、コンソールの大部分はロックされます。

ここで、PoC Horizon Cloud on Microsoft Azure 環境の作成を開始します。

2. Azure サブスクリプション情報をコンソールに追加します。

アクティビティ **4** で示すように、この情報は、サービスが API 呼び出しを使用してサブスクリプション内の環境を最初に立ち上げるために必要です。

- 1 [管理] - [サブスクリプションの管理] をクリックします。



次のユーザー インターフェイス ウィンドウが表示されます。

サブスクリプションの管理 - Microsoft Azure

アクション	追加	▼ ⓘ
サブスクリプション名 *	_____ ⓘ	
環境 *	選択	▼ ⓘ
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 *	_____ ⓘ	
アプリケーション キー *	_____ ⓘ	👁 ⓘ

- 2 サブスクリプション情報を初めて追加するので、デフォルトの [追加] アクションのままにし、コンソールでサブスクリプションを参照するために使用する名前を入力します。

この名前は、この Horizon Cloud テナントで複数の Azure サブスクリプションを使用する場合に、このサブスクリプションの値を他のサブスクリプションの値と区別するためにのみ使用されます。myhcspoc を使用しました。

[環境] には、[Azure - Commercial] を選択します。

次に、アクティビティ **4** で収集した値を残りの 4 つのフィールドにコピーします。

注: この [サブスクリプションの管理] ユーザー インターフェイスの [アプリケーション キー] フィールドは、アクティビティ **4** 「アプリケーション登録を作成する」でコピーしたクライアント シークレットの値を意味します。

表 6-6. [サブスクリプションの管理] ユーザー インターフェイスに表示されるラベルと、アクティビティ 4 の Azure ポータル名の比較

[サブスクリプションの管理] ユーザー インターフェイス	Azure ポータルでの名前	ユーザーの値
[サブスクリプション ID]	[サブスクリプション ID]	
[ディレクトリ ID]	[ディレクトリ (テナント) ID]	
[アプリケーション ID]	[アプリケーション (クライアント) ID]	
[アプリケーション キー]	クライアント シークレット キーの [値]	

次のスクリーンショットは、ここでの PoC の選択肢を示しています。プライバシーのため、値は編集されています。

サブスクリプションの管理 - Microsoft Azure ×

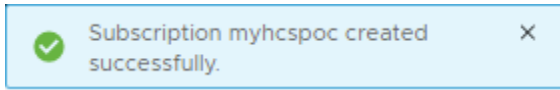
アクション	追加 ▼ ⓘ
サブスクリプション名 *	myhcspoc3 ⓘ
環境 *	Azure - Commercial ▼ ⓘ
サブスクリプション ID *	██████████████████████ ⓘ
ディレクトリ ID: *	██████████████████████ ⓘ
アプリケーション ID *	██████████████████████ ⓘ
アプリケーション キー *	██████████████████████ ⓘ

キャンセル
確認

3 必要な項目を指定したら、[確認] をクリックします。

システムは、すべての値が満足のいくものであり、アクティビティ **4** で意図したとおりに互いに結びついていることを確認し始めます。

すべての値が正しく結び付いていることがシステムで検証されると、青色の成功メッセージが一時的に表示されます。このメッセージは、値を追加した後に確認しました。



この時点で、[はじめに] ページに戻り、[ポッドの追加] ウィザードを開始できます。

3. [ポッドの追加] ウィザードを実行します。

- 1 [管理] - [ポッドの追加] をクリックします。



ウィザードのこの最初の手順では、サブスクリプション情報がすでに入力されているため、サブスクリプション名を [サブスクリプションの適用] で選択できます。

Microsoft Azure のキャパシティの追加



次のスクリーンショットは、[サブスクリプションの適用] から **hcspec** サブスクリプション名を選択したときのウィザードを示しています。このスクリーンショットでは、値が編集されています。

Microsoft Azure のキャパシティの追加 ×

1. サブスクリプション
2. ポッドのセットアップ
3. ゲートウェイ設定
4. サマリ

適用する Microsoft Azure サブスクリプションを選択するか、新しく追加してください。

ポッドのサブスクリプション

サブスクリプションの適用: myhcs poc ▾ ⓘ

サブスクリプション名: myhcs poc

環境: AZURE

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:

外部ゲートウェイに別のサブスクリプションを使用: ⓘ

キャンセル
次へ

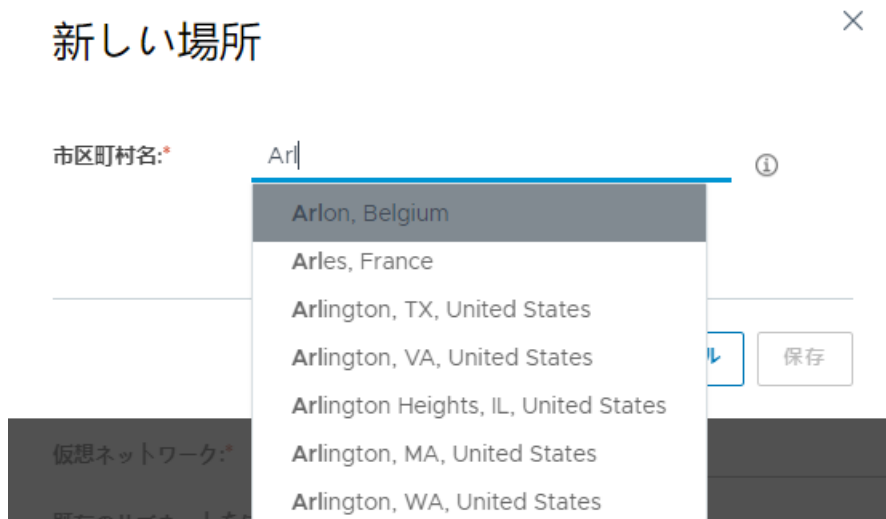
[次へ] をクリックします。

- 2 ウィザードの [ポッドのセットアップ] 手順で、[詳細] と [ネットワーク] の 2 つの主要な領域に入力します。

詳細

- [ポッド名] - コンソールに表示されるときにこのポッドに使用する名前を入力します。
(HCS-trialpod-1 を使用しました。)
- [場所] - [追加] をクリックし、[市区町村名] フィールドに市区町村名を入力します。

ここで、**Arl** と入力して、Arlington という名前を表示しました。



数文字を入力すると、システムは入力した文字と一致する名前の表示を開始するので、必要な市区町村名に最も近い名前をクリックします。(Arlington, WA, United States を選択しました。)

- [Microsoft Azure リージョン] - すべての割り当てを設定し、VNet を作成し、PoC Active Directory ドメイン仮想マシンを作成したリージョンを選択します。(West US 3 を使用しています。)

[詳細] の残りの項目はそのままにして、[ネットワーク] を完了しました。

ネットワーク

- [仮想ネットワーク] - VNet を選択します。(vnet-hcspoc を選択しました。)
- [既存のサブネットを使用] を [オン] の位置 (緑色) に切り替え、その VNet で作成したサブネットを選択します。
- [管理サブネット] - アクティビティ **5** で作成した **mgmt** サブネットを選択します。(hcspoc-mgmt を選択しました。)
- [仮想マシン サブネット - プライマリ] - アクティビティ **5** で作成した **vdi** サブネットを選択します。(hcspoc-vdi を選択しました。)
- [NTP サーバ] - ポッドの仮想マシンとの時刻同期に使用する 1 台以上の NTP サーバのリストを入力します。複数の名前を入力する場合は、カンマで区切ります。(us.pool.ntp.org という名前の NTP サーバを使用しています。)

前述の項目は、このウィザードの手順で特に設定した項目です。残りはデフォルト設定のままにします。

次のスクリーンショットは、この例を示しています。

Microsoft Azure のキャパシティの追加 ×

1. サブスクリプション
2. ポッドのセットアップ
3. ゲートウェイ設定
4. サマリ

詳細情報を入力し、ポッドを構成して接続します。

詳細

ポッド名: ⓘ

場所: ⓘ [編集](#)

Microsoft Azure リージョン: ⓘ

説明:

Azure リソース タグ:

名前	値	
		+ ⓘ

ネットワーク

仮想ネットワーク: ⓘ

既存のサブネットを使用: ⓘ

管理サブネット: ⓘ

仮想マシン サブネット - プライマリ: ⓘ

NTP サーバ: ⓘ

プロキシを使用: ⓘ

キャンセル
戻る
次へ

[次へ] をクリックします。

- 3 ウィザードの [ゲートウェイ設定] の手順で、[外部ゲートウェイを有効にしますか?] を [オフ] の位置に切り替えます。

この PoC セクションの PoC レシピの材料では、ポッドのデプロイ後にこのゲートウェイを追加できることを説明しました。ここでは、これらの選択をオフにします。

Microsoft Azure のキャパシティの追加 ×

1. サブスクリプション
2. ポッドのセットアップ
3. ゲートウェイ設定
4. サマリ

このポッドの外部および内部 Unified Access Gateway を設定します。Universal Broker の 2 要素認証が有効になっている場合、2 要素認証を使用した外部ゲートウェイが必要です。

外部ゲートウェイ

外部ゲートウェイを有効にしますか? ⓘ

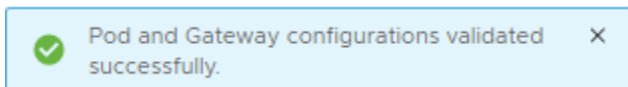
内部ゲートウェイ

内部ゲートウェイを有効にしますか? ⓘ

キャンセル
戻る
検証と続行

4 [検証と続行] をクリックします。

システムは、ウィザードに入力した内容に基づいて検証チェックを実行します。すべてがチェックされると、青いメッセージが短時間表示されます。



このデプロイのゲートウェイをオフに切り替えた場合でも、メッセージ テキストにはゲートウェイが言及されます。これは想定どおりです。

5 ウィザードの最後の [サマリ] 手順で、PoC 用に設定した正しい **mgmt** および **vdi** サブネットが一覧表示されていることを確認します。

この例の完全なビューを次に示します。

Microsoft Azure のキャパシティの追加 ×

1. サブスクリプション
2. ポッドのセットアップ
3. ゲートウェイ設定
4. サマリ

情報を送信する前に、サブスクリプションとポッドの設定の詳細を確認します。

Microsoft Azure のキャパシティのサマリ

ポッドのサブスクリプション名: myhcspec

ポッドの詳細

ポッド名:	HCS-trialpod-1	サイト	
説明:		場所:	Arlington, VA, United States
		Microsoft Azure リージョン:	West US 2

高可用性

有効: はい

ネットワーク

仮想ネットワーク:	hcspec [hcspec]	仮想マシン サブネット:	hcspec-vdi
管理サブネット:	hcspec-mgmt	NTP サーバ:	us.pool.ntp.org
プロキシを使用:	いいえ		

Azure リソース タグ

ポッドリソース タグ: -

外部ゲートウェイ

有効: いいえ

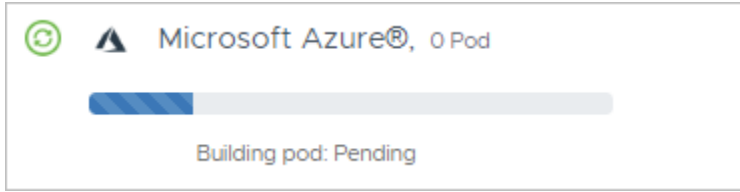
内部ゲートウェイ

有効: いいえ

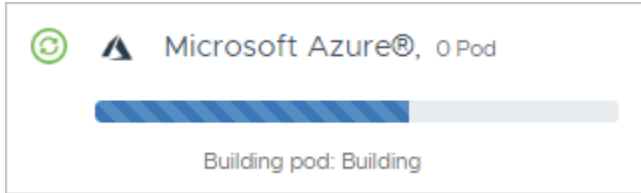
キャンセル
戻る
送信

6 [送信] をクリックします。

システムは、Azure サブスクリプションで Horizon Cloud on Microsoft Azure 環境の生成を開始します。コンソールには、以下で始まる進行状況の状態が反映されます。

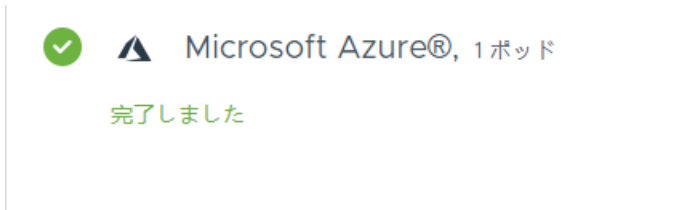


次に、以下に進みます。



Azure Cloud と Horizon Cloud 間のネットワーク トラフィックによっては、デプロイに 30 ~ 45 分かかることがあります。

プロセスが完了すると、コンソールに反映されます。



[完了] インジケータが表示されたら、次のセクションの手順を実行して、この Horizon Cloud on Microsoft Azure 環境に PoC Active Directory ドメインを登録します。

Horizon Cloud テナントへの PoC Active Directory の登録



このアクティビティによってコンソールの残りの部分のロックが解除されるため、新しい PoC Horizon Cloud on Microsoft Azure を開始して Day-2 タスクを開始する前に、このアクティビティを完了する必要があります。

このアクティビティを簡単に完了できるように、PoC Active Directory ドメイン仮想マシンを設定しました。

- 1 コンソールの [はじめに] ページでデプロイが成功したことを確認したら、[全般的なセットアップ] を展開して [Active Directory] 行を表示します。

その行で [構成] をクリックします。



- 2 [Active Directory の登録] ウィンドウで、アクティビティ **6** で作成された PoC Active Directory ドメインとユーザーに関する必要な情報を入力します。

必要な情報は、PoC Active Directory ドメインの NetBIOS 名、DNS ドメイン名、およびこの目的のためにセットアップされた Active Directory ユーザーの短い名前とパスワードです。

PoC 値は、**HCSPoC** の NetBIOS 名、DNS ドメイン名 **hcs poc.local1**、および **hcsbind1** と **hcsbind2** という名前の 2 つのユーザーです。次のスクリーンショットは、ここの入力を示しています。

Active Directory の登録 ×

Active Directory のドメイン情報とドメイン バインド アカウントの認証情報を指定します。プライマリおよび補助ドメイン バインド アカウントには、リカバリのためにスーパー管理者アクセス権が自動的に付与されます。

NetBIOS 名: [*]	SKYLO ①
DNS ドメイン名: [*]	skylo.local ①
プロトコル: [*]	LDAP ①
バインド ユーザー名: [*]	vmware ①
バインド パスワード: [*] ①
補助アカウント番号 1	①
バインド ユーザー名: [*]	vmware2 ①
バインド パスワード: [*] ①

[詳細プロパティ](#)

キャンセル
ドメイン バインド

[ドメイン バインド] をクリックします。

情報が保存され、[ドメイン参加] ウィンドウが表示されます。

- 3 [ドメイン参加] ウィンドウで、アクティビティ **6** で作成された PoC Active Directory 仮想マシンの IP アドレスと 3 番目の Active Directory ユーザーの認証情報を入力します。

PoC 値は、仮想マシンの 10.0.0.4 IP アドレスと、**hcsjoin** という名前のユーザーの認証情報です。次のスクリーンショットは、ここの入力を示しています。

ドメイン参加 ×

プライマリ DNS サーバ IP アドレス*	172.168.0.15	①
セカンダリ DNS サーバ IP アドレス:		①
デフォルトの組織単位 (OU):	CN=Computers	①
参加ユーザー名:	vmware	①
参加パスワード:	①

[補助参加アカウントの追加](#)

キャンセル
保存

[保存] をクリックします。

情報が保存され、[管理者の追加] ウィンドウが表示されます。

- 4 [管理者の追加] ウィンドウで、システムの検索で PoC Active Directory ドメインの [Domain Admins] グループが見つかるまで、[Domain Admins] の文字を入力します。

管理者の追加 ×

ユーザー グループ:

Domain A
×

Domain Admins
×

CN=Domain Admins,CN=Users,DC=skylo,DC=local

キャンセル
保存

[Domain Admins] をクリックして、その Active Directory グループを選択します。これは、アクティビティ **6** で作成された 3 つのユーザー アカウントがメンバーとして追加された Active Directory グループです。

管理者の追加 ×

ユーザー グループ:

+ Active Directory 検索

選択されたユーザー グループ:

+ SKYLO\ Domain Admins ×

キャンセル
保存

次に、[保存] をクリックします。

- この時点で、システムは自動的に、すぐにコンソールからユーザーをログアウトします。次のような画面が表示されます。

VMware Horizon® へようこそ

ログアウトが完了しました

[ログイン ページに戻る](#)

この強制ログアウトは意図的なものであることに注意してください。

Active Directory ドメインが Horizon Cloud on Microsoft Azure 環境に登録されたので、クラウド テナントへの認証には、2 つのゲートがあります。1 つは、テナント アカウントの認証情報を使用した認証用、もう 1 つは、選択した Active Directory Domain Admins グループのメンバーである Active Directory ユーザー アカウントを使用した認証です。

- メインのログイン ページに戻り、アカウントの認証情報を使用したときと同様に再度ログインします。
cloud.horizon.vmware.com から、システムは自動的に VMware Cloud Services ログイン ユーザー インターフェイスにリダイレクトし、ログイン フローを完了します。



← → ↻ console.cloud.vmware.com/csp/gateway/discovery

VMware Cloud Services

VMware アカウントを使用してログイン

メールアドレス

name@example.com

次へ



- 7 ログイン後、[Active Directory の認証情報] ウィンドウが表示されます。上記の手順 2 の NetBIOS 名がウィンドウに表示されます。

Active Directory の Domain Admins グループのメンバーであるユーザー アカウントの 1 つの認証情報を使用してログインします。

PoC では、次に示すように、**hcsjoin** アカウントの認証情報を使用します。

VMware Horizon® へようこそ

Active Directory の認証情報

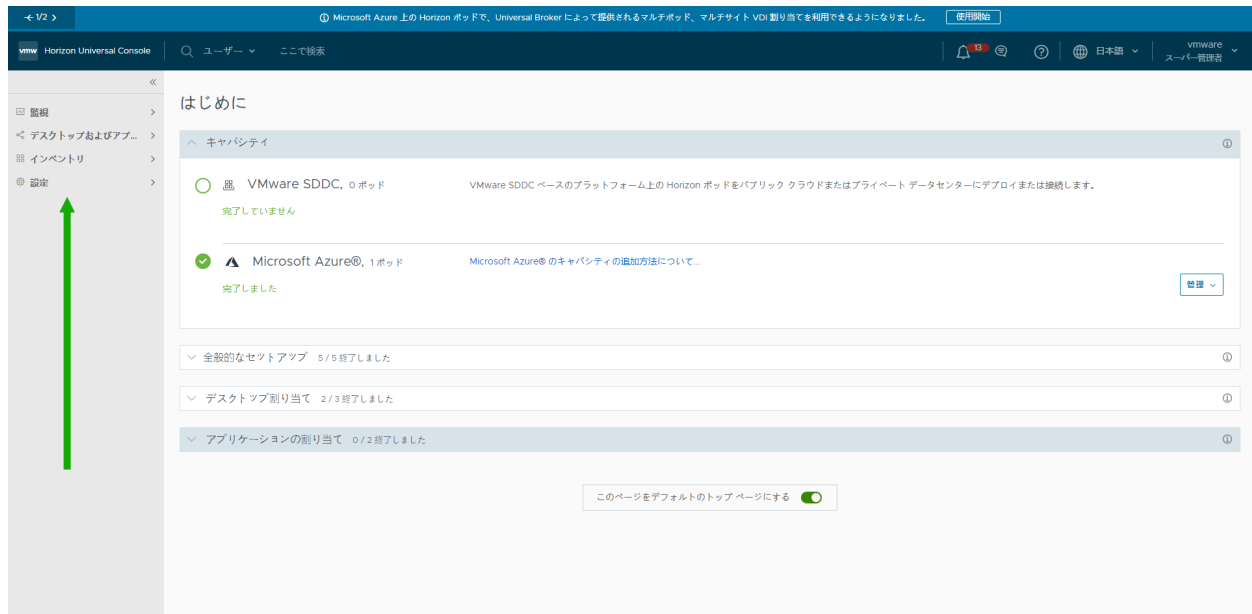
 
SKYLO 

これらの2つの認証ゲートが完了すると、Horizon Universal Consoleに戻ります。これで、すべての左側のナビゲーション領域にアクセスできるようになります。

通常この時点で、[Horizon Cloudの新機能]ウィンドウがポップアップ表示されます。このウィンドウは閉じることができ、上部のヘルプメニューから簡単に表示できます。ヘルプメニューは、次に示すように丸で囲んだ[?]で示します。



メニュー。



Horizon Cloud の使用開始



完了しました。この時点に達すると、Horizon Cloud Service on Microsoft Azure 環境の簡素化された確認作業で使用するバイステップのレシピを正しく完了したことになります。

これで、確認作業を開始できます。レシピはここで終了します。

最後の注意事項

このレシピの最初に選択した簡素化の1つは、最初に外部 Unified Access Gateway 構成なしでデプロイしてから、後で追加することです。

Day-2 のさまざまな PoC アクティビティを実行するには、その外部 Unified Access Gateway 構成を追加します。

[ポッドを編集] ウィザードを実行して外部 Unified Access Gateway 構成を追加するには、特定の条件を満たす署名付き SSL 証明書を指定する必要があります。

この署名付き SSL 証明書が必要な理由は、Unified Access Gateway 機能でクライアント接続に SSL を必要とすることです。証明書には、信頼された証明書認証局 (CA) の署名が必要です。署名付き SSL サーバ証明書は、PEM 形式で、FQDN に基づいている必要があります。単一の PEM ファイルに完全な証明書チェーンおよびプライベートキーが含まれている必要があります。たとえば、単一の PEM ファイルに SSL サーバ証明書、必要な中間 CA 証明書、ルート CA 証明書、およびプライベートキーが含まれている必要があります。OpenSSL は、PEM ファイルの作成に使用できるツールです。

以下のページを参照してください。

- [SSL 証明書を必要な PEM 形式に変換する](#)
- [Horizon Cloud on Microsoft Azure 環境へのゲートウェイ構成の追加](#)

VMware Tech Zone のオンライン ビデオと追加コンテンツ

VMware Digital Workspace Tech Zone は、Horizon Cloud on Microsoft Azure 評価ガイドを提供します。次のガイドには、デプロイ プロセスについて視覚的に理解できるビデオが含まれています：[VMware Horizon Cloud Service on Microsoft Azure の評価ガイド](#)

第 1 世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - 概要レベルの手順

このワークフローでは、ポッド マネージャ ベースのポッドのデプロイから仮想デスクトップおよびアプリケーションの構成までの、第 1 世代 Horizon Universal Console の概要レベルの手順について説明します。エンド ユーザーが資格のある仮想デスクトップとアプリケーションを起動すると、手順は終了します。

重要： この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

注： このワークフローは、特に Horizon Cloud on Microsoft Azure のポッド マネージャ テクノロジーに基づいたポッドに関するもので、Horizon Connection Server テクノロジーを使用した Horizon ポッドのデプロイに関するものではありません。

重要： 管理コンソールの表示は動的で、現在のサービス レベルで利用可能な機能が反映されます。ただし、ポッドのソフトウェアの最新レベルにまだ更新されていないクラウド接続されたポッドがある場合は、コンソールには最新のポッド ソフトウェア レベルに依存する機能は表示されません。また、特定のリリースでは、Horizon Cloud に個別にライセンスされた機能または特定のテナント アカウント構成でのみ使用可能な機能が含まれる場合があります。お持ちのライセンスまたはテナント アカウント構成にそのような機能の使用が含まれる場合のみ、コンソールにその機能に関連する要素が動的に反映されます。例については、[Horizon Cloud での管理タスクに使用されるクラウドベースのコンソールのツアー](#)を参照してください。

使用したい機能が管理コンソール内に見つからない場合は、VMware アカウントの担当者に問い合わせ、お持ちのライセンスおよびテナント アカウント構成にその機能を使用する資格が付与されているか確認してください。

- 1 前提条件に従って準備します。[新しいポッド デプロイの VMware Horizon Cloud Service on Microsoft Azure 要件チェックリスト](#)を参照してください。
- 2 Horizon Cloud 以外の準備タスクを実行します。[Horizon Cloud ポッドを Microsoft Azure にデプロイする前の準備](#)を参照してください。
- 3 ポッドをデプロイするための DNS、ポート、およびプロトコルの要件に従います。[Microsoft Azure での Horizon Cloud ポッドの DNS の要件および 2019 年 9 月のリリースのマニフェスト以降での Horizon Cloud ポッドのポートとプロトコルの要件](#)を参照してください。

- 4 Horizon Universal Console にログインし、ウィザードを実行してポッドをデプロイします。
- 5 Horizon 制御プレーンで Active Directory ドメインを登録します。ここでは、サービス アカウントの名前を提供することも含まれます。これらのサービス アカウントが、Horizon Cloud の運用に必要なサービス アカウントで説明されている要件を満たしていることを確認します。
- 6 管理コンソールに対する認証と管理コンソールでの操作の実行について、組織内のメンバーに適切なロールを割り当てます。Horizon Cloud で使用されるロールには 2 つのタイプがあります。クラウドベースのコンソールを使用して Horizon Cloud 環境で作業するためにユーザーに付与する 2 種類のロールに関するベスト プラクティスを参照してください。
- 7 テナントの Universal Broker 構成を完了します。Universal Broker 設定の構成を参照してください。
- 8 DNS サーバに必要な CNAME レコードを作成します。Universal Broker に対するこれらの CNAME および CNAME レコード要件の目的については、DNS サーバでマッピングする Horizon Cloud ポッドのゲートウェイのロード バランサ情報の取得方法および Universal Broker 設定の構成を参照してください。

注： 構成の Azure ロード バランサにプライベート IP アドレスを使用する外部ゲートウェイ構成がある場合は、そのプライベート IP アドレスへのインターネット トラフィックを管理するファイアウォールまたは NAT があることが必須です。そのファイアウォールまたは NAT は、パブリック IP アドレスを提供し、外部ゲートウェイ構成のデプロイ時に指定された FQDN がパブリックに解決可能になるように構成される必要があります。制御プレーンは、外部ゲートウェイに対して指定された FQDN と通信できる必要があります。

- 9 オプション：Horizon Cloud テナント アカウントが VMware Cloud Services エンゲージメント プラットフォームにまだオンボーディングされていない場合は、ここでオンボーディングすることを推奨します。クラウドベースのコンソールを使用して Horizon Cloud テナントを VMware Cloud Services エンゲージメント プラットフォームにオンボーディングするを参照してください。
- 10 ゴールド イメージを作成します。ゴールド イメージの作成は、マルチステップ プロセスで行います。Horizon Cloud テナントで使用できるゴールド イメージを作成するさまざまな方法の概要については、Microsoft Azure に Horizon Cloud ポッドのデスクトップ イメージを作成を参照してください。ゴールド イメージの作成は、ベース仮想マシンのインポートから開始します。このベース仮想マシンは、ビジネスおよびエンド ユーザーのニーズに合わせてカスタマイズします。
- 11 イメージが最終的に意図するエンドユーザー割り当てのタイプに応じて、必要に応じて次の手順の 1 つ以上を実行します。
 - 単一セッション VDI デスクトップまたはネイティブ アプリケーションのプロビジョニングに使用される単一セッション イメージで、エンド ユーザーが VDI デスクトップで使用するサードパーティ アプリケーションをインストールし、デスクトップ壁紙の設定、(GPU 対応のイメージのための) GPU ドライバのインストールなどのその他の適用可能なカスタマイズを構成します。イメージのインポート プロセスの一部と

して実行されていない場合、Microsoft Sysprep のベスト プラクティスに従ってイメージを最適化することもできます。イメージ仮想マシンの [Microsoft Windows クライアント オペレーティング システムのカスタマイズ](#)、適切な GPU ドライバのインストール、および最適なりモート エクスペリエンス パフォーマンスを得るためにゴールド イメージで実行すべき 5 つの重要なステップを参照してください。

ヒント: イメージ仮想マシンをさらに調整して、VDI の使用事例で VMware Blast Extreme を使用するための構成を改善するには、[VMware Blast Extreme 最適化ガイド](#)を読み、そのガイドのコーデック オプションに関する推奨事項に従って、イメージ内のコーデック オプションの追加のチューニングを実行することがベスト プラクティスです。

- マルチセッション デスクトップとリモート アプリケーションのプロビジョニングに使用されるマルチセッション イメージで、そのマルチセッション イメージからエンド ユーザーに提供するサードパーティ アプリケーションをインストールし、デスクトップ壁紙の設定、(GPU 対応のイメージのための) GPU ドライバのインストールなどの適用可能なその他のカスタマイズを構成します。イメージのインポート プロセスの一部として実行されていない場合、Microsoft Sysprep のベスト プラクティスに従ってイメージを最適化することもできます。インポートされた仮想マシンが、デフォルトで Office 365 ProPlus を含む Microsoft Windows 10 または Windows 11 Enterprise マルチセッション システムの 1 つを実行している場合、Microsoft のドキュメント トピック [Office 365 ProPlus に対する共有コンピュータのライセンス認証の概要](#)で説明されているように、仮想マシンが Office 365 ProPlus の共有コンピュータのアクティベーション用に構成されていることを確認する必要があります。インポートされた仮想マシンで Office 365 ProPlus が共有コンピュータのアクティベーション用に構成されていない場合は、状況に適した Microsoft ドキュメントに記載されている方法を使用してください。イメージ仮想マシンの [Microsoft Windows Server オペレーティング システムのカスタマイズ](#)、イメージ仮想マシンの [Microsoft Windows 10 Enterprise マルチセッション オペレーティング システムのカスタマイズ](#)、適切な GPU ドライバのインストール、および最適なりモート エクスペリエンス パフォーマンスを得るためにゴールド イメージで実行すべき 5 つの重要なステップを参照してください。

ヒント: イメージ仮想マシンをさらに調整して、VDI の使用事例で VMware Blast Extreme を使用するための構成を改善するには、[VMware Blast Extreme 最適化ガイド](#)を読み、そのガイドのコーデック オプションに関する推奨事項に従って、イメージ内のコーデック オプションの追加のチューニングを実行することがベスト プラクティスです。

- 12 そのイメージを、割り当て可能なイメージ (イメージのシーリングまたは公開とも呼ばれる) に変換します。構成済み仮想マシンを割り当て可能なイメージに変換するを参照してください。
- 13 公開済みのマルチセッション イメージからセッション デスクトップとリモート アプリケーションをプロビジョニングするには、次の手順を実行します。
 - a セッション デスクトップを提供するデスクトップ ファームを作成し、エンド ユーザーにこれらのデスクトップを使用する資格を付与するための割り当てを作成します。ファームの作成および RDSH セッション デスクトップ割り当ての作成を参照してください。
 - b リモート アプリケーションを提供するアプリケーション ファームを作成し、アプリケーション インベントリにアプリケーションを追加してから、エンド ユーザーにこれらのリモート アプリケーションを使用する資格を付与するための割り当てを作成します。ファームの作成、RDSH ファームからの新しいリモート アプリケーションのインポート、およびリモート アプリケーション割り当ての作成を参照してください。

- 14 公開済みの単一セッション VDI デスクトップ イメージから単一セッション VDI デスクトップをプロビジョニングするには、専用またはフローティング VDI デスクトップ割り当てを作成します。これらのデスクトップ割り当ての作成については、[Microsoft Azure](#) での [Horizon Cloud 環境のポッドのデスクトップ割り当てについてとそのセクション](#)を参照してください。
- 15 App Volumes アプリケーションをエンドユーザーにプロビジョニングするには、App Volumes アプリケーションをアプリケーション インベントリに追加し、エンドユーザーにそれらのアプリケーションを使用する資格を与えるアプリケーション割り当てを作成します。次に、デスクトップ割り当てを作成し、エンドユーザーにそれらのアプリケーションをベース デスクトップで使用できる資格を付与します。アプリケーション割り当てにより、ユーザーは資格が付与されたデスクトップの Windows オペレーティング システム内で、ユーザーに資格が割り当てられた App Volumes アプリケーションを使用できるようになります。[App Volumes アプリケーション - 概要と前提条件](#)を参照してください。
- 16 デプロイに 2 要素認証構成がある場合は、次のタスクを実行する必要があります。

- ポッドの外部ゲートウェイに 2 要素認証が構成され、ゲートウェイの Unified Access Gateway インスタンスがデプロイされているのと同じ VNet トポロジ内で 2 要素認証サーバにアクセスできない場合は、外部ゲートウェイのロード バランサの IP アドレスからの通信を許可するようにその 2 要素認証サーバを構成します。

このシナリオでは、ゲートウェイ展開と同じ VNet トポロジ内で 2 要素認証サーバにアクセスできないため、Unified Access Gateway インスタンスは、そのロード バランサ アドレスを使用してそのサーバとの接続を試みます。その通信トラフィックを許可するには、その外部ゲートウェイのリソース グループにあるロード バランサ リソースの IP アドレスが、確実に 2 要素認証サーバの構成でクライアントまたは登録されたエージェントとして指定されているようにします。この通信を許可する方法の詳細については、お使いの 2 要素認証サーバのドキュメントを参照してください。

- 同じ VNet トポロジ内で 2 要素認証サーバにアクセスできる場合は、Microsoft Azure でのデプロイの Unified Access Gateway インスタンス用に作成された適切な NIC からの通信を許可するように 2 要素認証サーバを構成します。

ネットワーク管理者が、展開に使用される Azure VNet トポロジとそのサブネットに対する 2 要素認証サーバのネットワーク可視性を決定します。2 要素認証サーバは、ネットワーク管理者が 2 要素認証サーバにネットワークの可視性を与えたサブネットに対応する Unified Access Gateway インスタンスの NIC の IP アドレスからの通信を許可する必要があります。

Microsoft Azure のゲートウェイのリソース グループには、そのサブネットに対応する 4 つの NIC があり、そのうち 2 つが 2 個の Unified Access Gateway インスタンスに対して現在アクティブです。もう 2 つはアイドル状態で、ポッドとそのゲートウェイが更新を完了した後にアクティブになります。

実行中のポッド操作のため、および各ポッドの更新後のために、ゲートウェイと 2 要素認証サーバ間の通信トラフィックをサポートするには、これらの 4 つの NIC の IP アドレスがそのサーバ構成でクライアントまたは登録されたエージェントとして指定されていることを確認します。この通信を許可する方法の詳細については、お使いの 2 要素認証サーバのドキュメントを参照してください。

これらの IP アドレスを取得する方法については、[必要な Horizon Cloud ポッド ゲートウェイ情報での 2 要素認証システムの更新](#)を参照してください。

上記のワークフローの手順が完了したら、Universal Broker の仲介 FQDN をエンド ユーザーに提供します。エンド ユーザーは Horizon Client または Horizon HTML Access (Web クライアント) でその仲介 FQDN を使用して、使用資格が付与されたデスクトップとリモート アプリケーションを起動します。

各ワークフロー手順を実行する方法の詳細については、上記の各手順にリンクされたトピックを参照してください。

第 1 世代テナント - 第 1 世代 Horizon Cloud ポッドを Microsoft Azure にデプロイする前の準備

第 1 世代 Horizon Universal Console にログインしてポッド デプロイ ウィザードを初めて実行する前に、次の準備作業を行う必要があります。このポッド デプロイ ウィザードは、ポッド マネージャ ベースのタイプのポッドをデプロイします。

重要: この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

注意: このウィザードは、ポッド マネージャ ベースのタイプのポッドを Microsoft Azure にデプロイします。現在、コンソールには、Horizon Connection Server のテクノロジーを使用する Azure VMware Solution (AVS) に Horizon ポッドをデプロイするためのデプロイ ウィザードが用意されていません。

1 [3 章 第 1 世代テナント - 2023 年 11 月 2 日のサービス更新以降の新しいポッド デプロイに対する VMware Horizon Cloud Service on Microsoft Azure 要件チェックリスト](#)を参照して、前提条件をすべて満たしていることを確認します。特に、次の点に注意してください。

- Microsoft Azure アカウントとサブスクリプションに、ポッドに必要な仮想マシンの数とサイズが含まれていることを確認します。オプションの Unified Access Gateway 構成をデプロイする場合は、それらも対象になります。[第 1 世代テナント - Microsoft Azure の Horizon Cloud ポッドに対する Microsoft Azure 仮想マシンの要件](#)を参照してください。

ポッドのサブスクリプションとは別の専用のサブスクリプションを使用する外部ゲートウェイ構成でポッドをデプロイする予定がある場合は、他のサブスクリプションに外部ゲートウェイに必要な仮想マシンの数とサイズが含まれていることを確認します。この使用事例では、VNet は複数のサブスクリプションにまたがらないため、その個別のサブスクリプションには専用の VNet が必要です。また、サポートされる VNet トポロジは同じ Microsoft Azure リージョン内の VNet を接続しているため、このサブスクリプションはポッドのサブスクリプションと同じリージョンに存在する必要があります。

- [3 章 第 1 世代テナント - 2023 年 11 月 2 日のサービス更新以降の新しいポッド デプロイに対する VMware Horizon Cloud Service on Microsoft Azure 要件チェックリスト](#)に記載されているように、次の手順を実行します。
 - サブスクリプションで Azure StorageV2 アカウント タイプの使用が制限されていないことを確認します。App Volumes 機能にはストレージ アカウントが必要です。
 - ポッド デプロイ ウィザードでカスタム リソース タグを指定する予定がない場合は、サブスクリプションでリソース グループに固有のタグ名が不要であることを確認します。

- サブスクリプションに Azure ポリシーがないことを確認します。これにより、そのサブスクリプションのポッドのコンポーネントの作成をブロック、拒否、または制限することになります。

注意： サブスクリプションにリソース グループの作成に関する制限がある場合、ポッドのデプロイ プロセスは早い段階で失敗する可能性があります。サブスクリプションが上記のアイテムと一致しない場合、ポッド マネージャ仮想マシンのリソース グループを作成する最初の手順は完了しません。したがって、ポッドのデプロイ プロセスが1時間後にタイムアウトになった場合は、まずサブスクリプションに特定の条件に基づいてリソース グループの作成をブロック、拒否、または制限する Azure ポリシーが設定されているかを確認します。

- ポッドをデプロイするリージョンに仮想ネットワーク (VNet) があり、仮想ネットワークが Horizon Cloud ポッドの要件を満たしていることを確認します。既存の VNet がない場合には、要件を満たす VNet を作成します。第1世代 Horizon Cloud - Microsoft Azure での必要な仮想ネットワークの構成を参照してください。

ポッドの VNet とは別の専用の VNet を使用する、またはポッドのサブスクリプションとは別の専用のサブスクリプションを使用する外部ゲートウェイ構成でポッドをデプロイする場合は、ポッドの VNet と同じリージョンに VNet が存在すること、および第1世代 Horizon Cloud - Microsoft Azure での必要な仮想ネットワークの構成を満たしていることを確認します。この使用事例では、これら2つの VNet をピアリングする必要があります。

重要： 一部の Microsoft Azure リージョンでは、GPU が有効な仮想マシンはサポートされません。GPU 対応のデスクトップまたはリモート アプリケーションでポッドを使用する場合は、使用する NV シリーズ、NVv4 シリーズ、NCv2 シリーズの仮想マシン タイプが、ポッド用に選択した Microsoft Azure のリージョンで提供されていることと、この Horizon Cloud リリースでサポートされていることを確認します。詳細については、<https://azure.microsoft.com/ja-jp/regions/services/>にある Microsoft のドキュメントを参照してください。

- ポッドをデプロイする前に、ポッドのサブネットを VNet 上で手動で作成する場合は、VNet で必要な数のサブネットが作成されたこと、およびそのアドレス空間が第1世代 Horizon Cloud - Microsoft Azure での必要な仮想ネットワークの構成を満たしていること、またリソースがないことを確認します。第1世代テナント - ポッドのデプロイの前に、Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成する。

注意： ポッドのデプロイのために VNet 上に作成するこれらのサブネットは空である必要があります。ポッドをデプロイする前にサブネットを作成することが可能ですが、これらのサブネットにいかなるリソースも配置しないでください。またいかなる IP アドレスも使用しないでください。IP アドレスがサブネットで既に使用されていると、ポッドのデプロイに失敗する可能性があります。

サブネットを事前に作成しない場合、ポッドのデプロイ プロセスは画面上のウィザードに入力した CIDR 情報を使用してサブネットを作成します。

- 仮想ネットワークが、外部名を解決している有効なドメイン ネーム サービス (DNS) サーバを指すように設定されていることを確認します。第1世代テナント - Microsoft Azure の Horizon Cloud ポッドに使用する VNet トポロジに必要な DNS サーバの設定を参照してください。

重要： ポッドのデプロイ プロセスでは、外部名および内部名の解決が必要です。外部名を解決できない DNS サーバを VNet がポイントしている場合、デプロイ プロセスは失敗します。

- 外部ゲートウェイ構成を持つポッドを、ポッドのサブスクリプションとは別のサブスクリプションで作成する既存のリソース グループにデプロイする場合は、デプロイヤがそのリソース グループを自動作成するのではなく、ポッドのデプロイ ウィザードを開始する前にそのサブスクリプションにリソース グループが存在することを確認する必要があります。Horizon Cloud が必要とする権限をリソース グループ レベルで設定するか、サブスクリプション レベルで設定するかを決定します。第1世代テナント - 組織が第1世代 Horizon Cloud のアプリケーション登録にカスタム ロールを使用することを希望する場合を参照してください。
- このリリースでの使用がサポートされている Active Directory が設定済みで、お使いの仮想ネットワークがそれに到達することができ、DNS サーバがその名前を解決できることを確認します。第1世代テナント - Horizon Cloud - Active Directory ドメイン構成を参照してください。

- 2 計画されたデプロイ オプションに従って、必要な数のサービス プリンシパルを作成します。ポッドの外部ゲートウェイ構成を独自のサブスクリプションにデプロイする場合、そのサブスクリプションと、ポッド自身に使用されるサブスクリプションのサービス プリンシパルが必要です。詳細な手順については[第1世代テナント - ポッドのサブスクリプションでの Horizon Cloud アプリケーション登録の作成](#)を参照してください。

重要： Horizon Cloud の使用のために構成する各サービス プリンシパルには、そのサービス プリンシパルの関連付けられたサブスクリプションで適切なロールを割り当てる必要があります。サービス プリンシパルへのロールは、そのサービス プリンシパルに関連付けられた Microsoft Azure サブスクリプションの Horizon Cloud 管理対象リソースで Horizon Cloud が動作するために必要なアクションを許可する必要があります。ポッドのサブスクリプションのサービス プリンシパルには、ポッドを正常にデプロイし、ポッドおよびポッドが管理するリソース上で動作するアクションを許可するロールが必要です。それによって、管理コンソールを使用して開始された管理者ワークフローを満たし、ポッドを長期にわたって維持することができます。ポッドの外部 Unified Access Gateway 構成に個別のサブスクリプションを使用する場合、そのサブスクリプションのサービス プリンシパルには、そのゲートウェイ構成に必要なリソースを正常にデプロイし、それらの Horizon Cloud が管理するリソース上で動作するアクションを許可するロールが必要です。それによって、管理者ワークフローを満たし、それらのゲートウェイに関連するリソースを長期にわたって維持することができます。

[第1世代テナント - 組織が第1世代 Horizon Cloud のアプリケーション登録にカスタム ロールを使用することを希望する場合](#)の説明に従って、次のいずれかの方法を使用してサービス プリンシパルにアクセスを許可する必要があります。

- サブスクリプション レベルで、共同作成者ロールを割り当てます。共同作成者ロールは、Microsoft Azure の組み込みロールの1つです。共同作成者ロールについては、Microsoft Azure ドキュメントの[「Azure リソースの組み込みロール」](#)を参照してください。
- サブスクリプション レベルで、Horizon Cloud がポッド関連リソースの展開、および管理者によって開始された進行中のワークフローとポッド メンテナンス操作のために必要とする[第1世代テナント - 組織が第1世代 Horizon Cloud のアプリケーション登録にカスタム ロールを使用することを希望する場合](#)をサービス プリンシパルに提供するように設定したカスタム ロールを割り当てます。
- 外部 Unified Access Gateway 構成に個別のサブスクリプションを使用し、既存のリソース グループにデプロイする場合、有効な組み合わせは、範囲を限定した権限を提供するロールを使用してそのリソース グループおよび関連する VNet にアクセスするための権限をサービス プリンシパルに許可し、さらに、組み込みの Reader ロールを使用してサブスクリプションにアクセスするための権限をサービス プリンシパルに許可することです。

また、ロールは Horizon Cloud に使用するサービス プリンシパルに直接割り当てる必要があります。サービス プリンシパルへの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。

- 3 [第1世代テナント - 第1世代 Horizon Cloud で Microsoft Azure サブスクリプションにおける状態が登録済みになっている必要があるリソース プロバイダ](#)の説明に従って、Horizon Cloud が必要とするリソース プロバイダがすべて [登録済み] 状態になっていることを確認します。
- 4 Microsoft Azure ポータルから、ポッドのサブスクリプションとその外部ゲートウェイのサブスクリプション（デプロイ オプションを使用する場合）のために、Microsoft Azure サブスクリプション ID、アプリケーション

ン ID、アプリケーション認証キー、および Microsoft Azure AD ディレクトリ ID の値を取得します。これらのリソースは、Horizon Cloud が Microsoft Azure サブスクリプション内で操作を実行するために使用されます。第1世代テナント - Horizon Cloud ポッドのデプロイ ウィザードのためのサブスクリプション関連情報を参照してください。

- 5 Unified Access Gateway 構成でポッドをデプロイしている場合、エンド ユーザーのクライアントがデスクトップおよびリモート アプリケーションへの接続を信頼できるようにする署名付きの TLS/SSL サーバ証明書を取得します。この証明書は、エンド ユーザーがクライアントで使用する FQDN に一致し、信頼されている認証局 (CA) によって署名される必要があります。また、証明書チェーン内のすべての証明書には、すべての中間証明書を含め、有効な有効期限が設定されていなければなりません。チェーン内のいずれかの証明書が期限切れの場合、ポッドのオンボーディング プロセスの後半で予期しない不具合が発生する可能性があります。

エンド ユーザーのクライアントが接続を信頼できるように、Unified Access Gateway が CA 署名付きの証明書を提供します。インターネットからの信頼できるアクセスをサポートするには、ポッドの外部 Unified Access Gateway 構成をデプロイします。企業のネットワーク内の信頼できるアクセスをサポートするには、内部 Unified Access Gateway 構成を使用します。どちらの構成タイプも、ポッドの編集ワークフローを使用して最初のポッド デプロイ プロセスまたはポッド後のデプロイ中にデプロイできます。

重要： この FQDN には、アンダー スコアを含めることはできません。このリリースでは、FQDN にアンダー スコアが含まれていると、Unified Access Gateway インスタンスへの接続が失敗します。

- 6 Unified Access Gateway 構成で使用する署名付き SSL サーバ証明書が PEM 形式でない、またはプライベート キー付きの証明書チェーン全体を含む単一の PEM ファイルでない場合は、証明書の情報を必要な PEM 形式に変換します。第1世代テナント - 第1世代 Horizon Cloud ポッドのデプロイに必要な PEM 形式への証明書ファイルの変換の手順を参照してください。
- 7 Horizon Cloud にアクセスするための登録をまだ実行していない場合は、次の 2 つの項目のいずれかが完了していることを確認します。
 - VMware Customer Connect アカウントを取得し、そのアカウントに Horizon Cloud アクセスを登録します。
 - グループまたは組織が VMware Cloud Services エンゲージメント プラットフォームを使用して Horizon Cloud に登録した場合、または VMware Cloud services または Workspace ONE を使用して Horizon Cloud の使用のために登録した場合は、VMware Cloud services ドキュメントの組織へのユーザーの追加トピックで説明するように、VMware Cloud services 組織の領域に参加するように招待されたときにアクティベーション リンクが記載された招待メールが届きます。このような E メールを受信した場合は、Horizon Cloud にアクセスする前に Eメールの指示に従って操作してください。

これらの準備タスクが完了したら、cloud.horizon.vmware.com の Horizon Universal Console にログインします。このアドレスは、VMware Cloud Services の認証情報または VMware Customer Connect の認証情報を使用してログインする VMware Cloud Services ログインにリダイレクトされます。

ログイン フローの完了後、コンソールの [クラウドのキャパシティを追加] セクションが表示されます。[管理] - [ポッドの追加] をクリックして、ポッド デプロイ ウィザードを起動できます。各画面で必要な情報を入力して、ウィザードを完了します。詳細な手順については [第1世代テナント - Microsoft Azure へのポッドの自動デプロイを実行するための第1世代 Horizon Universal Console の使用](#) を参照してください。

注： クラウドベースのコンソールへのログイン認証は、VMware Cloud Services を使用したアカウント認証情報の認証に依存します。そのサービスが必要な認証要求を完了できない場合、その期間内にコンソールにログインすることはできません。コンソールの最初のログイン画面でログインの問題が発生する場合は、Horizon Cloud システム ステータス ページ (<https://status.workspaceone.com>) で最新のシステム ステータスを確認してください。そのページでは、アップデートを定期受信にすることもできます。

第1世代テナント - Microsoft Azure の Horizon Cloud ポッドに対する Microsoft Azure 仮想マシンの要件

ポッドをデプロイし、ポッドのゲートウェイ構成をデプロイして標準的な運用を行う場合、Microsoft Azure のクラウド キャパシティで特定の種類とサイズの仮想マシン (VM) が必要になります。サブスクリプションには、これらの仮想マシンをサポートする適切な割り当てと構成が必要です。個別のサブスクリプションでポッドの外部ゲートウェイをデプロイするオプションを使用している場合、そのサブスクリプションには、その外部ゲートウェイ構成をサポートするための割り当てと構成が必要です。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、[該当記事を参照](#)してください。

重要： ポッド デプロイ ウィザードは、Microsoft Azure 環境に、指定したポッドとゲートウェイ構成（ある場合）を構築するのに十分なコアの割り当てがあることを検証します。ウィザードで指定したサブスクリプション情報に基づいて十分な割り当てがないとウィザードが判断した場合、画面にメッセージが表示され、ウィザードは次のステップに進みません。

注： GPU が有効な仮想マシンは、一部の Microsoft Azure リージョンでのみ使用できます。詳細については、[リージョン別の Azure 製品](#) を参照してください。

以下の表では、仮想マシンの仕様の列に次の情報が示されています。

- Microsoft Azure のドキュメントで使用されているシリーズ名
- Microsoft Azure ポータルに表示されるクォータに使用されている vCPU のファミリ名
- そのファミリからの仮想マシン タイプの特定の名前

Microsoft Azure ポータルでサブスクリプションの現在の割り当てを表示するには、[すべてのサービス] - [サブスクリプション] に移動して、サブスクリプションをクリックし、[使用量 + クォータ] をクリックします。Microsoft Azure の Microsoft Windows 仮想マシンのサイズの詳細については、Microsoft Azure のドキュメントの次のトピックとそのサブトピックを参照してください。 <https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/sizes>

ポッド マネージャ仮想マシン

これらの仮想マシンは、一般的にポッド自体の中心となります。ポッド マネージャ仮想マシンは、ポッドでプロビジョニングされた仮想デスクトップで実行されている Horizon Agent ソフトウェアへのエンドユーザー クライアントの接続を容易にする役割を担います。

v2204 サービス リリース以降、新しい Horizon Cloud on Microsoft Azure 展開は、デフォルトで高可用性が構成された状態でデプロイされます。展開には 2 台のポッド マネージャ仮想マシンがあります。

表 6-7. ポッド管理仮想マシンの要件 - ポッドのコア仮想マシン向け（ゲートウェイ構成は含まない）

仮想マシン	Microsoft Azure 仮想マシンの仕様	数量	説明
ポッド マネージャ インスタンス	Linux - Standard Dv3 ファミリー： Standard_D4_v3 (4 コア、16 GB のメモリ) OS ディスク：標準的な HDD 30 GiB <u>注：</u> Standard_D4_v3 タイプが Microsoft Azure リージョンで使用できない場合、ポッド デプロイヤーは代わりに Standard Dv2 ファミリーの Standard_D3_v2 (4 コア、14 GB のメモリ) を使用します。	定常状態の動作中はポッドごとに 2 つ ポッドの Blue/Green 更新プロセスの End-to-End 時間中は、ポッドごとに 4 つ。	定常状態の動作中には、2 台の仮想マシンが存在し、パワーオンされ、ポッドを実行します。新しいポッドのマニフェストが VMware オペレーション チームによって利用可能になったときに、システムがポッドの Blue/Green 更新プロセス用の Green コンポーネントの構築を開始すると、ポッド マネージャ仮想マシンにつき 2 つ目のインスタンスが作成され、パワーオンされます。その時点では、ポッド マネージャ仮想マシンの合計実行数は 4 です。End-to-End の更新プロセスの一部として、システムが Green コンポーネントの使用に切り替える時刻をスケジューリングします。切り替えが完了した後、ポッドは定常状態の動作のために新しく作成された 2 台の仮想マシンを使用しており、Blue コンポーネント セットにある以前に使用されていた 2 台の仮想マシンは停止して削除されます。 環境のサイズは、システムが Blue/Green 更新プロセスのためにポッドの Green コンポーネントの構築を開始した時点から、ポッドが新しい Green コンポーネントを使用するように切り替えられる時点までの、End-to-End の更新期間で並行して実行される 4 つのポッド マネージャ インスタンスに対応できる必要があります。ポッドの Blue/Green 更新プロセスの説明については、 Horizon Cloud ポッド - メンテナンスと更新 を参照してください。

ゲートウェイ関連の仮想マシン

次のインスタンスは、ゲートウェイ関連の仮想マシンのこのカテゴリに分類されます。

- ポッドでプロビジョニングされたリソースにアクセスするエンドユーザー クライアントのセキュア ゲートウェイとして機能するように構成された Unified Access Gateway インスタンス。

- 外部ゲートウェイをポッドの VNet とは別の VNet にデプロイすることを選択したシナリオで作成されるゲートウェイ コネクタ仮想マシン。このゲートウェイ コネクタは、そのシナリオでのクラウド管理操作を処理しません。

注： 2020 年 7 月の四半期リリース以降、ポッド全体のデプロイまたは新しいゲートウェイの追加のいずれかの時点で、新しいゲートウェイをデプロイする場合、Unified Access Gateway インスタンスでサポートされる仮想マシン モデルのリストから選択できます。2020 年 7 月のリリース以前は、Standard_A4_v2 仮想マシン モデルを使用するためにゲートウェイ インスタンスが必要でした。画面上のウィザードで選択できるサポート対象の仮想マシン モデルのリストは、ゲートウェイ インスタンスをデプロイする Microsoft Azure リージョンで使用可能な仮想マシン モデルによって異なります。表示される選択は、ゲートウェイのデプロイに使用する Microsoft Azure サブスクリプションの仮想マシンの割り当てによっても異なります。ポッド デプロイ ウィザードの [仮想マシン モデル] メニューには、これらの要件を満たす仮想マシン モデルが動的に反映されます。

ソフトウェアの更新では、ゲートウェイ インスタンスの仮想マシン モデルが維持されます。ポッドの更新前のゲートウェイ インスタンスの仮想マシン モデルは、アップデート後の仮想マシン モデルになります。

表 6-8. Unified Access Gateway 仮想マシンの要件

仮想マシン	Microsoft Azure 仮想マシンの仕様	数量	説明
Unified Access Gateway インスタンス	<p>このリリース以降では、新しいゲートウェイのデプロイ用に、次の仮想マシン モデルから選択できます。</p> <ul style="list-style-type: none"> ■ Linux Standard Av2 ファミリー <ul style="list-style-type: none"> — Standard_A4_v2 (4 コア、8 GB のメモリ)、OS ディスク: 標準 HDD 20 GiB ■ Linux Standard FSv2 ファミリー: <ul style="list-style-type: none"> ■ Standard_F8s_v2 (8 コア、16 GB のメモリ)、OS ディスク: SSD 32 GiB 	<p>外部または内部 Unified Access Gateway 構成を使用するか、同じポッドで両方のタイプを使用するかによって異なります。</p> <p>構成が外部または内部のみの場合:</p> <ul style="list-style-type: none"> ■ 定常状態の動作中はポッドごとに 2 つ ■ ポッド関連の Blue/Green 更新アクティビティの End-to-End 時間中はポッドごとに 4 つ。 <p>Unified Access Gateway 構成が外部および内部の両方設定されているポッドの場合:</p> <ul style="list-style-type: none"> ■ 定常状態の動作中はポッドごとに 4 つ ■ ポッド関連の Blue/Green 更新アクティビティの End-to-End 時間中はポッドごとに 8 つ。 	<p>Unified Access Gateway は、デプロイ ウィザードでゲートウェイ設定を行うときに、ポッドでデプロイされるオプションの機能です。ポッドで Unified Access Gateway インスタンスを使用することを決定した場合、環境がポッドの End-to-End の Blue/Green 更新中に実行しているこれらのインスタンスに対応できる必要があります。定常状態インスタンスの数は、外部および内部の両方の Unified Access Gateway 構成を選択するかどうかによって決まります。</p> <p>定常状態の動作中に外部のみまたは内部のみの Unified Access Gateway 構成しかない場合、2 つのインスタンスが存在し、パワーオンになり、Unified Access Gateway 機能を提供します。更新プロセスで、2 つの追加インスタンスが作成され、パワーオンされて Unified Access Gateway のソフトウェア アップデートが実行されます。更新の完了後、ポッドは新しく作成された仮想マシンの使用に移行し、Blue コンポーネント セットにある以前に使用されていた仮想マシンは停止して削除されます。</p> <p>定常状態の動作中に内部と外部の両方の Unified Access Gateway 構成を使用する場合、4 つのインスタンスが存在し、パワーオン状態になり、Unified Access Gateway 機能を提供します。2 つのインスタンスが外部構成の機能を提供し、2 つのインスタンスが内部構成の機能を提供します。更新中は、1 つの構成あたり 2 つの追加インスタンスが作成され、パワーオンされて Unified Access Gateway のソフトウェア アップデートが実行されます。更新の完了後、ポッドは新しく作成された仮想マシンの使用に移行し、Blue コンポーネント セットにある以前に使用されていた仮想マシンは停止して削除されます。</p> <p>環境のサイズは、システムが Blue/Green 更新プロセスのためにポッドの Green コンポーネントの構築を開始した時点から、ポッドが新しい Green コンポーネントを使用するように切り替えられる時点までの、End-to-End の更新期間で並行して実行される示された Unified Access Gateway インスタンスに対応できる必要があります。ポッドの Blue/Green 更新プロセスの説明については、Horizon Cloud ポッド - メンテナンスと更新を参照してください。</p>

表 6-9. 個別の VNet に外部ゲートウェイがある場合：ゲートウェイ コネクタ仮想マシンの要件

仮想マシン	Microsoft Azure 仮想マシンの仕様	数量	説明
ゲートウェイ コネクタ インスタンス	Linux Standard Av2 ファミリ： Standard_A1_v2 (1 コア、2 GB のメモリ) OS ディスク：標準的な HDD 10 GiB	定常状態の操作中に、この外部ゲートウェイ タイプごとに1つ ポッド関連の Blue/Green 更新アクティビティの End-to-End 時間中はこの外部ゲートウェイ タイプごとに2つ。	外部ゲートウェイが個別の VNet にデプロイされると、この仮想マシンが作成され、その外部ゲートウェイ構成でのクラウド管理操作に使用されます。更新中に追加のインスタンスが作成され、パワーオン状態になり、外部ゲートウェイ構成の Unified Access Gateway でソフトウェアの更新が実行されます。更新が完了すると、新しく作成された仮想マシンへの移行が行われ、以前使用されていた仮想マシンは停止して削除されます。このオプションの構成を使用する場合は、ポッド関連の Blue/Green 更新アクティビティ中に End-to-End で実行されるこれらのインスタンスに環境が対応できる必要があります。

ゴールド イメージ - 全般

ゴールド イメージとは、Horizon Cloud がそれを公開イメージに変換できるように構成されている、Microsoft Windows オペレーティング システムの仮想マシンです。これらの仮想マシンは、ゴールド パターンと呼ばれている場合があります。

ゴールド イメージは、それらを作成したときの選択に応じて、GPU 対応かそうでないかのいずれかになります。

Horizon Cloud では、シングルポッドのゴールド イメージとマルチポッドのゴールド イメージの両方を作成できます。どちらのタイプの作成も、コンソールの自動化された [Marketplace からの仮想マシンのインポート] ウィザードを使用して行われます。

自動ウィザードでは、デフォルトで特定の仮想マシン サイズが自動的に使用されます。このデフォルトは、内部設定と、特定のオペレーティング システム (OS) のウィザードでの選択、および GPU を含めるかどうかに基づいています。

ゴールド イメージ仮想マシン

v2207 サービス リリース以降、シングルポッド イメージとマルチポッド イメージの両方に同じ仮想マシン モデル要件があります。シングルポッド イメージは、コンソールの [インポートされた仮想マシン] ページを使用してインポートされます。マルチポッド イメージは、コンソールの [マルチポッド イメージ] ページを使用してインポートされます。

表 6-10. ゴールド イメージ 仮想マシンの要件

仮想マシン	Microsoft Azure 仮想マシンの仕様	数量	説明
ゴールド イメージ	<p>GPU が有効なゴールド イメージでは、システムは次を使用します。</p> <ul style="list-style-type: none"> (Standard NVSv3 ファミリの vCPU からの) Standard_NV12s_v3 OS ディスク：標準的な HDD 127 GiB <p>Windows 11 以外の OS を使用する GPU 非対応のゴールド イメージの場合、システムは以下を使用します。</p> <ul style="list-style-type: none"> (Standard DSv2 ファミリの vCPU からの) Standard_DS2_v2 OS ディスク：標準的な HDD 127 GiB <p>Microsoft Windows 11 OS または Windows 11 Enterprise マルチセッション OS を使用する GPU 非対応のゴールド イメージの場合、システムは以下を使用します。</p> <ul style="list-style-type: none"> (Standard DSv3 ファミリの vCPU からの) Standard_D4s_v3 OS ディスク：標準的な HDD 127 GiB 	必要に応じて変更できます。	<p>ゴールド イメージとは、Horizon Cloud がそれを公開イメージに変換できるように構成されている、Microsoft Windows オペレーティング システムの仮想マシンです。</p> <p>Windows 単一セッション オペレーティング システム仮想マシンは、VDI デスクトップを作成するために使用する基盤を提供します。</p> <p>RDS 対応の Windows オペレーティング システム仮想マシンは、セッションベースのデスクトップおよびリモート アプリケーションをエンド ユーザーに提供するファームに仮想マシンを作成するために使用される基盤を提供します。この RDS 対応カテゴリには、Windows Server OS と Windows Enterprise マルチセッション OS の両方が含まれます。</p> <p>各ゴールド イメージは、Microsoft Windows オペレーティング システムと GPU 対応であるか非対応かを組み合わせたものになります。このため、ポッドで提供するものが次のとおりである場合：</p> <ul style="list-style-type: none"> Microsoft Windows 2016 Datacenter を使用する RDSH デスクトップ、GPU なし Microsoft Windows 2016 Datacenter を使用する RDSH デスクトップ、GPU あり <p>少なくとも 2 つのゴールド イメージ仮想マシンが必要になります。</p> <p>ゴールド イメージを公開イメージに変換するプロセスは、イメージの公開と呼ばれたり、イメージのシーリングとも呼ばれることがあります。作成される公開イメージは、割り当てで使用するための最終状態になっているため、シールドされたイメージまたは割り当て可能なイメージと呼ばれることがあります。</p> <p>公開ワークフローが完了すると、システムはゴールド イメージを自動的にパワーオフします。公開イメージを更新すると、システムは仮想マシンを再度パワーオンします。</p> <p>注： コンソールの [複製] アクションを使用してイメージを複製する場合、システムはその複製のための構成を取得するためにゴールド イメージの仮想マシンを一時的にパワーオンして、再びパワーオフします。</p> <p>シングルポッドのゴールド イメージを作成する方法については、デスクトップ イメージと Horizon Cloud ポッドの作成のトピックを参照してください。</p>

ファーム仮想マシン

RDSH ファームの仮想マシンは、エンド ユーザーにセッション ベースのデスクトップとリモート アプリケーションを提供する RDS 対応のインスタンスです。セッション デスクトップを提供するには少なくとも 1 つの RDSH ファームが必要で、リモート アプリケーションを提供するには 1 つの RDSH ファームが必要です。管理者またはエンドユーザーのニーズを満たすために、追加のファームをデプロイすることを決定することができます。

注： 現在のサービス リリースでは、セッション ベースのデスクトップとリモート アプリケーションを同じファームから配布することはできません。

表 6-11. ファーム仮想マシンの要件

仮想マシン	Microsoft Azure 仮想マシンの仕様	数量	説明
RDSH ファーム	<p>ポッドでファームを作成するときに選択できるようにする一連の Microsoft Azure 仮想マシン タイプをカスタマイズできます。標準の Microsoft Azure リージョンで一般的に使用可能な一連の Microsoft Azure 仮想マシン サイズから独自のリストをカスタマイズできます。ファームで使用できる一連の仮想マシン タイプのカスタマイズの詳細については、『Horizon Cloud 管理ガイド』を参照してください。</p> <p>ファームを作成または編集するときに、ファームの RDSH インスタンスの OS ディスク サイズをカスタマイズして、システムのデフォルト値から変更できます。</p> <p>標準の Microsoft Azure リージョンで一般的に利用可能な Windows 仮想マシン サイズの詳細については、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes にある Microsoft のドキュメントを参照してください。</p> <p>注： 本番環境では、ファームに使用する仮想マシン タイプに少なくとも 2 個の CPU が確実に搭載されているようにします。この基準を満たすことで、エンドユーザー接続に関する不測の問題を回避できます。この基準は、バージョン 7.x 以降から Horizon Agent をインストールまたは更新するために、2 個以上の CPU を備えていることが Horizon Agent の推奨事項であることによるものです。この Horizon Agent の基準は、バージョン 7.8 以降の Horizon 製品ドキュメントに記載されています (最小 2 CPU の参照は、バージョン 7.8 の仮想マシンへの Horizon Agent のインストールから始まります)。</p>	ニーズおよび Horizon Cloud 環境で仮想マシンのサイズをカスタマイズした方法によって異なります。	これらの仮想マシンの電源状態は、ファームの構成とエンド ユーザーの要件によって異なります。

VDI デスクトップ仮想マシン

VDI デスクトップ仮想マシンは、エンド ユーザーに VDI デスクトップを提供するインスタンスです。

注： 2020 年 7 月の四半期サービス リリースの新機能は、Microsoft Azure のポッドでの App Volumes 機能の使用です。コンソールの App Volumes キャプチャ プロセスを使用してネイティブ アプリケーションを Horizon Cloud インベントリに追加すると、キャプチャ プロセスをサポートするために、システムによって 2 台の仮想マシンの VDI デスクトップ割り当てが作成されます。このシステムにより生成された割り当てに使用される仮想マシン タイプは、アプリケーション キャプチャ プロセスのコンソールで選択した公開イメージに使用されるものと同じモデルです。

表 6-12. VDI デスクトップ仮想マシンの要件

仮想マシン	Microsoft Azure 仮想マシンの仕様	数量	説明
VDI デスクトップ	<p>ポッドで VDI デスクトップ割り当てを作成するときに選択できるようにする一連の Microsoft Azure 仮想マシン タイプをカスタマイズできます。標準の Microsoft Azure リージョンで一般的に使用可能な一連の Microsoft Azure 仮想マシン サイズから独自のリストをカスタマイズできます。VDI デスクトップ割り当てで使用できる一連の仮想マシン タイプのカスタマイズの詳細については、『Horizon Cloud 管理ガイド』を参照してください。</p> <p>注: Standard_B2I や Standard_B1 など、Microsoft が VDI のユースケースには適していないと判断した少数の Microsoft Azure 仮想マシン サイズは、使用の対象から自動的に除外されます。</p> <p>VDI デスクトップ割り当てを作成または編集するときに、VDI デスクトップ インスタンスの OS ディスク サイズをカスタマイズして、システムのデフォルトから変更できます。</p> <p>これらの Windows 仮想マシンのサイズに関する詳細情報については、Microsoft のドキュメント (https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes) を参照してください。</p> <p>注: 本番環境では、VDI デスクトップ割り当てに使用する仮想マシン タイプに少なくとも 2 個の CPU が確実に搭載されているようにします。この基準を満たすことで、エンドユーザー接続に関する不測の問題を回避できます。この基準は、バージョン 7.x 以降から Horizon Agent をインストールまたは更新するために、2 個以上の CPU を備えていることが Horizon Agent の推奨事項であることによるものです。この Horizon Agent の基準は、バージョン 7.8 以降の Horizon 製品ドキュメントに記載されています (最小 2 CPU の参照は、バージョン 7.8 の仮想マシンへの Horizon Agent のインストールから始まります)。</p>	ニーズおよび Horizon Cloud 環境で仮想マシンのサイズをカスタマイズした方法によって異なります。	これらの仮想マシンの電源状態は、VDI デスクトップ割り当ての設定とエンド ユーザーの要件によって異なります。

特殊なケースのサポート関連のジャンプ ボックス仮想マシン

VMware にサポート リクエストを発行し、サポート チームがそのリクエストを処理する方法として、VMware が管理するアプライアンスとの通信用の一時的なジャンプ ボックス仮想マシンをデプロイすることを決めた場合、サブスクリプション コアとクォータはその時点でそのデプロイに対応する必要があります。サポート関連のジャンプ ボックス デプロイの権限がお客様から要求されます。

このジャンプ ボックスは、VMware サポート チームの監督の下にデプロイされ、サポート リクエストの対応で仮想マシンが不要になると、VMware サポート チームの監督の下で削除されます。

表 6-13. 一時的なサポート関連のジャンプ ボックス仮想マシンの要件

仮想マシン	Microsoft Azure 仮想マシンの仕様	数量	説明
サポート関連のジャンプ ボックス	Linux Standard F ファミリ : Standard_F2 (2 コア、4 GB のメモリ) OS ディスク : 標準的な HDD 30 GiB	1	このサポート関連のジャンプ ボックス仮想マシンは、VMware のサポートへのサポート リクエストに対応して、VMware 管理対象アプライアンスとの安全な通信を提供するように設計されています。

第 1 世代 Horizon Cloud - Microsoft Azure での必要な仮想ネットワークの構成

Horizon Cloud ポッドを環境にデプロイするには、Microsoft Azure 環境に既存の仮想ネットワークが必要です。デプロイするリージョンに仮想ネットワーク (VNet) がない場合は、仮想ネットワークを作成する必要があります。ポッドの外部ゲートウェイを、ポッドの VNet とは別の専用の VNet にデプロイする場合は、その VNet も作成し、それから 2 つの VNet をピアリングする必要があります。ポッドの外部ゲートウェイが、ポッドとは別の専用のサブスクリプションを使用するようにする場合、その外部ゲートウェイに使用する別の VNet を作成して、2 つの VNet をピアリングする必要があります。これは、単一の VNet は複数のサブスクリプションにまたがらないため、外部ゲートウェイを専用のサブスクリプションにデプロイする場合、そのデプロイでは、外部ゲートウェイがポッドの VNet にピアリングされた別の VNet を使用する必要もあるためです。

重要： この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

注意： ポッドのデプロイのために VNet 上に事前に手動で作成したサブネットは空のままである必要があります。これらのサブネットの IP アドレスを使用しているアイテムを持つ既存のサブネットを再利用しないでください。IP アドレスがサブネットですでに使用されている場合、ポッドがデプロイに失敗したり、その他のダウンストリーム IP アドレスの競合の問題などの問題が発生する可能性が高くなります。これらのサブネットに何らかのリソースを投入したり、IP アドレスを使用したりしないでください。この警告通知には Horizon Cloud からデプロイされたポッドが含まれています。すでにデプロイされているポッドがあるサブネットを再利用しないでください。

どの VNet に外部ゲートウェイをデプロイしていますか？	サブネットの作成	必要なサブネット
<p>ポッドの VNet を使用して外部ゲートウェイでポッドをデプロイする場合</p>	<p>この構成では、事前に VNet でサブネットを作成してポッドのデプロイ ウィザードでそのサブネットを指定するか、必要なサブネットのアドレス空間をウィザードに直接入力すると、ポッド デプロイヤが VNet にサブネットを作成します。</p> <p>重要： 既存の VNet がピアリングされている場合、デプロイヤは VNet のアドレス空間を自動的に更新することができません。VNet がピアリングされている場合のベストプラクティスは、第 1 世代テナント - ポッドのデプロイの前に、Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成するに記載されているように、事前にサブネットを作成することです。サブネットを事前に作成せずに、デプロイ ウィザードで VNet の既存アドレス空間に含まれていないサブネット CIDR を入力した場合、ウィザードにはエラー メッセージが表示されます。この場合は、有効なサブネット アドレス空間を指定して続行するか、ピアリングされていない仮想ネットワークを使用します。</p>	<p>この構成を使用してポッドをデプロイするには、次のサブネットが必要です。</p> <ul style="list-style-type: none"> ■ ポッド自身の管理アクティビティに含まれる仮想マシンで使用される IP アドレスの場合は管理サブネット。 ■ プライマリ仮想マシン サブネット – テナント サブネットまたはデスクトップ サブネットとも呼ばれます。このサブネットは、サブネット上の RDSH サーバの仮想マシンおよび VDI デスクトップ仮想マシンに使用される IP アドレスを提供します。内部 Unified Access Gateway 構成がデプロイ ウィザードで指定されている場合、Unified Access Gateway 仮想マシンもこのサブネットからの IP アドレスを使用します。 <p>重要： VDI デスクトップの仮想マシン、RDS 対応イメージ、ポッドのファームの各 RDSH 仮想マシンはこれらの IP アドレスを使用します。このプライマリ仮想マシンのサブネットはポッドのデプロイ後に拡張できないため、このポッドで提供するデスクトップの数を考慮して、十分に対応できる範囲に設定します。たとえば、このポッドで今後 1,000 台以上のデスクトップを提供することが予想される場合は、これ以上の IP アドレス範囲を設定します。2020 年 7 月以降のリリースでは、新機能を使用することで、後でポッドを編集し、ファーム仮想マシンや VDI デスクトップ仮想マシンで使用する仮想マシンのサブネットを追加できます。この新機能によって、ファームおよび VDI デスクトップ割り当ての拡大に対応するために、長期にわたって仮想マシンのサブネットを柔軟に追加できます。ファームおよび VDI デスクトップ割り当ての定義で追加のサブネットを明示的に指定しない限り、このプライマリ仮想マシンのサブネットがデフォルトで使用されるため、ベストプラクティスとして、このプライマリ仮想マシンのサブネットの範囲を、予想されるファーム仮想マシンおよびデスクトップの台数に十分対応できる範囲に設定します。</p> <ul style="list-style-type: none"> ■ オプションの外部 Unified Access Gateway 構成によって使用される IP アドレス用の DMZ サブネット。

どの VNet に外部ゲートウェイをデプロイしていますか？	サブネットの作成	必要なサブネット
		<p>デプロイヤーにサブネットの自動作成を実施させる場合、デプロイヤーは対応する VNet に新しいサブネットを常に作成します。VNet のアドレス空間の観点から、次のようにウィザードに入力したサブネット アドレス空間を、デプロイヤーが処理します。</p> <ul style="list-style-type: none"> ■ VNet のアドレス空間にまだ存在していないアドレス空間をウィザードで指定すると、デプロイヤーは自動的にそれらのアドレス空間を追加するために VNet の構成を更新します。次に、VNet に新しいサブネットが作成されます。 ■ ウィザードで指定したアドレス空間がすでに VNet の既存のアドレス空間に含まれている場合、デプロイヤーはその指定したアドレス空間を使用して VNet に新しいサブネットを作成します。
<p>ポッドの VNet またはサブスクリプションとは別に、専用の VNet またはサブスクリプションを使用する外部ゲートウェイを持つように選択してポッドをデプロイする場合</p>	<p>この構成では、2 つの VNet が含まれ、これらの VNet をピアリングする必要があるため、ベスト プラクティスとして、VNet で事前にサブネットを作成し、ポッドのデプロイウィザードでそれらのサブネットを指定します。第 1 世代テナント - ポッドのデプロイの前に、Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成するの説明に従って、事前にサブネットを作成します。デプロイ ウィザードには、デプロイヤーがサブネットを作成するために必要なサブネットのアドレス空間をウィザードに直接入力するオプションがありますが、VNet のアドレス空間にないアドレス空間を指定すると、VNet はピアリングされた VNet であるため、デプロイヤーはそのアドレス空間を VNet に追加できません。</p> <p>この場合、1 つの VNet にポッドのサブネットがあり、もう 1 つの VNet に外部ゲートウェイのサブネットがあります。これらの 2 つの VNet をピアリングする必要があります。ポッドの VNet を VNet-1、外部ゲートウェイの VNet を VNet-2 と呼ぶことにします。VNet ごとに、ポッド デプロイヤーが自動的に作成するサブネットのアドレス空間を指定するか、事前に作成したサブネットを指定できます。</p>	<p>このタイプのデプロイでは、ポッドの VNet (VNet-1) は管理サブネットとデスクトップサブネットを取得し、それらは外部ゲートウェイがポッドの専用 VNet にある場合の説明と同じ目的で使用されます。ただし、ポッドの VNet はこの構成では DMZ サブネットを取得しません。これは、DMZ サブネットがこの構成の別の VNet (VNet-2) にある外部 Unified Access Gateway 構成での使用を目的としているためです。このデプロイ構成では、外部ゲートウェイの VNet は次のサブネットを取得します。</p> <ul style="list-style-type: none"> ■ 外部ゲートウェイ自体の管理アクティビティに含まれる仮想マシン (ゲートウェイのコネクタ仮想マシン、および外部ゲートウェイの Unified Access Gateway インスタンス) が使用する IP アドレスのための管理サブネット ■ 外部ゲートウェイの Unified Access Gateway インスタンスによって使用されるバックエンド サブネット ■ 外部ゲートウェイの Unified Access Gateway インスタンスによって使用される DMZ サブネット

登録アカウントに応じた Microsoft Azure ポータルを使用して、次の手順を行います。たとえば、これらの Microsoft Azure クラウドのための特定のポータル エンドポイントがあります。

- Microsoft Azure Commercial (標準グローバル地域)
- Microsoft Azure China

■ Microsoft Azure US Government

自分のアカウントに該当する URL を使用してポータルにログインします。

手順

- 1 Microsoft Azure ポータルで、ポータルの検索バーで **仮想ネットワーク** を検索し、対応する仮想ネットワークの結果を選択することで、[仮想ネットワーク] ペインに移動します。
- 2 [仮想ネットワーク] ペインで、[作成] をクリックして VNet 作成ウィザードを開始します。
- 3 ウィザードで、画面上のウィザードの手順で次の情報を指定します。

オプション	説明
サブスクリプション	ポッドをデプロイするときに使用する予定がある、同じサブスクリプションを選択します。
リソース グループ	既存のリソース グループを選択するか、仮想ネットワークの作成時に新しいリソース グループを作成することができます。
名前	VNet の名前を指定します。
地域	ポッドをデプロイする予定がある、同じ Microsoft Azure リージョンを選択します。
アドレス空間	VNet のアドレス空間を指定します。
サブネットとアドレス範囲	Microsoft Azure では、VNet を作成するときに1つのサブネットを作成する必要があります。デフォルト値を保持することも、名前や範囲をカスタマイズすることもできます。ポッドの必要なサブネットのいずれかにこのサブネットを使用する場合は、ポッド デプロイの要件に応じて適切なアドレス範囲を指定してください。たとえば、ポッドのテナント サブネットにこのサブネットを使用する場合は、デプロイ ウィザードが要求する /27 に最小限適合する IP アドレス範囲を持つことを確認してください。第1世代テナント - ポッドのデプロイの前に、 Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成する を参照してください。 重要： このサブネットを、ポッドの必要なサブネットの1つに使用する場合は、その他のリソースに使用できません。

オプションの設定に対しては、デフォルト値を保持します。

- 4 確認の手順に進み、[作成] をクリックします。

結果

ご利用の Microsoft Azure アカウントで、仮想ネットワーク (VNet) が作成されます。

次のステップ

ポッドのデプロイ プロセスによって作成を行う代わりに必要なサブネットを手動で作成する場合、ポッドに使用するサブネットで新しく作成された VNet を構成します。第1世代テナント - ポッドのデプロイの前に、[Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成する](#)および第1世代テナント - Microsoft Azure で Horizon Cloud ポッド用に既存のサブネットを使用する場合の手順を参照してください。

実行中の DNS サービスと、ポッドで使用する Active Directory サービスへの接続により、新しく作成された VNet を構成します。第1世代テナント - Microsoft Azure の Horizon Cloud ポッドに使用する VNet トポロジに必要な DNS サーバの設定の手順を参照してください。

ファイアウォールや、その他のネットワーク動作に関連して、現在の VNet 構成が、[第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件](#)、[DNS 名および第1世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件](#)に記載されているとおりに、ポッド デプロイの DNS、ポート、およびプロトコルの要件に準拠していることを確認します。

重要： ポッド マネージャ仮想マシンには、Microsoft Azure VNet でのアウトバウンド インターネット アクセスが必要です。専用の VNet に外部ゲートウェイをデプロイする場合、その VNet はアウトバウンド インターネット アクセスが可能なゲートウェイ コネクタ仮想マシンをサポートする必要があります。プロキシベースのアウトバウンド インターネット アクセスが必要な場合は、ポッドのデプロイ ウィザードのフィールドを完成させるときにプロキシ サーバ情報を指定する必要があります。

第1世代テナント - ポッドのデプロイの前に、Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成する

ピアリングされた VNet を使用している場合、ベスト プラクティスは、ポッドをデプロイする前に必要なサブネットを作成し、デプロイ ウィザードを実行する前に VNet でサブネットが必要とするアドレス空間が確保されるようにすることです。VNet がピアリングされていない場合でも、第1世代のポッドのデプロイ プロセスに必要なサブネットを作成させる代わりに、VNet であらかじめ作成することができます。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、[該当記事を参照してください](#)。

重要： 2019 年 9 月のリリースでのポッドのマニフェスト バージョンから、そのバージョン以降のマニフェストで新しくデプロイされたポッドと、そのバージョンまたはそれ以降のバージョンに更新されたポッドの両方について、ポッドの管理サブネットでのポッドの Microsoft Azure Database for PostgreSQL サービス リソースとのネットワーク通信もサポートされる必要があります。新しいポッドをデプロイする前、または既存のポッドをアップグレードする前に、作成するポッド管理サブネットで、Microsoft.Sql サービスがサービス エンドポイントとしてリストされている必要があります。デプロイまたは更新プロセスでは、サブネットにエンドポイントがあるかどうかをチェックされ、サブネットでエンドポイントが有効になっていない場合は続行されません。詳細については、[第1世代テナント - Microsoft Azure で Horizon Cloud ポッド用に既存のサブネットを使用する場合を参照してください](#)。

サブネットを事前に作成する場合、クラスレス ドメイン間ルーティング (CIDR) 表記のアドレス範囲がポッド デプロイ ウィザードの最小要求に準じていることを確認する必要があります。

- 管理サブネットの場合、/27 以上の CIDR が必要です。このサブネットは、ポッド自身の管理アクティビティに含まれる仮想マシンで使用される IP アドレスのためのものです。
- プライマリ仮想マシンのサブネット (デスクトップまたはテナント サブネットとも呼ばれる) の場合、/27 以上の CIDR が必要です。本番環境では、/24 ~ /21 の CIDR (256 ~ 2048 アドレス) を推奨します。このサブネットは、サブネット上の RDSH サーバの仮想マシンおよび VDI デスクトップ仮想マシンに使用される IP アドレスのためのものです。ポッド マネージャの仮想マシンは、このサブネットからの IP アドレスを使用します。

ポッドに内部 Unified Access Gateway 構成がある場合、それらの Unified Access Gateway 仮想マシンもこのサブネットからの IP アドレスを使用します。ポッドに、ポッドの VNet を使用してデプロイされた外部ゲートウェイ構成がある場合、その外部ゲートウェイの Unified Access Gateway 仮想マシンもこのサブネットの IP アドレスを使用します。

重要： VDI デスクトップの仮想マシン、RDS 対応イメージ、ポッドのファームの各 RDSH 仮想マシンはこれらの IP アドレスを使用します。このプライマリ仮想マシンのサブネットはポッドのデプロイ後に拡張できないため、このポッドで提供するデスクトップの数を考慮して、十分に対応できる範囲に設定します。たとえば、このポッドで今後 1,000 台以上のデスクトップを提供することが予想される場合は、これ以上の IP アドレス範囲を設定します。2020 年 7 月以降のリリースでは、新機能を使用することで、後でポッドを編集し、ファーム仮想マシンや VDI デスクトップ仮想マシンで使用する仮想マシンのサブネットを追加できます。この新機能によって、ファームおよび VDI デスクトップ割り当ての拡大に対応するために、長期にわたって仮想マシンのサブネットを柔軟に追加できます。ファームおよび VDI デスクトップ割り当ての定義で追加のサブネットを明示的に指定しない限り、このプライマリ仮想マシンのサブネットがデフォルトで使用されるため、ベスト プラクティスとして、このプライマリ仮想マシンのサブネットの範囲を、予想されるファーム仮想マシンおよびデスクトップの台数に十分対応できる範囲に設定します。

- 外部の Unified Access Gateway 構成をポッドの VNet にデプロイする場合、CIDR が /28 以上の DMZ サブネットが必要です。このサブネットは、Unified Access Gateway 仮想マシンの NIC がこの外部ゲートウェイ構成のロード バランサと通信するために使用する IP アドレス用です。管理および DMZ サブネットの範囲を同じ場所に共存させるには、IP アドレスを指定して DMZ サブネット範囲を管理サブネットと同様のものに指定することができます。たとえば、管理サブネットが 192.168.8.0/27 の場合、一致する DMZ サブネットは 192.168.8.32/27 になります。
- 外部の Unified Access Gateway 構成をポッドとは別の専用の VNet にデプロイする場合、その VNet には次の 3 つのサブネットが必要です。
 - 管理サブネット。/27 以上の CIDR が必要です。このサブネットは、ゲートウェイ コネクタ仮想マシンなど、外部ゲートウェイ全体の管理アクティビティに含まれる仮想マシンによって使用される IP アドレスのためのものです。
 - バックエンド サブネット。/27 以上の CIDR が必要です。このサブネットは、Unified Access Gateway 仮想マシンの NIC がポッドの VNet を使用してピアリングされた VNet を介してポッドがプロビジョニングされたファームおよびデスクトップ仮想マシンと通信するために使用する IP アドレス用です。

- フロントエンド (DMZ) サブネット。/28 以上の CIDR が必要です。このサブネットは、Unified Access Gateway 仮想マシンの NIC が外部ゲートウェイのロード バランサと通信するために使用する IP アドレスのためのものです。管理およびフロントエンド サブネットの範囲をこの VNet 内の同じ場所に共存させるには、IP アドレスを指定して DMZ サブネット範囲を管理サブネットと同様のものに指定することができます。たとえば、管理サブネットが 192.168.8.0/27 の場合、マッチしたフロントエンド サブネットは 192.168.8.32/27 になります。

重要： それぞれの CIDR は、プリフィックスとビット マスクの各組み合わせが、プリフィックスを開始 IP アドレスとする IP アドレス範囲になるように定義する必要があります。Microsoft Azure では、CIDR プリフィックスを範囲の先頭にする必要があります。たとえば、192.168.182.48/28 という正しい CIDR の場合、IP アドレス範囲は 192.168.182.48 ~ 192.168.182.63 になり、プリフィックスは開始 IP アドレス (192.168.182.48) と同じになります。ただし、192.168.182.60/28 という間違った CIDR の場合、IP アドレス範囲は 192.168.182.48 ~ 192.168.182.63 になり、開始 IP アドレスは 192.168.182.60 のプリフィックスと同じになりません。CIDR は、開始 IP アドレスが CIDR プリフィックスと一致する IP アドレス範囲になるように定義してください。

前提条件

Microsoft リージョンに、ポッドに使用する VNet があることを確認します。第1世代 Horizon Cloud - Microsoft Azure での必要な仮想ネットワークの構成を参照してください。

サブネットに使用するアドレス範囲が重複しないことを確認します。サブネット範囲が重複していると、ポッド デプロイ ウィザードがエラーを表示します。

手順

1 Microsoft Azure ポータルで、ここで説明したサブネットを作成する必要がある VNet に移動します。

2 [サブネット] をクリックします。

3 [+ サブネット] をクリックします。

[サブネットの追加] 画面が表示されます。

4 必須のフィールドに情報を入力します。

オプション	説明
名前	サブネットの名前を指定します。
アドレスの範囲 (CIDR ブロック)	サブネットの CIDR を入力します。

5 このサブネットを管理サブネットにする場合は、[サービス エンドポイント] セクションで Microsoft.Sql サービスを選択します。

6 [OK] をクリックします。

サブネットは、VNet に追加されます。

7 残りの必要なサブネットを追加するため、手順 3 ~ 5 を繰り返します。

8 外部ゲートウェイを専用の VNet にデプロイする場合は、その VNet のサブネットに対して手順を繰り返します。

結果

注意： ポッドのデプロイのために VNet 上に事前に手動で作成したサブネットは空のままである必要があります。これらのサブネットの IP アドレスを使用しているアイテムを持つ既存のサブネットを再利用しないでください。IP アドレスがサブネットですでに使用されている場合、ポッドがデプロイに失敗したり、その他のダウンストリーム IP アドレスの競合の問題などの問題が発生する可能性が高くなります。これらのサブネットに何らかのリソースを投入したり、IP アドレスを使用したりしないでください。この警告通知には Horizon Cloud からデプロイされたポッドが含まれています。すでにデプロイされているポッドがあるサブネットを再利用しないでください。

次のステップ

作成した管理サブネットに対して、Microsoft.Sql サービスがサービス エンドポイントとして有効になっていることを確認します。第1世代テナント - Microsoft Azure で Horizon Cloud ポッド用に既存のサブネットを使用する場合を参照してください。このサービスはポッドの管理サブネットで有効にする必要があります、外部ゲートウェイを専用の VNet にデプロイする場合、サービスはそのゲートウェイの管理サブネットでも有効にする必要があります。

第1世代テナント - Microsoft Azure で Horizon Cloud ポッド用に既存のサブネットを使用する場合

2019 年 9 月のリリースから、そのリリースのマニフェスト バージョンまたはそれ以降のバージョンを使用して新たにデプロイされた第1世代ポッドと、そのリリースのマニフェスト バージョンまたはそれ以降のバージョンに更新されたポッドの両方について、ポッドの管理サブネットで Microsoft Azure Database for PostgreSQL サービス エンドポイントとのネットワーク通信もサポートされる必要があります。新しいポッドをデプロイする前、または既存のポッドをアップグレードする前に、作成するポッド管理サブネットで、Microsoft.Sql サービスをサービス エンドポイントとして有効にする必要があります。デプロイまたは更新プロセスでは、サブネットにエンドポイントがあるかどうかチェックされ、管理サブネットでエンドポイントが有効になっていない場合は続行されません。このサービス エンドポイントを有効にすることに加えて、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) ルールが管理サブネット上にある場合は、新しいポッドをデプロイしたり既存のポッドをアップグレードしたりする前に、Microsoft Azure Database for PostgreSQL サービスに対するトラフィックを許可するように構成する必要があります。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。KB-92424 で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

重要： 2019 年 12 月のリリースでは、ポッドの外部 Unified Access Gateway 構成をポッドの VNet とは別の専用の VNet にデプロイする機能が導入されています。この機能を使用する場合、外部ゲートウェイの VNet の管理サブネットもこの要件を満たし、Microsoft.Sql サービスをそのサブネット上のサービス エンドポイントとして有効にする必要があります。

2019 年 9 月のリリースでは、Microsoft Azure の Horizon Cloud ポッドの必須要素としての、Microsoft Azure Database for PostgreSQL サービスの使用が導入されています。Microsoft のドキュメントで説明されているように、Microsoft Azure Database for PostgreSQL は、完全に管理されたデータベースとしてのサービスを提供します。ポッドのデプロイまたは更新では、単一サーバのデプロイ タイプを使用して、Microsoft Azure Database for PostgreSQL サーバ リソースがポッドのリソース グループにデプロイされます。デプロイおよび

更新プロセスでは、ポッドの VNet に VNet ルールも自動的に追加されます。この VNet ルールは、ポッドの管理サブネットへの Microsoft Azure Database for PostgreSQL サーバのトラフィックを制限します。ポッドと、その Microsoft Azure Database for PostgreSQL サーバとの間の通信では、管理サブネットを使用します。これにより、ポッドの管理サブネットにいくつかの要件が適用されます。

管理サブネットで、Microsoft.Sql サービスをサービス エンドポイントとして有効にする

デプロイされた Microsoft Azure Database for PostgreSQL サーバの管理サブネットへのトラフィックを制限する VNet ルールでは、サブネットで Microsoft.Sql サービス エンドポイントが有効になっている必要があります。ポッド デプロイヤーによってサブネットが作成されるシナリオでは、デプロイヤーによって、ポッドの管理サブネットが作成する管理サブネット上で有効になっている Microsoft.Sql サービス エンドポイントが確保されます。ただし、管理サブネットを自分で作成する場合は、新しいポッドをデプロイする前、または既存のポッドを更新する前に、管理サブネットが確実にこれらの要件を満たしている必要があります。次のスクリーンショットは、Microsoft Azure ポータルを使用して、サブネット上で Microsoft.Sql サービスをサービス エンドポイントとして有効にする例を示しています。ポータルでサブネットをクリックした後、[サービス エンドポイント] セクションで [サービス] ドロップダウン リストを使用して Microsoft.Sql を選択し、保存します。

g11nv2-mangement ×
vmw-hcs-vnet-westus2

名前 クリップボードにコピー
g11nv2-mangement

サブネット アドレス範囲 * ⓘ
172.168.165.0/27
172.168.165.0 - 172.168.165.31 (27 + 5 個の Azure 予約アドレス)

IPv6 アドレス空間の追加 ⓘ

NAT ゲートウェイ ⓘ
なし

ネットワーク セキュリティ グループ
なし

ルート テーブル
なし

サービス エンドポイント

仮想ネットワークからサービス エンドポイントを介して特定の Azure リソースへのトラフィックを許可する。サービス エンドポイントのポリシーを作成します。 [詳細情報](#)

サービス ⓘ
Microsoft.Storage

サービス	状態
Microsoft.Storage	成功

サービス エンドポイント ポリシー
0 項目が選択されました

保存 **キャンセル**

Microsoft Azure ポータルを使用して管理サブネットに移動し、[サービス] ドロップダウンで Microsoft.Sql を選択することができます。

ファイアウォールまたは NSG で、Microsoft Azure Database for PostgreSQL サービスへのポッド通信が許可されていることを確認する

第 1 世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名にリストされているように、管理サブネットでは、管理サブネットのネットワーク ルールを構成して、ポッドから Microsoft Azure Database for PostgreSQL サービスへの通信を許可する必要があります。新しいポッドをデプロイする前、または既存のポッドを更新する前に、管理サブネットがこの要件を満たしていることを確認する必要があります。

ファイアウォールまたは NSG がサービス タグを使用してアクセスを指定することをサポートする場合は、次のいずれかの方法でポッド通信を許可します。

- グローバル Azure SQL サービス タグ : sql
- ポッドがデプロイされている Azure リージョンの地域固有の SQL サービス タグ:sql.region(Sql.WestUS など)

ファイアウォールまたは NSG がサービス タグを使用してアクセスを指定することをサポートしない場合は、ポッドのリソース グループで作成されたデータベース サーバリソースのホスト名を使用できます。サーバリソースの名前は、*.postgres.database.azure.com のパターンに従います。

セキュリティ グループ内のサービス タグの詳細については、[サービス タグ](#)にある Microsoft Azure ドキュメントのトピックを参照してください。

第 1 世代テナント - Microsoft Azure の Horizon Cloud ポッドに使用する VNet トポロジに必要な DNS サーバの設定

第 1 世代 Horizon Cloud ポッド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。ポッドのデプロイ中に、デプロイヤは Horizon Cloud 制御プレーンの外部アドレスから Microsoft Azure 環境にポッド ソフトウェアを安全にダウンロードします。内部仮想マシン (VM) 名を解決する機能は、Microsoft Azure 環境に展開される仮想マシンでのポッドの Horizon Cloud Active Directory ドメイン参加の操作に必要です。

重要： この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

重要： 最終的には、特定の DNS 名に到達する必要があるポッド関連の仮想マシンでこれを実行できることが重要です。これを実行する必要があるポッド関連の仮想マシンによって内部マシン名と外部名の両方を解決できるように VNet トポロジが構成されている必要があります。ポッドをデプロイする Microsoft Azure で使用している VNet トポロジによって、関連する必要なサブネットにデプロイされたポッド仮想マシンがその DNS 名前解決を取得できることを確認する必要があります。DNS の解決要件の詳細については、[第 1 世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名](#)を参照してください。

外部ゲートウェイをポッドの VNet とは別の専用の VNet にデプロイする機能を使用する場合、前のパラグラフで説明したように、それらの VNet をピアリングする必要があり、ユーザーおよびネットワーク チームは、ピアリングされた VNet トポロジがポッドの主要な DNS 要件を満たすためにそのトポロジの DNS 設定を提供していることを確認する必要があります。Horizon Cloud ドキュメント セットは、ネットワーク チームがユーザーの使用に合わせてカスタマイズした高度な VNet トポロジの詳細については説明しません。

Microsoft Azure サブスクリプションのデフォルトでは、内部ネットワーク接続は設定されていません。本番環境では通常、ユーザーおよびネットワーク チームは、外部名を解決でき、会社のマシン用の Microsoft Azure で動作可能な有効な DNS サーバをポイントするように仮想ネットワークの DNS を設定します。たとえば、Microsoft Windows Server 2016 仮想マシンをその仮想ネットワークにデプロイして DNS サーバとして動作させ、仮想ネットワークの DNS 設定をデプロイされた DNS サーバの IP アドレスをポイントするように構成できます。

概念実証の環境では、組織のプライバシーとセキュリティ ポリシーで許可されている場合、外部の名前解決のために内部 DNS を外部のパブリック DNS に委譲するように構成できます。その目的で、一部の組織や ISP では 208.67.222.222 の OpenDNS や 8.8.8.8 の Google Public DNS など、再帰的パブリック ネーム サーバを提供しています。これらの再帰的パブリック ネーム サーバのサンプル リストについては、Wikipedia の記事「[再帰的パブリック ネーム サーバ](#)」を参照してください。

前提条件

Microsoft Azure リージョンに、ポッド デプロイャ ウィザードで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。[第1世代 Horizon Cloud - Microsoft Azure での必要な仮想ネットワークの構成](#)を参照してください。

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、ポッドの正常なデプロイに必要な特定の外部名に到達して解決できることを確認します。詳細については、[第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名](#)を参照してください。

手順

- 1 Microsoft Azure ポータルで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、ポッド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。

次のステップ

DNS、ポート、およびプロトコルに対するポッド デプロイャのアクセス要件を満たしていることを VNet トポロジから確認します。[第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名](#)および[第1世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件](#)を参照してください。

第 1 世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名

第 1 世代の Horizon Cloud on Microsoft Azure デプロイの Day-0 以降を成功させるには、このドキュメント ページで説明するホスト名が解決可能であり、このページに記載されている特定のポートおよびプロトコルを使用して管理およびテナント サブネットからアクセス可能であるようにする必要があります。

このページについて

VMware ナレッジベースの記事 [KB93762](#) で説明されているように、Horizon インフラストラクチャの監視機能は廃止されました。2023 年 10 月の時点で、廃止された機能に関連するポートとプロトコルの情報はこのページから削除されました。

重要： このページは、第 1 世代のテナント環境があり、その第 1 世代の環境に Horizon Cloud on Microsoft Azure デプロイがある場合にのみ使用します。2022 年 8 月の時点で、Horizon Cloud Service - next-gen は一般公開され、独自の [次世代の使用に関するドキュメント セット](#) はこちらから入手できます。

次世代と第 1 世代のどちらの環境を使用しているかは、環境にログインし、Horizon Universal Console ラベルに表示されるブラウザの URL フィールドのパターンで確認することができます。次世代環境の場合、コンソールの URL アドレスには /hcsadmin/ のような部分が含まれます。第 1 世代コンソールの URL の場合は、異なるセクション (/horizonadmin/) があります。

簡単な紹介

このページに「DNS 名」という語句と「ホスト名」という語句が含まれている理由は、DNS が、これらのホスト名間の通信を行うためにホスト名を解決するためのネットワーク標準であるためです。

ホスト名とは、特定のネットワーク上のマシン インスタンスに割り当てられた一意の名前のことです。ソフトウェア ネットワーク業界で説明されているように、システムは DNS (Domain Name System) を使用して、通信目的でホスト名を IP アドレスに解決します。

ポッドのデプロイ プロセスでは、デプロイされたインスタンスが、このページで説明するホスト名 (DNS 名) に対して、デプロイで選択した VNet を介してネットワーク通信を行う必要があります。

ポッドがサブスクリプションに正常にデプロイされると、新しいソフトウェアが利用可能になったときにポッドのソフトウェアを更新するポッドの更新プロセスと同様に、さまざまな日常のサービス操作で特定のホスト名へのネットワーク アクセスが必要になります。

このページでは、要件について説明します。このページでは、DNS 名という語句とホスト名という語句を同じ意味で使用する場合があります。

いくつかの全体的なキー ポイント

これらの必要な DNS 名について

Horizon Cloud ポッドをデプロイして実行するには、Microsoft Azure VNet を介した特定の DNS アドレスへのネットワーク アクセスが必要です。ポッド デプロイを機能させるには、これらのアドレスへのネットワーク アクセスを許可するようにファイアウォールを構成する必要があります。各 DNS アドレスの目的を次の表に示します。

VNet の DNS 構成では、これらの DNS アドレスへのネットワーク通信を許可するほかに、この記事の説明に従って名前を解決する必要があります。

ポッド マネージャの VNet とは別の専用の VNet に外部ゲートウェイをデプロイするオプションを選択する場合、その VNet のサブネットは、ポッド マネージャの VNet の管理サブネットと同じ DNS 要件を満たす必要があります。

ポッド デプロイヤーとそのワークフローに加えて、さまざまなサービス機能は、エンドツーエンドで動作するために特定の DNS アドレスへのアクセスを必要とします。これらの DNS 名は、次の表にも記載されています。

これらの DNS 名の一部には、地域の要素があります。

VMware エコシステム内の緊密な連携で説明されているように、Horizon Cloud は、幅広い VMware エコシステムから入手可能な他の製品と併用できます。これらの他の製品には、追加の DNS 要件がある場合があります。このような追加の DNS 要件については、ここでは詳しく説明しません。このような DNS 要件については、ポッドと統合する特定の製品のドキュメント セットを参照してください。

ポッドのデプロイ後の、サービス関連の継続的な運用のためのポートおよびプロトコルについて

ポッドが正常にデプロイされたら、Horizon Cloud の継続的な運用のためには特定のポートおよびプロトコルが必要です。詳細については、[第 1 世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件](#)を参照してください。

第 1 世代テナント - 地域別の制御プレーンの DNS 名

「Horizon Service へようこそ」E メールには、自分のテナント アカウントがどの地域の制御プレーン インスタンスで作成されたかが示されます。「ようこそ」E メールが送信されたときに存在していた既知の問題により、受信した E メールには判読可能な名前ではなく、リージョンで使用されているシステム文字列名が表示されることがあります。「ようこそ」E メールにシステム文字列の名前が表示されている場合は、次の表を使用して、E メールに表示される文字列と地域別制御プレーンの DNS 名を関連付けることができます。

表 6-14. 地域別制御プレーンの DNS 名にマッピングされた「ようこそ」E メール内の地域

「ようこそ」E メール内の記載	地域別の DNS 名
USA	cloud.horizon.vmware.com
EU_CENTRAL_1 または Europe	cloud-eu-central-1.horizon.vmware.com
AP_SOUTHEAST_2 または Australia	cloud-ap-southeast-2.horizon.vmware.com
PROD1_NORTHCENTRALUS2_CP1 または USA-2	cloud-us-2.horizon.vmware.com
PROD1_NORTHEUROPE_CP1 または Europe-2	cloud-eu-2.horizon.vmware.com
PROD1_AUSTRALIAEAST_CP1 または Australia-2	cloud-ap-2.horizon.vmware.com
Japan	cloud-jp.horizon.vmware.com
UK	cloud-uk.horizon.vmware.com
Europe-3	cloud-de.horizon.vmware.com

ポッドの全体的なデプロイ プロセス、ポッドの更新、各種サービス機能の有効化、および継続的な運用に関するホスト名、DNS の要件

サービスの機能をエンドツーエンドで正しく使用するには、次のホスト名が解決可能であり、次の表に記載されている特定のポートおよびプロトコルを使用して管理およびテナント サブネットからアクセス可能であるようにする必要があります。特定のホスト名にアクセスできる必要があるサービス機能には、次のようなものがあります。

- ポッド マネージャ ベースのポッドを Microsoft Azure サブスクリプションに自動的にデプロイするポッド デプロイヤ
- ポッドのソフトウェアをより新しいソフトウェア バージョンに更新するポッド更新機能
- Marketplace からのインポート ウィザードを使用するイメージのインポート プロセス
- 自動エージェント更新 (AAU) などのエージェント関連機能
- Universal Broker
- Cloud Monitoring Service (CMS) に関連する機能

特にポッドのデプロイとポッドの更新の場合

次のホスト名が解決可能であり、次の表に記載されている特定のポートおよびプロトコルを使用して管理およびテナント サブネットからアクセス可能であるようにする必要があります。これらのワークフローで使用されるアプライアンスは、特定の送信ポートを使用して、これらのプロセスに必要なソフトウェアを Microsoft Azure 環境に安全にダウンロードします。これらの DNS 名は、適切なワークフロー関連アプライアンスがクラウドの制御プレーンと通信するためにも使用されます。

新しいポッドのデプロイの場合、ネットワーク ファイアウォール、ネットワーク セキュリティ グループ (NSG) ルール、およびプロキシ サーバを構成する必要があります。これにより、主要なデプロイ関連アプライアンスは、必要なポートで DNS アドレスにアクセスできます。そうしないと、ポッドのデプロイ プロセスは失敗します。

外部ゲートウェイを専用の VNet にデプロイする機能を使用している場合

その VNet の管理サブネットは、ポッドの VNet の管理サブネットについて以下の表に記載されているものと同じ DNS 要件を満たしている必要があります。外部ゲートウェイ VNet のバックエンド サブネットと DMZ サブネットには、特定の DNS 要件はありません。

外部ゲートウェイ、内部ゲートウェイ、またはその両方を使用してポッドをデプロイする場合

ポッド デプロイヤがこれらのゲートウェイ構成で構成する証明書をアップロードする必要があります。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 ゲートウェイ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、ポッドのデプロイは接続中フェーズにおいて失敗します。これらの名前は、証明書の取得に使用した CA に大きく依存しているため、VMware のコントロールには含まれません。

App Volumes on Azure 機能を使用する場合

ポッド デプロイは、ポッド マネージャのリソース グループ内で、ポッドの App Volumes on Azure 機能で使用する Azure ストレージ アカウントをプロビジョニングします。プロビジョニングすると、Azure Cloud は、*.file.core.windows.net のパターンを持つ完全修飾ドメイン名 (FQDN) をそのストレージ アカウントに割り当てます。ここで、* は、Azure によって生成されたストレージ アカウントの名前です。この FQDN は、App Volumes がそのストレージ アカウントの基盤となるファイル共有にアクセスしてマウントし、App Volumes 機能を提供できるように、DNS サーバによって解決できる必要があります。ポッド マネージャ インスタンス内で実行される App Volumes Manager プロセスと、VDI デスクトップで実行される App Volumes Agent について、DNS サーバが常にその FQDN を解決するようにする必要があります。このエンドポイントは、Microsoft Azure クラウド環境内の Microsoft Azure エンドポイントであり、接続は Microsoft Azure クラウド スペース内で直接行われます。

テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件

次の表に、テナント全体に適用できる新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件を示します。

2021 年の初めより、サービスの地域別制御プレーン インスタンスにアップグレードした結果、どの地域別制御プレーン インスタンスにおいても dlmes20qfad06k.cloudfront.net DNS 名は不要になりました。すべての地域別制御プレーン インスタンスで、hydra-softwarelib-cdn.azureedge.net DNS 名が使用されるようになりました。次の表は、現状に合わせた内容になっています。

注： この表の プロキシ トラフィック 列は、Horizon Cloud on Microsoft Azure デプロイの構成にプロキシが含まれている場合にネットワーク トラフィックがプロキシを通過するかどうかを示します。プロキシ トラフィック 列に「いいえ」と表示されている場合、デプロイの構成にプロキシが含まれている場合でも、表に示されているホスト名へのネットワーク トラフィックを許可する必要があります。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件

サブネット ソース	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
管理	<p>Horizon Cloud テナント アカウントで指定されている地域別制御プレーンのインスタンスに応じた、次のいずれかの名前。地域別のインスタンスは、Microsoft Azure および Horizon ポッドの Horizon Cloud へのデプロイとオンボーディングの記載どおりに、アカウントの作成時に設定されます。</p> <ul style="list-style-type: none"> ■ cloud.horizon.vmware.com ■ cloud-us-2.horizon.vmware.com ■ cloud-eu-central-1.horizon.vmware.com ■ cloud-eu-2.horizon.vmware.com ■ cloud-ap-southeast-2.horizon.vmware.com ■ cloud-ap-2.horizon.vmware.com ■ cloud-jp.horizon.vmware.com ■ cloud-uk.horizon.vmware.com ■ cloud-de.horizon.vmware.com 	443	TCP	はい	<p>地域別制御プレーンのインスタンス</p> <ul style="list-style-type: none"> ■ 米 国 : cloud.horizon.vmware.com ■ ヨーロッパ : cloud-eu-central-1.horizon.vmware.com ■ cloud-eu-2.horizon.vmware.com

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件

サブネット ソース	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
					n.v mw are. com ■ アジ ア パ シフ ィツ ク : clou d- ap- sout hea st-2. hori zon. vm war e.co m, clou d- ap- 2.ho rizo n.v mw are. com ■ 日 本 : clou d- jp.h oriz on.v mw are. com ■ 英 国 : clou d- uk.h

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
					oriz on.v mw are. com ■ ドイ ツ: clou d- de.h oriz on.v mw are. com
管理	softwareupdate.vmware.com	443	TCP	はい	VMwar e 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 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。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	hydra-softwarelib-cdn.azureedge.net	443	TCP	いいえ ポッド マ ネージャ と Unified Access Gatewa y バイナ リ マニフ ェストは ここに保 存され、 ここから 提供され ます。こ れらのマ ニフェス トは、ポ ッドとゲ ートウェ イのデブ ロイおよ びアップ グレード 時にのみ 使用され ます。こ のエンド ポイント へのこの 接続は、 プロキシ 経由では なく直接 行われる ように構 成されま す。	Horizon Cloud コンテン ツ配信サ ーバ。管 理サブネ ットで は、この サイト は、ポッ ド インフ ラストラ クチャで 使用され る必要な バイナリ をダウン ロードす るサービ スによっ て使用さ れます。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	packages.microsoft.com	443 および 11371	TCP	いいえ このサイ トは、ア プリーケー ションお よびサー ビスの外 部にあり ます。し たがっ て、接続 は構成さ れたプロ キシを使 用しませ ん。 このエン ドポイン トは、 Microso ft Azure クラウド 環境内の Microso ft Azure エンドポ イントで あり、接 続は Microso ft Azure クラウド スペース 内で直接 行われま す。	Microso ft ソフト ウェア パ ッケージ サーバ。 Microso ft Azure コマンド ライン イン ターフェ イス (CLI) ソ フトウェ アを安全 にダウン ロードす るために 使用しま す。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	azure.archive.ubuntu.com	80	TCP	いいえ このサイ トは、ア プリーケー ションお よびサー ビスの外 部にあり ます。し たがっ て、接続 は構成さ れたプロ キシを使 用しませ ん。 このエン ドポイン トは、 Microso ft Azure クラウド 環境内の Microso ft Azure エンドポ イントで あり、接 続は Microso ft Azure クラウド スペース 内で直接 行われま す。	Ubuntu ソフトウ ェア バッ ケージ サー バ。 Ubuntu オペレー ティング システム の更新用 にポッド 関連の Linux ベ ースの仮 想マシン によって 使用され ます。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	api.snapcraft.io	443	TCP	いいえ このエン ドポイン トは、ア プリケー ションお よびサー ビスの外 部にあり ます。接 続は構成 されたプ ロキシを 使用しま せん。	Ubuntu ソフトウ ェア バッ ケージ サ ーバ。ポ ッド マネ ージャと Unified Access Gatewa y インス タンス は、 Ubuntu オペレー ティング システム を実行し ます。こ れらの Ubuntu オペレー ティング システム は、この Ubuntu サイトか ら Ubuntu オペレー ティング システム の更新を 取得する ように構 成されて います。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	archive.ubuntu.com	80	TCP	いいえ このエン ドポイン トは、ア プリケー ションお よびサー ビスの外 部にあり ます。接 続は構成 されたプ ロキシを 使用しま せん。	Ubuntu ソフトウ ェア バッ ケージ サ ーバ。ポ ッド マネ ージャと Unified Access Gatewa y インス タンス は、 Ubuntu オペレー ティング システム を実行し ます。こ れらの Ubuntu オペレー ティング システム は、この Ubuntu サイトか ら Ubuntu オペレー ティング システム の更新を 取得する ように構 成されて います。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	changelogs.ubuntu.com	80	TCP	いいえ このサイ トは、ア プリーケー ションお よびサー ビスの外 部にあり ます。し たがっ て、接続 は構成さ れたプロ キシを使 用しませ ん。	Ubuntu ソフトウ ェア バッ ケージ サ ーバ。ポ ッド マネ ージャと Unified Access Gatewa y インス タンス は、 Ubuntu オペレー ティング システム を実行し ます。こ れらの Ubuntu オペレー ティング システム は、この Ubuntu サイトを 使用して Ubuntu オペレー ティング システム の更新を 追跡する ように構 成されて います。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	security.ubuntu.com	80	TCP	いいえ このエンド ポイント は、ア プリー ケー ション およ びサ ー ビ ス の 外 部 に あ り ま す。 接 続 は 構 成 さ れ た プ ロ キ シ を 使 用 し ま せ ん。	Ubuntu ソフ トウ ェア バツ ケー ジ サ ー バ。 ポ ッド マ ネ ー ジャ と Uni fied Acc ess Gat ewa y イ ンス タ ンス は、 Ubu ntu オペ レー ティ ング シス テム を 実 行 し ま す。 こ れ ら の Ubu ntu オペ レー ティ ング シス テム は、 こ の Ubu ntu サイ トを 使 用 し て セ キュ リ ティ 関 連 の Ubu ntu オペ レー ティ ング シス テム の 更 新 を 実 行 す る よ う に 構 成 さ れ て い ま す。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	esm.ubuntu.com	80 および 443	TCP	いいえ このエン ドポイン トは、ア プリーケー ションお よびサー ビスの外 部にあり ます。接 続は構成 されたプ ロキシを 使用しま せん。	Ubuntu ソフトウ ェア バッ ケージ サ ーバ。ポ ッド マネ ージャと Unified Access Gatewa y インス タンス は、 Ubuntu オペレー ティング システム を実行し ます。こ れらの Ubuntu オペレー ティング システム は、この Ubuntu サイトを 使用し て、 Ubuntu ベース OS およ びスケー ルアウト インフラ ストラク チャ内の 高度で重 大な CVE (Comm on Vulnera bilities and Exposu

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
					res) に対 するセキ ュリティ 更新を追 跡するよ うに構成 されてい ます。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	<p>ポッドをデプロイする Microsoft Azure クラウドに 応じて、以下のいずれかになります。</p> <ul style="list-style-type: none"> ■ Microsoft Azure (グローバル) : login.microsoftonline.com ■ Microsoft Azure Germany : login.microsoftonline.de ■ Microsoft Azure China : login.chinacloudapi.cn ■ Microsoft Azure US Government : login.microsoftonline.us 	443	TCP	はい	<p>この Web ア ドレスは 通常、ア プリケー ションに よって Microso ft Azure サービ スを認証 するた めに使 用され ます。 Microso ft Azure ドキュ メント での関 連する 説明に ついて は、 「OAuth 2.0 承認 コード フロー」、 「Azure Active Directo ry v2.0 および OpenID Connect プロト コル」、 およ び 「Nation al Clouds」 を参照 してく ださい。 「Nation al Clouds」 のトピ ックで は、</p>

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
					各 Microso ft Azure Nationa l Cloud に対応す る Azure AD 認証 エンドポ イントの 相違点に ついて説 明しま す。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	<p>ポッドをデプロイする Microsoft Azure クラウドに 応じて、以下のいずれかになります。</p> <ul style="list-style-type: none"> ■ Microsoft Azure (グローバル) : management.azure.com ■ Microsoft Azure Germany : management.microsoftazure.de ■ Microsoft Azure China : management.chinacloudapi.cn ■ Microsoft Azure US Government : management.usgovcloudapi.net 	443	TCP	はい	<p>Microsoft Azure Resource Manager エンドポイントへのポッド 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</p>

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
					を提供し ます。
管理	ポッドをデプロイする Microsoft Azure クラウドに 応じて、以下のいずれかになります。 <ul style="list-style-type: none"> ■ Microsoft Azure (グローバル) : graph.windows.net ■ Microsoft Azure Germany : graph.cloudapi.de ■ Microsoft Azure China : graph.chinacloudapi.cn ■ Microsoft Azure US Government : graph.windows.net 	443	TCP	はい	Azure Active Directo ry (Azure AD) Graph API への アクセ ス。これ は、 OData REST API エン ドポイン トを介し た Azure Active Directo ry (Azure AD) へ のポッド によるブ ログラム アクセス に使用さ れます。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	<p>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、以下のいずれかになります。</p> <ul style="list-style-type: none"> ■ グローバル Azure SQL サービス タグ : <code>Sql</code> ■ ポッドがデプロイされている Azure リージョンの地域固有の SQL サービス タグ : <code>Sql.region</code> (<code>Sql.WestUS</code> など) <p>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ない場合は、データベースのホスト名を使用できません。この名前は、<code>*.postgres.database.azure.com</code> のパターンに従います。</p>	5432	TCP	いいえ このエンドポイントは、Microsoft Azure クラウド環境内の Microsoft Azure PostgreSQL データベースサービスです。接続は、Microsoft Azure クラウドスペース内で直接行われます。	この Horizon Cloud on Microsoft Azure デプロイ用に構成された Microsoft Azure PostgreSQL データベースサービスへのポッド通信に使用されます。セキュリティグループ内のサービスタグの詳細については、 サービス タグ にある Microsoft Azure ドキュメントのトピックを参照してください。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	<p>Horizon Cloud テナント アカウントで指定されている地域別制御プレーンのインスタンスに応じた、次のいずれかの名前。地域別のインスタンスは、Microsoft Azure および Horizon ポッドの Horizon Cloud へのデプロイとオンボーディングの記載どおりに、アカウントの作成時に設定されます。</p> <ul style="list-style-type: none"> ■ connector-azure-us.vmwarehorizon.com ■ connector-azure-eu.vmwarehorizon.com ■ connector-azure-aus.vmwarehorizon.com ■ connector-azure-jp.vmwarehorizon.com ■ connector-azure-uk.vmwarehorizon.com ■ connector-azure-de.vmwarehorizon.com 	443	TCP	はい	<p>Universal Broker サービスのリージョン インスタンス</p> <ul style="list-style-type: none"> ■ 米 国 : connector-azure-us.vmwarehorizon.com ■ ヨーロッパ : connector-azure-eu.vmwarehorizon.com ■ オーストラリア : connector-azure-aus.vm

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
					war eho rizo n.co m ■ 日 本： con nec tor- azur e- jp.v mw are hori zon. com ■ 英 国： con nec tor- azur e- uk.v mw are hori zon. com ■ ドイ ツ： con nec tor- azur e- de.v mw are hori zon. com

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	<p>Horizon Cloud アカウントにどの地域別制御プレーンが適用されているかに応じて異なります。</p> <ul style="list-style-type: none"> ■ 北米 : kinesis.us-east-1.amazonaws.com ■ ヨーロッパ、ドイツ : kinesis.eu-central-1.amazonaws.com ■ オーストラリア : kinesis.ap-southeast-2.amazonaws.com ■ 日本 : kinesis.ap-northeast-1.amazonaws.com ■ 英国 : kinesis.eu-west-2.amazonaws.com 	443	TCP	はい	Cloud Monitoring Service (CMS)

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
管理	<ul style="list-style-type: none"> ■ *.blob.core.windows.net: ■ sauron-jp.horizon.vmware.com 	443	TCP	いいえ	<p>*.blob.c ore.win dows.n et エンド ポイントは、 Azure BLOB ス トレージ へのプロ グラムに よるアク セスに使 用されま す。この エンドポ イントは Microso ft Azure クラウド 環境内の Microso ft Azure エンドポ イントで あり、そ のエンド ポイント との通信 は Microso ft Azure クラウド スペース 内で直接 行いま す。 sauron- jp.horiz on.vmw are.com エンドポ イントを 使用する と、 VMwar</p>

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
					<p>e 監視システムは、VMware 管理対象インスタンスのセキュリティイベントを検出できます。展開されたインスタンスに対する VMware の管理責任を有効にします。これには、これらのインスタンスのシステム監視 VMware 必須である必要があります。</p>

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
テナント	hydra-softwarelib-cdn.azureedge.net	443	TCP	いいえ	Horizon Cloud コンテンツ配信サーバー。テナント サブネットでは、このサイトは、システムの自動化された [Market place からのイメージのインポート] ワークフローやエージェント ベアリング ワークフローに関連するプロセスを含む、さまざまなシステム イメージ関連のプロセスによって使用されます。

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
テナント	scapi.vmware.com	443	TCP	いいえ	VMware Service Usage Data Program に使用される VMware Cloud Services。テナントサブネットから送信される場合、ポッドプロビジョニングされたデスクトップインスタンスおよびファームウェアサーバーインスタンスの Horizon Agent は、エージェント関連の構成情報を送信します。
テナント	*.file.core.windows.net	445	TCP	いいえ	このエンドポイントは、Microsoft Azure クラウド環境内の Microsoft App Volumes on Azure 機能に使用されます。ポッドマネージャのリ

表 6-15. テナント全体に適用される新しいポッドのデプロイ、ポッドの更新、およびサービス運用の DNS 要件 (続き)

サブネット ソース	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
				ft Azure ファイル ストレ ージサー ビスです。 接続は、 Microso ft Azure クラウド スペース 内で直接 行われま す。	ソース グ ループ内 の SMB ファイル 共有への プログラ ムによる アクセス に使用さ れ、その SMB ファ イル共 有に格納 されてい る App Volume s AppSta ck にア クセスし ます。

VMware システム監視の必須要件 - monitor.horizon.vmware.com

このセクションで説明する必須要件により、VMware 監視システムは、Horizon Cloud on Microsoft Azure 環境の管理サブネット、テナント サブネット、および DMZ サブネットにデプロイされている VMware 管理対象インスタンスのセキュリティ イベントを検出できます。

Horizon Cloud on Microsoft Azure 環境の場合、VMware は、ポッド マネージャ インスタンス、Unified Access Gateway インスタンス、App Volumes に関連する Azure ファイル、Azure PostgreSQL サービス、およびトラブルシューティングが必要な場合はサポート関連のジャンプ ボックス インスタンスなどのリソースを制御および管理します。

デプロイされたインスタンスに対する VMware の管理責任には、これらのインスタンスの必須の VMware システム監視が必要です。

この必須の VMware システム監視は、次に説明する要件を満たす必要があります。

大まかに説明すると、デプロイのインスタンスは、ポート 1514 (TCP および UDP) およびポート 1515 (TCP および UDP) でホスト名 `monitor.horizon.vmware.com` に送信で到達する必要があります。

注： 外部ゲートウェイ構成の Unified Access Gateway インスタンスは、DMZ ネットワークからの `monitor.horizon.vmware.com` を解決する必要があります。

重要： Horizon Cloud on Microsoft Azure 展開でプロキシトラフィックが構成されている場合は、プロキシを経由せずにこれらのエンドポイントと通信する必要があります。このステートメントは、エンドポイントが TCP/UDP と TCP/UDP `monitor.horizon.vmware.com:1514` `monitor.horizon.vmware.com:1515` 意味します。「送信通信にプロキシまたはファイアウォールを使用している場合に適用される要件」という見出しの後のテキストを参照してください。

ネットワークで SSL インспекションが有効になっている場合に適用される要件

ネットワークで SSL インспекションが有効になっている場合は、ホスト `monitor.horizon.vmware.com` を除外するように指定する必要があります。

環境に内部ゲートウェイ構成がある場合に適用される要件

ナレッジベースの記事 [KB90145](#) のすべての手順と情報に従って、内部ゲートウェイ構成の送信通信を確立する必要があります。最後にある注意事項を含め、ナレッジベース記事のすべての説明に従ってください。

さらに送信通信にプロキシまたはファイアウォールを使用する場合は、送信通信にプロキシまたはファイアウォールを使用する場合に適用可能な次の要件を満たす必要があります。

送信通信にプロキシまたはファイアウォールを使用している場合に適用される要件

送信通信にプロキシまたはファイアウォールを使用する場合は、次のようにプロキシまたはファイアウォールで通信を許可する必要があります。

- 商用環境 - 1514 (TCP および UDP) および 1515 (TCP および UDP) でホスト名 `monitor.horizon.vmware.com` を許可します
- 米国連邦環境 - VMware Federal Support でケースを開き、監視システムのホスト名を要求してください。

このような環境では、次のソースに対して前述の通信を許可する必要があります。

- 管理 - ポッド マネージャ インスタンス
- DMZ - 外部ゲートウェイ構成の Unified Access Gateway インスタンス
- テナント - 内部ゲートウェイ構成の Unified Access Gateway インスタンス

注： 環境に内部ゲートウェイ構成がある場合は、内部ゲートウェイ構成に適用可能な前述の要件である、[ナレッジベースの記事 KB90145](#) の手順を満たす必要があります。

アクティブなサポート リクエストに必要な場合は、一時的なジャンプ ボックス ポートとプロトコル

VMware にサポート リクエストを発行し、サポート チームがそのリクエストを処理する方法として、VMware が管理するアプライアンスとの SSH 通信用の一時的なジャンプ ボックス仮想マシンをデプロイすることを決めた場合、そのジャンプ ボックスにはここで説明するポートとプロトコルが必要です。

サポート関連のジャンプ ボックス デプロイの権限がお客様から要求されます。VMware サポート チームは、サポート状況に応じて必要な情報をお客様に通知します。

このサポート関連のジャンプ ボックス仮想マシンは、次の宛先への送信元として通信するように設計されています。

- SSH およびポート 22 を使用するポッドのポッド マネージャ仮想マシンのポート 22。
- HTTPS を使用する Unified Access Gateway 仮想マシンのポート 9443。
- 外部ゲートウェイが専用の VNet にデプロイされている環境で、SSH を使用するゲートウェイ コネクタ仮想マシンのポート 22。

これらの仮想マシンには IP アドレスが動的に割り当てられているため、次のネットワーク ルールを使用して、説明されている通信を行うことができます。サポート リクエスト活動中は、サポート関連のジャンプ ボックス デプロイの要件について、VMware のサポートからのガイダンスと監督を受けるようにしてください。

- 接続元と接続先の両方としての管理サブネット CIDR（接続先ポート：22、接続元ポート：任意、プロトコル：TCP）。
- 接続元と接続先の両方としての管理サブネット CIDR（接続先ポート：9443、接続元ポート：任意、プロトコル：TCP、Unified Access Gateway 構成が関係する場合）。

第1世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件

このページは、一般的な第1世代 Horizon Cloud Service on Microsoft Azure 環境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ポッドの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。

このページについて

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

注： [VMware ナレッジベースの記事 KB93762](#) で説明されているように、Horizon インフラストラクチャの監視機能は廃止され、第1世代のテナントではこの機能を有効化したり使用したりできなくなります。2023年10月の時点で、廃止された機能に関連するポートとプロトコルの情報はこのページから削除されました。

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 Cloud Service on Microsoft Azure 環境で使用する機能によって多少異なります。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、ポッドのデプロイと日常の運用のためのネットワーク トラフィックには、特定のホスト名の要件があります。

ネットワーク トラフィックは特定のホスト名に到達する必要があります。デプロイがプロキシを使用するように構成されている場合、一部のネットワーク サービスがプロキシを使用し、その他のネットワーク サービスは直接接続されることが予想されます。ホスト名へのネットワーク トラフィックの詳細については、[第 1 世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名を参照してください](#)。

VMware 製品でサポートされているその他のポートの詳細については、[VMware Ports and Protocols](#) を参照してください。

ポッドのデプロイ プロセスの一環として、デプロイヤーはデプロイされたすべての仮想マシンのネットワーク インターフェイス (NIC) にネットワーク セキュリティ グループ (NSG) を作成します。これらの NSG で定義されているルールの詳細については、[Horizon Cloud ポッド内の仮想マシンに対する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](#)を参照してください。

継続的な運用のために主要なポッド コンポーネントで必要となるポートとプロトコル

DNS の要件に加えて、次の表には、デプロイ後に進行中の操作に関してポッドが正常に操作されるために必要なポートおよびプロトコルが記載されています。これらの表の一部には、特定のシナリオで必要なポートとプロトコル、またはポッドで特定の機能を有効にした場合に必要なポートとプロトコルも記載されます。

Microsoft Azure ポータルでは、ポッド マネージャ仮想マシンには `vmw-hcs-podID` (`podID` はポッドの UUID) や `node` を含む名前が付けられます。

注： v2204 サービス リリース以降、新しい Horizon Cloud Service on Microsoft Azure 展開はデフォルトで高可用性が構成された状態でデプロイされます。展開には 2 台のポッド マネージャ仮想マシンがあります。次の表で、「ポッド マネージャ仮想マシン」という語句が表示されている場合は、特に指定されていない限り、両方のポッド マネージャ仮想マシンに適用されます。

システムでの Microsoft Azure ロード バランサとポッド マネージャ仮想マシンの使用は、マニフェスト 1600 (2019 年 9 月のサービス リリース) から開始されました。したがって、マニフェスト 1600 以降で新しくデプロイされたすべてのポッドには、ポッドの Microsoft Azure ロード バランサが 1 台あります。マニフェスト 1600 より前に最初にデプロイされ、その後以降のマニフェストに更新されたポッドにも、ポッドの Microsoft Azure ロード バランサが 1 台あります。ポッドのロード バランサに言及する表の行は、このようなすべてのポッドに適用されます。

表 6-16. ポッドの操作に関するポートおよびプロトコル

ソース	ターゲット	ポート	プロトコル	目的
ポッド マネージャ仮想マシン	ポッドのその他のポッド マネージャ仮想マシン	4101	TCP	このトラフィックは、ポッド マネージャ仮想マシン間の JMS ルーティングです。
ポッド マネージャ仮想マシン	Unified Access Gateway 仮想マシン	9443	HTTPS	このポートは、ポッドの 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ポッド マネージャ仮想マシンによって使用されます。このポート要件は、最初にポッドを Unified Access Gateway 構成でデプロイするときと、ポッドを編集して Unified Access Gateway 構成を追加またはその Unified Access Gateway 構成の設定を更新するときに適用されます。
ポッドの Microsoft Azure ロード バランサ	ポッド マネージャ仮想マシン	8080	HTTP	ロード バランサのバックエンド プール内の仮想マシンの健全性チェック。 v2204 リリースより前にデプロイされた、高可用性トグルが設定されておらず、高可用性がまだ追加されていないポッドの場合、ロード バランサのバックエンド プールにはチェックするポッド マネージャ仮想マシンが 1 台あります。
ポッド マネージャ仮想マシン	ドメイン コントローラ	389	TCP UDP	Active Directory への Horizon Cloud テナントの登録が必要です。最初のポッドをオンボーディングした後に、コンソールの [Active Directory ドメインの登録] ワークフローを実行する必要があります。 LDAP がそのワークフローで指定される場合、このポートは LDAP 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。
ポッド マネージャ仮想マシン	グローバル カタログ	3268	TCP	Active Directory への Horizon Cloud テナントの登録が必要です。最初のポッドをオンボーディングした後に、コンソールの [Active Directory ドメインの登録] ワークフローを実行する必要があります。 LDAP がそのワークフローで指定されたプロトコルになる場合、LDAP サービスにはこのポートが必要です。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 構成にグローバル カタログ ロールを含むサーバです。
ポッド マネージャ仮想マシン	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 へのポッドの登録が必要です。
ポッド マネージャ仮想マシン	ドメイン コントローラ	636、 3269	TCP	Active Directory への Horizon Cloud テナントの登録が必要です。最初のポッドをオンボーディングした後に、コンソールの [Active Directory ドメインの登録] ワークフローを実行する必要があります。 これらのポートは、LDAPS がその登録済み Active Directory の構成で指定されたプロトコルになる場合のみ、LDAP over SSL (LDAPS) サービスに必要です。LDAPS は、テナントがサービスの LDAPS 機能の使用を有効にしている場合にのみ、登録済み Active Directory に対して指定できます。それ以外の場合は、デフォルトで LDAP が必要です。
ポッド マネージャ仮想マシン	DNS サーバ	53	TCP UDP	DNS サービス。
ポッド マネージャ仮想マシン	NTP サーバ	123	UDP	NTP サービス。NTP の時刻同期を提供するサーバ。

表 6-16. ポッドの操作に関するポートおよびプロトコル (続き)

ソース	ターゲット	ポート	プロトコル	目的
ポッド マネージャ仮想マシン	True SSO 登録サーバ	32111	TCP	True SSO 登録サーバ。Horizon ポッドで True SSO を使用している場合に必要です。 32111 は、登録サーバのインストールで使用されるデフォルトのポートです。このポート番号は、必要に応じて登録サーバのインストール中に構成できます。 このトピックの True SSO 、 証明書管理 、および Horizon Cloud on Microsoft Azure 環境 セクションも参照してください。
ポッド マネージャ仮想マシン	Workspace ONE Access サービス	443	HTTPS	注： この行は、シングルポッド ブローカ構成の環境に適用されます。この情報は、Universal Broker 構成の環境ではありません。シングルポッド ブローカによって構成された環境では、Workspace ONE Access Connector はポッドと通信してエンドユーザーの資格 (割り当て) を取得します。 Workspace ONE Access をポッドと統合していない場合は省略できます。シングルポッド ブローカによって構成された環境では、この接続を使用して、ポッドと Workspace ONE Access サービスの間に信頼関係が作成され、Workspace ONE Access Connector はポッドと同期されます。使用中の Workspace ONE Access 環境に対して、ポッドがポート 443 でアクセスできることを確認します。Workspace ONE Access クラウド サービスを使用している場合、Workspace ONE Access Connector およびポッドがアクセス権を持つ必要のある、Workspace ONE Access サービスの IP アドレスのリスト (VMware のナレッジベースの記事 KB2149884 にある) も参照してください。

ゲートウェイ コネクタ仮想マシンのポートとプロトコルの要件

この表は、外部ゲートウェイを別の VNet にデプロイしたときに使用されるゲートウェイのコネクタ仮想マシンに適用されます。DNS の要件に加えて、デプロイ後に継続的な運用に関して外部ゲートウェイが正常に操作されるためには、次の表に記載されたポートおよびプロトコルが必要です。

次の表では、コネクタ仮想マシンという用語は、クラウド管理プレーンと外部ゲートウェイ間の接続を管理するゲートウェイのコネクタ仮想マシンを指します。Microsoft Azure ポータルでは、この仮想マシンには `vmw-hcs-ID` (`ID` はゲートウェイのデプロイ ID) や `node` を含む名前が付けられます。

表 6-17. ポッドの操作に関するポートおよびプロトコル

ソース	ターゲット	ポート	プロトコル	目的
コネクタ仮想マシン	DNS サーバ	53	TCP UDP	DNS サービス。
コネクタ仮想マシン	NTP サーバ	123	UDP	NTP サービス。NTP の時刻同期を提供するサーバ。

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

DNS および上記のプライマリ ポートとプロトコルの要件に加え、次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適切に動作するようにポッドで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高可用性が有効なポッドを使用した接続では、トラフィックは次の表に記載されているようにポッドの Unified Access Gateway インスタンスからターゲットに対して許可される必要があります。ポッドのデプロイ中に、ネットワーク セキュリティ グループ (NSG) は、ポッドの Unified Access Gateway インスタンスによる使用に対応するために Microsoft Azure 環境に作成されます。

表 6-18. ポッドの Unified Access Gateway インスタンスからのトラフィックに関するポートの要件

ソース	ターゲット	ポート	プロトコル	目的
Unified Access Gateway	ポッドの Microsoft Azure ロード バランサ	8443	TCP	ログイン認証トラフィック。Unified Access Gateway インスタンスからのトラフィックは、ポッドのロード バランサを経由してポッド マネージャ仮想マシンに到達します。
Unified Access Gateway	NTP サーバ	123	UDP	<p>NTP サービス。NTP の時刻同期を提供するサーバ。</p> <p>テナントが Universal Broker を使用するように構成されている場合は、以下の要件が満たされていることを確認してください。</p> <ul style="list-style-type: none"> ■ 外部 Unified Access Gateway 構成には、DMZ サブネットから NTP サーバへの接続が必要です。 ■ 内部 Unified Access Gateway 構成には、テナント サブネットから NTP サーバへの接続が必要です。 <p>理由は、サービスが Unified Access Gateway アプライアンスと UTC (協定世界時) を実行している Universal Broker の NTP サーバとの間に時刻ドリフトがあることを検出すると、時刻ドリフトに対処するように求める E メールが送信されるためです。Universal Broker と Unified Access Gateway アプライアンス間の時刻ドリフトにより、エンドユーザー接続が失敗することがあります。内部 Unified Access Gateway 構成がテナント サブネットから NTP サーバに接続されていない場合、このような時刻ドリフトが発生する可能性が高くなります。理由は、NTP サーバがない場合、これらの Unified Access Gateway アプライアンスは基盤となる仮想マシンの時刻に依存するためです。</p> <p>使用する NTP サーバが内部 NTP サーバであり、DMZ インターフェイスからの通信が許可されていない場合は、SR を開いて、デプロイ後に VMware Horizon Cloud Service チームが Unified Access Gateway 構成へのルートの追加を支援できるようにしてください。これにより、Unified Access Gateway が NTP サーバと通信できるようになります。VMware Horizon Cloud Service チームには、ルートを追加するための API 呼び出しがあります。</p> <p>ヒント: テナントがシングル ポッド仲介を使用するように構成されている場合、シングル ポッド ブローカのシナリオでは Unified Access Gateway アプライアンスの時刻ドリフトがエンドユーザーの接続に影響しないため、上記の要件を満たすことがベスト プラクティスと考えられます。</p>
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	4172	TCP UDP	PCoIP
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	<p>Blast Extreme</p> <p>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、および 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。</p>

表 6-18. ポッドの Unified Access Gateway インスタンスからのトラフィックに関するポートの要件 (続き)

ソース	ターゲット	ポート	プロトコル	目的
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	クライアント ドライブ リダイレクト (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	RADIUS インスタンス	1812	UDP	その Unified Access Gateway の構成に RADIUS 2 要素認証を使用する場合、RADIUS のデフォルト値はここに表示されます。
Unified Access Gateway	RSA SecurID Authentication Manager サーバ	5555	TCP	その Unified Access Gateway の構成に RSA SecurID 2 要素認証を使用する場合、ここでは、エージェント認証の RSA SecurID 認証 API エージェントの通信ポートに使用されるデフォルト値を示します。

Universal Broker で必要なポートおよびプロトコル

ポッドからのエンドユーザー割り当ての仲介に Universal Broker を使用できるようにするには、次の表の説明に従ってポート 443 を構成する必要があります。アクティブなポッド マネージャは、ポート 443 を介して Universal Broker サービスとの永続的な WebSocket 接続を確立し、ランダムに選択されたポートを介して Universal Broker サービスからの接続要求を受信します。

表 6-19. Universal Broker のポート要件

ソース	接続元ポート	ターゲット	ターゲットポート	プロトコル	目的
アクティブなポッド マネージャ	使用可能なポートからランダムに選択されます。	Universal Broker サービス	443	最初は HTTPS、次に WebSocket	Universal Broker サービスとの永続的な WebSocket 接続を確立します。

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

ポッドでプロビジョニングされた仮想デスクトップおよびリモート アプリケーションにデバイスから接続するには、エンド ユーザーは互換性のあるインストール済みの VMware Horizon Client またはそのブラウザ (Horizon HTML Access クライアントと呼ばれる) を使用します。エンド ユーザーのクライアントからのトラフィックが、ポッドでプロビジョニングされた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開く必要があるポートは、エンド ユーザーの接続方法の選択によって異なります。

ポッド専用の VNet で外部ゲートウェイ構成を使用するためのデプロイ オプションを選択する場合

デプロイヤーは、Microsoft Azure 環境に Unified Access Gateway インスタンスをデプロイします。このとき、そのロード バランサのバックエンド プールのインスタンスに Microsoft Azure ロード バランサ リソースもデプロイされます。このロード バランサは、DMZ サブネット上のこれらのインスタンスの NIC と通信し、Microsoft Azure でのパブリック ロード バランサとして構成されます。図 6-1. ポッドが外部および内部ゲートウェイの両方で構成された Horizon クラウド ポッド アーキテクチャの図 (外部ゲートウェイはポッドと同じ VNet にデプロイされた ; 外部ゲートウェイ仮想マシンに 3 つの NIC、内部ゲートウェイ仮想マシンに 2 つの NIC がある ; 外部ゲートウェイのロード バランサに対してパブリック IP アドレスが有効) は、このパブリック ロード バランサと Unified Access Gateway インスタンスの場所を示します。ポッドがこの構成を使用している場合、インターネット上のエンド ユーザーからのトラフィックは、Unified Access Gateway インスタンスに要求を配信するロード バランサに向かいます。この構成に対しては、これらのエンド ユーザー接続が、次のリストにあるポートおよびプロトコルを使用してロード バランサにアクセス可能であるようにする必要があります。デプロイ後に、外部ゲートウェイのロード バランサは `vmw-hcs-podID-uag` という名前のリソース グループにあります。ここで `podID` はポッドの UUID です。

内部 Unified Access Gateway 構成を使用するためのデプロイヤー オプションを選択する場合

内部ゲートウェイ構成は、デフォルトでポッド専用の VNet にデプロイされます。デプロイヤーは、Microsoft Azure 環境に Unified Access Gateway インスタンスをデプロイします。このとき、そのバックエンド プールのインスタンスに Microsoft Azure ロード バランサ リソースもデプロイされます。このロード バランサは、テナント サブネット上のこれらのインスタンスの NIC と通信し、Microsoft Azure での内部ロード バランサとして構成されます。図 6-1. ポッドが外部および内部ゲートウェイの両方で構成された Horizon クラウド ポッド アーキテクチャの図 (外部ゲートウェイはポッドと同じ VNet にデプロイされた ; 外部ゲートウェイ仮想マシンに 3 つの NIC、内部ゲートウェイ仮想マシンに 2 つの NIC がある ; 外部ゲートウェイのロード バランサに対してパブリック IP アドレスが有効) は、この内部ロード バランサと Unified Access Gateway インスタンスの場所を示します。ポッドがこの構成を使用している場合、企業ネットワーク内のエンド ユーザーからのトラフィックは、Unified Access Gateway インスタンスに要求を配信するロード バランサに向かいます。この構成に対しては、これらのエンド ユーザー接続が、次のリストにあるポートおよびプロトコルを使用してロード バランサにアクセス可能であるようにする必要があります。デプロイ後に、内部ゲートウェイのロード バランサは `vmw-hcs-podID-uag-internal` という名前のリソース グループにあります。ここで `podID` はポッドの UUID です。

ポッドではなく、専用の VNet で外部ゲートウェイ構成を使用する、または専用のサブスクリプションを使用するオプション (VNet は複数のサブスクリプションにまたがらないため、これは専用の VNet を使用する特別なサブケースです) のいずれかのデプロイヤー オプションを選択する場合

デプロイヤーは、Microsoft Azure 環境に Unified Access Gateway インスタンスをデプロイします。このとき、そのロード バランサのバックエンド プールのインスタンスに Microsoft Azure ロード バランサ リソースもデプロイされます。このロード バランサは、DMZ サブネット上のこれらのインスタンスの NIC と通信し、Microsoft Azure でのパブリック ロード バランサとして構成されます。図 6-2. 外部ゲートウェイがポッドの VNet とは別の専用の VNet にデプロイされている場合の外部ゲートウェイのアーキテクチャ要素の図は、このパブリック ロード バランサと、ゲートウェイ専用の VNet 内の Unified Access Gateway インスタンスの場所を示します。ポッドがこの構成を使用している場合、インターネット上のエンド ユーザーからのトラフィックは、Unified Access Gateway インスタンスに要求を配信するロード バランサに向かいます。この構成に対しては、これらのエンド ユーザー接続が、次のリストにあるポートおよびプロトコルを使用してロード バランサにアクセス可能であるようにする必要があります。デプロイ後、外部ゲートウェイのロード バランサは、`vmw-hcs-ID-uag` という名前のリソース グループにあります。ここで `ID` は、ポッドの詳細ページの [デプロ

イヤ ID] フィールドに表示される値です。『管理ガイド』の説明に従って、コンソールの [キャパシティ] ページからポッドの詳細ページにアクセスします。

ポッドに Unified Access Gateway 構成がない場合

注： シングルポッド仲介を使用するようにテナントが構成されている本番環境の場合、内部エンドユーザー接続のベスト プラクティスは、ポッドで内部 Unified Access Gateway ゲートウェイ構成を使用することです。これらの接続は、シングルポッド仲介シナリオのゲートウェイ構成経由になります。

シングルポッド仲介とポッドと統合した Workspace ONE Access の構成では、通常、Workspace ONE Access を介してエンド ユーザーが接続します。このシナリオでは、Workspace ONE Access と Workspace ONE Access Connector がポッドを直接参照するように構成する必要があります。エンド ユーザーは、Workspace ONE Access を使用して、ポッドでプロビジョニングされたリソースに接続していません。この構成の場合、『VMware Horizon Cloud Service 管理ガイド』の説明に従って、コンソールのポッドの [サマリ] ページを使用して、SSL 証明書をポッド マネージャ仮想マシンにアップロードします。次に、Workspace ONE Access をポッドと統合する手順を完了します。

表 6-20. ポッドの構成に外部 Unified Access Gateway インスタンスがある場合の外部エンド ユーザー接続のポートおよびプロトコル

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	ログイン認証トラフィック。クライアント ドライブ リダイレクト (CDR)、マルチメディア リダイレクト (MMR)、USB リダイレクト、および RDP トラフィックのトンネルも実行できます。 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	4172	TCP UDP	Unified Access Gateway 上の PCoIP Secure Gateway を介した PCoIP

表 6-20. ポッドの構成に外部 Unified Access Gateway インスタンスがある場合の外部エンド ユーザー接続のポートおよびプロトコル (続き)

ソース	ターゲット	ポート	プロトコル	目的
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。 デブ ロイ での 設定 内容 によ って 異な る	TCP	<p>Horizon Client からのデータ トラフィック用の Unified Access Gateway 上の Blast Secure Gateway を介した Blast Extreme。Horizon Cloud ポッドの場合、このポートはデプロイ ウィザードの [Blast Extreme TCP ポート] メニューを使用して選択されます。ネットワークで、外部ゲートウェイに指定したいいずれかへの送信アクセスがクライアントに許可されていることを確認します。この URL は、クライアントが、Unified Access Gateway インスタンスの前にあるロード バランサを介して、これらのインスタンスへの Horizon Blast セッションを確立するために使用されます。</p> <p>2021年10月のサービス リリース以降、ゲートウェイ構成の新規デプロイで、デプロイヤは対応する Unified Access Gateway 構成で構成する Blast Extreme TCP ポートに対して 8443 または 443 を選択できるようにします。以前は、デプロイヤはデフォルトで 443 を構成し、ポートを選択できませんでした。ゲートウェイ構成が 2021年10月のサービス リリースの日付より前にデプロイされた場合、その構成では通常、Unified Access Gateway 管理設定の [Blast 外部 URL] フィールドに 443 ポートが設定されています。</p> <p>注: ポート 8443 は、より効率的で、パフォーマンスが向上し、Unified Access Gateway インスタンスでのリソース使用率が低いため、推奨されます。ポート 443 は、より非効率的で、パフォーマンスが低下します。ポート 443 を使用すると、インスタンスで CPU の輻輳が発生します。ポート 443 は、組織でクライアント側の制限が設定されている場合 (組織で 8443 ではなく 443 送信のみが許可されているなど) にのみデプロイで使用されます。</p>
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 を介した 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 を介した Blast Extreme (アダプティブ トランスポート)。

表 6-20. ポッドの構成に外部 Unified Access Gateway インスタンスがある場合の外部エンド ユーザー接続のポートおよびプロトコル (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	443	TCP	<p>ログイン認証トラフィック。クライアント ドライブ リダイレクト (CDR)、マルチメディア リダイレクト (MMR)、USB リダイレクト、および RDP トラフィックのトンネルも実行できます。</p> <p>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。</p>
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。 デブ ロイ での 設定 内容 によ って 異な る	TCP	<p>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 を介した Blast Extreme。Horizon Cloud ポッドの場合、このポートはデプロイ ウィザードの [Blast Extreme TCP ポート] メニューを使用して選択されます。ネットワークで、外部ゲートウェイに指定したいいずれかへの送信アクセスがクライアントに許可されていることを確認します。この URL は、ブラウザの Horizon HTML Access クライアントが、Unified Access Gateway インスタンスの前にあるロード バランサを介して、これらのインスタンスへの Horizon Blast セッションを確立するために使用されます。</p> <p>2021年10月のサービス リリース以降、ゲートウェイ構成の新規デプロイで、デプロイは対応する Unified Access Gateway 構成で構成する Blast Extreme TCP ポートに対して 8443 または 443 を選択できるようにします。以前は、デプロイはデフォルトで 443 を構成し、ポートを選択できませんでした。ゲートウェイ構成が 2021年10月のサービス リリースの日付より前にデプロイされた場合、その構成では通常、Unified Access Gateway 管理設定の [Blast 外部 URL] フィールドに 443 ポートが設定されています。</p> <p>注: ポート 8443 は、より効率的で、パフォーマンスが向上し、Unified Access Gateway インスタンスでのリソース使用率が低いため、推奨されます。ポート 443 は、より非効率的で、パフォーマンスが低下します。ポート 443 を使用すると、インスタンスで CPU の輻輳が発生します。ポート 443 は、組織でクライアント側の制限が設定されている場合 (組織で 8443 ではなく 443 送信のみが許可されているなど) にのみデプロイで使用されます。</p>

表 6-21. ポッドの構成に内部 Unified Access Gateway インスタンスがある場合の内部エンド ユーザー接続のポートおよびプロトコル

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	<p>ログイン認証トラフィック。クライアント ドライブ リダイレクト (CDR)、マルチメディア リダイレクト (MMR)、USB リダイレクト、および RDP トラフィックのトンネルも実行できます。</p> <p>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。</p> <p>『VMware Horizon Cloud Service 管理ガイド』で「URL コンテンツ リダイレクトについて」のトピックを参照してください。</p>
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	4172	TCP UDP	Unified Access Gateway 上の PCoIP Secure Gateway を介した PCoIP

表 6-21. ポッドの構成に内部 Unified Access Gateway インスタンスがある場合の内部エンド ユーザー接続のポートおよびプロトコル (続き)

ソース	ターゲット	ポート	プロトコル	目的
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。 デブ ロイ での 設定 内容 によ って 異な る	TCP	<p>Horizon Client からのデータ トラフィック用の Unified Access Gateway 上の Blast Secure Gateway を介した Blast Extreme。Horizon Cloud ポッドの場合、このポートはデプロイ ウィザードの [Blast Extreme TCP ポート] メニューを使用して選択されます。ネットワークで、外部ゲートウェイに指定したいずれかへの送信アクセスがクライアントに許可されていることを確認します。この URL は、クライアントが、Unified Access Gateway インスタンスの前にあるロード バランサを介して、これらのインスタンスへの Horizon Blast セッションを確立するために使用されます。</p> <p>2021年10月のサービス リリース以降、ゲートウェイ構成の新規デプロイで、デプロイヤは対応する Unified Access Gateway 構成で構成する Blast Extreme TCP ポートに対して 8443 または 443 を選択できるようにします。以前は、デプロイヤはデフォルトで 443 を構成し、ポートを選択できませんでした。ゲートウェイ構成が 2021年10月のサービス リリースの日付より前にデプロイされた場合、その構成では通常、Unified Access Gateway 管理設定の [Blast 外部 URL] フィールドに 443 ポートが設定されています。</p> <p>注: ポート 8443 は、より効率的で、パフォーマンスが向上し、Unified Access Gateway インスタンスでのリソース使用率が低いため、推奨されます。ポート 443 は、より非効率的で、パフォーマンスが低下します。ポート 443 を使用すると、インスタンスで CPU の輻輳が発生します。ポート 443 は、組織でクライアント側の制限が設定されている場合 (組織で 8443 ではなく 443 送信のみが許可されているなど) にのみデプロイで使用されます。</p>
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 を介した 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 を介した Blast Extreme (アダプティブ トランスポート)。

表 6-21. ポッドの構成に内部 Unified Access Gateway インスタンスがある場合の内部エンド ユーザー接続のポートおよびプロトコル (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	443	TCP	<p>ログイン認証トラフィック。クライアント ドライブ リダイレクト (CDR)、マルチメディア リダイレクト (MMR)、USB リダイレクト、および RDP トラフィックのトンネルも実行できます。</p> <p>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。</p>
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。 デブ ロイ での 設定 内容 によ って 異な る	TCP	<p>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 を介した Blast Extreme。Horizon Cloud ポッドの場合、このポートはデプロイ ウィザードの [Blast Extreme TCP ポート] メニューを使用して選択されます。ネットワークで、外部ゲートウェイに指定したいいずれかへの送信アクセスがクライアントに許可されていることを確認します。この URL は、ブラウザの Horizon HTML Access クライアントが、Unified Access Gateway インスタンスの前にあるロード バランサを介して、これらのインスタンスへの Horizon Blast セッションを確立するために使用されます。</p> <p>2021年10月のサービス リリース以降、ゲートウェイ構成の新規デプロイで、デプロイは対応する Unified Access Gateway 構成で構成する Blast Extreme TCP ポートに対して 8443 または 443 を選択できるようにします。以前は、デプロイはデフォルトで 443 を構成し、ポートを選択できませんでした。ゲートウェイ構成が 2021年10月のサービス リリースの日付より前にデプロイされた場合、その構成では通常、Unified Access Gateway 管理設定の [Blast 外部 URL] フィールドに 443 ポートが設定されています。</p> <p>注: ポート 8443 は、より効率的で、パフォーマンスが向上し、Unified Access Gateway インスタンスでのリソース使用率が低いため、推奨されます。ポート 443 は、より非効率的で、パフォーマンスが低下します。ポート 443 を使用すると、インスタンスで CPU の輻輳が発生します。ポート 443 は、組織でクライアント側の制限が設定されている場合 (組織で 8443 ではなく 443 送信のみが許可されているなど) にのみデプロイで使用されます。</p>

表 6-22. VPN を介するなどの直接接続を使用する場合の内部エンド ユーザー接続のポートおよびプロトコル

ソース	ターゲット	ポート	プロトコル	目的
Horizon Client	ポッドの Microsoft Azure ロード バランサ	443	TCP	ログイン認証トラフィック。クライアントからのトラフィックは、ポッドのロード バランサを経由してポッド マネージャ仮想マシンに到達します。
Horizon Client	デスクトップまたはファーム RDSH 仮想マシン内の Horizon Agent	4172	TCP UDP	PCoIP
Horizon Client	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

表 6-22. VPN を介するなどの直接接続を使用する場合の内部エンド ユーザー接続のポートおよびプロトコル (続き)

ソース	ターゲット	ポート	プロトコル	目的
Horizon Client	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
Horizon Client	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	クライアント ドライブ リダイレクト (CDR) とマルチ メディア リダイレクト (MMR)
ブラウザ	デスクトップまたはファーム RDSH 仮想マシン内の Horizon Agent	443	TCP	HTML Access

ベース仮想マシン、VDI デスクトップ仮想マシン、およびファーム RDSH 仮想マシン内にインストールされたエージェントからのトラフィックのポートおよびプロトコルの要件

次のポートは、ベース仮想マシン、デスクトップ仮想マシン、およびファーム RDSH 仮想マシンにインストールされているエージェントに関連するソフトウェアと、ポッド マネージャ仮想マシンとの間のトラフィックを許可する必要があります。

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 Horizon Agent	ポッド マネージャ 仮想マシン	4001	TCP	<p>仮想マシンのエージェントが証明書のサムプリント検証の一部としてポッドと通信するために使用し、ポッドとの SSL 接続を保護するために交換される Java Message Service (JMS、非 SSL)。キーがネゴシエートされ、仮想マシンとポッド マネージャとの間で交換された後、エージェントはポート 4002 を使用してセキュアな SSL 接続を確立します。たとえば、[インポートされた仮想マシン] ページで [エージェント ペアリングをリセット] アクションを実行するには、ベースのインポートされた仮想マシンとポッド間でのエージェント ペアリング ワークフローのためにポート 4001 を使用した通信が必要です。</p> <p>注: 定常状態の動作には、ポート 4001 と 4002 の両方が必要です。エージェントがポッドのキーを再設定する必要がある場合があります。そのため、ポート 4001 を開いたままにしておく必要があります。</p>
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 Horizon Agent	ポッド マネージャ 仮想マシン	4002	TCP	これらの仮想マシンのエージェントがセキュアな SSL 接続を使用してポッドと通信するために使用する Java Message Service (JMS、SSL)。
デスクトップ仮想マシン、ファーム RDSH 仮想マシン内の Horizon Agent	VMware Cloud Services のホスト名 scapi.vmware.com	443	TCP	VMware Service Usage Data Program に使用されます。テナントサブネットから送信される場合、VMware Cloud Services のホスト名 scapi.vmware.com に送信される Horizon Agent からのトラフィック。
デスクトップまたはファーム RDSH 仮想マシンの FlexEngine エージェント (VMware Dynamic Environment Manager のエージェント)	デスクトップまたはファーム RDSH 仮想マシンで実行される FlexEngine エージェントによる使用のためにセットアップしたファイル共有	445	TCP	VMware Dynamic Environment Manager 機能を使用している場合、SMB ファイル共有への FlexEngine エージェント アクセス。

App Volumes 機能に必要なポートおよびプロトコル

Horizon Cloud on Microsoft Azure の App Volumes アプリケーション：概要と前提条件 で説明したように、Horizon Cloud ポッドでの使用がサポートされている App Volumes 機能の使用をサポートするには、ポッドのテナント サブネットでポート 445 を TCP プロトコル トラフィック用に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。

また、「第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名」で説明されているように、Azure Cloud がその SMB ファイル共有をプロビジョニングすると、Azure Cloud は *.file.core.windows.net のパターンで完全修飾ドメイン名 (FQDN) を割り当てます。ここで * は Azure が生成した SMB ファイル共有のストレージ アカウントの名前です。App Volumes がこれらのファイル共有にアクセスしてマウントし、AppStack を取得できるように、この FQDN は DNS サーバによって解決可能である必要があります。ポッド マネージャ インスタンス内で実行される App Volumes Manager プロセスと、VDI デスクトップで実行される App Volumes Agent について、DNS サーバが常にその FQDN を解決するようにする必要があります。

重要： Horizon Cloud ポッドと NSX Cloud バージョン 3.1.1 以降を統合し、App Volumes 割り当てを使用する場合は、NSX PCG をデプロイした後、そのポッドを使用して最初の App Volumes 割り当てを作成する前に、NSX ファイアウォール ルール内のポッドのテナント サブネットに対してこのポート 445/TCP を手動で開く必要があります。

表 6-23. 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	ポッド マネージャのリソース グループ内の SMB ファイル共有	445	TCP	ポッドのテナント サブネットに、SMB ファイル共有に保存されている App Volumes AppStack にアクセスします。

Workspace ONE Assist for Horizon との統合 - DNS、ポート、およびプロトコルの要件

Workspace ONE Assist for Horizon は、Workspace ONE UEM 製品ラインの製品です。2021 年 8 月の Horizon Cloud リリースの時点で、特定の要件が満たされると、その製品の使用を Horizon Cloud テナントのポッドからプロビジョニングされた VDI デスクトップと統合できます。要件の詳細については、[VMware Workspace ONE Assist ドキュメント領域](#)にある『VMware Workspace ONE Assist for Horizon ガイド』を参照してください。

アシスタント機能を使用するには、VDI デスクトップ仮想マシンと、Horizon Cloud テナントとの統合をサポートする Workspace ONE Assist サーバ間のアウトバンド通信が必要です。

DNS 要件

Workspace ONE Assist サーバの DNS 名が解決可能であり、VDI デスクトップ仮想マシンが配置されるポッドのテナント サブネットからアクセスできることを確認します。前述の『VMware Workspace ONE Assist for Horizon ガイド』には、Workspace ONE Assist サーバの DNS 名が記載されています。

ポートとプロトコルの要件

ポート 443、TCP、HTTPS を使用する送信トラフィックは、Workspace ONE Assist for Horizon アプリケーションがインストールされている VDI デスクトップ仮想マシンから許可される必要があります。

アクティブなサポート リクエストに必要な場合は、一時的なジャンプ ボックス ポートとプロトコル

VMware にサポート リクエストを発行し、サポート チームがそのリクエストを処理する方法として、VMware が管理するアプライアンスとの SSH 通信用の一時的なジャンプ ボックス仮想マシンをデプロイすることを決めた場合、そのジャンプ ボックスにはここで説明するポートとプロトコルが必要です。

サポート関連のジャンプ ボックス デプロイの権限がお客様から要求されます。VMware サポート チームは、サポート状況に応じて、通信要件をお知らせします。

このサポート関連のジャンプ ボックス仮想マシンは、次の宛先への送信元として通信するように設計されています。

- SSH およびポート 22 を使用するポッドのポッド マネージャ仮想マシンのポート 22。
- HTTPS を使用する Unified Access Gateway 仮想マシンのポート 9443。
- 外部ゲートウェイが専用の VNet にデプロイされている環境で、SSH を使用するゲートウェイ コネクタ仮想マシンのポート 22。

サポート リクエストの性質とデプロイで使用されるアプライアンスによって、通信のターゲットとして許可する必要がある VMware 管理対象アプライアンスが決まります。

表 6-24. サポート関連のジャンプ ボックスのポートおよびプロトコル

ソース	ターゲット	ポート	プロトコル	目的
ジャンプ ボックス仮想マシン	<ul style="list-style-type: none"> ■ ポッド マネージャ仮想マシン ■ ゲートウェイ コネクタ仮想マシン 	22	SSH	VMware のサポートでサポート リクエストに対応するためにリストされた 1 つ以上のアプライアンスとのこの通信を必要とする場合、ジャンプ ボックス仮想マシンは、管理サブネットを介してターゲット アプライアンスのポート 22 と通信します。
ジャンプ ボックス仮想マシン	Unified Access Gateway 仮想マシン	9443	HTTPS	VMware のサポートでサポート リクエストに対応するためにこの通信を必要とする場合、ジャンプ ボックス仮想マシンは管理サブネットを介して通信し、Unified Access Gateway 構成で設定します。

これらの仮想マシンには IP アドレスが動的に割り当てられているため、次のネットワーク ルールを使用して、説明されている通信を行うことができます。サポート リクエスト活動中は、サポート関連のジャンプ ボックス デプロイの要件について、VMware のサポートからのガイダンスと監督を受けるようにしてください。

- 接続元と接続先の両方としての管理サブネット CIDR (接続先ポート : 22、接続元ポート : 任意、プロトコル : TCP)。
- 接続元と接続先の両方としての管理サブネット CIDR (接続先ポート : 9443、接続元ポート : 任意、プロトコル : TCP、Unified Access Gateway 構成が関係する場合)。

True SSO、証明書管理、および Horizon Cloud on Microsoft Azure 環境

Horizon Cloud ポッドでプロビジョニングされたデスクトップ仮想マシンは、登録サーバと直接通信しません。Horizon Cloud on Microsoft Azure 環境のアクティブなポッド マネージャ仮想マシンは、証明書要求を登録サーバにリレーします。証明書が取得されると、デスクトップ仮想マシンの Horizon Agent はその証明書を使用して、デスクトップ ユーザーの代わりに証明書ログイン操作を実行します。

Horizon Cloud on Microsoft Azure 環境のポッド マネージャ仮想マシンの要求-応答アーキテクチャは、Horizon 環境の Horizon Connection Server の場合と同じです。Horizon Cloud on Microsoft Azure 環境では、ポッド マネージャ仮想マシンは、プライマリ仮想マシン サブネット (テナント サブネットとも呼ばれる)、および VDI 管理者が [ポッドの編集] ワークフローを使用して追加した可能性のある追加の仮想マシン サブネット上のデスクトップ仮想マシンに接続されています。

ユーザー証明書とチャンネル証明書の 2 つのクラスの証明書がさまざまなコンポーネントによって検証されます。True SSO が、認証サーバによって検証されたユーザー証明書を追加します。この Horizon Cloud on Microsoft Azure 環境の場合、その認証サーバは Microsoft Active Directory サーバです。Microsoft アーキテクチャではこの証明書の検証に使用できるポート番号が決定されるため、ポートは Microsoft アーキテクチャ自体の一部であり、Horizon Cloud on Microsoft Azure 環境自体に固有ではないため、この検証には幅広いポート番号を使用できます。

Horizon Cloud on Microsoft Azure 環境で True SSO を使用する場合、Horizon Agent は CSR を生成し、そのポッド マネージャ仮想マシンとその Horizon Agent の間にすでに配置されている通信チャンネルを介して、環境のアクティブなポッド マネージャ仮想マシンに CSR を送信します。ポッド マネージャ仮想マシンは、安全な SSL 暗号化 TCP チャンネル (ポート 32111 または登録サーバのインストールでユーザーが構成したポート) を介して登録サーバに要求をリレーします。登録サーバは CMC 要求を生成し、ポッド マネージャによって提供される CSR とユーザー名を追加し、登録エージェント証明書を使用して CMC に署名し、MS-DCOM (RPC) プロトコルを使用して認証局に送信します。

Horizon Agent は証明書を受け取り、ログイン認証情報としてシリアル化して、Windows ログイン プロセスに送信します。LSASS Windows コンポーネントは証明書を受け取り、証明書を検証し (有効で信頼されていること、およびローカル マシンが証明書のプライベート キーを保持していることを確認する)、ドメイン コントローラ (DC) に送信します。DC は、ユーザー証明書で指定されている CRL を確認することを選択できます。

視覚的に豊かなネットワークの図

これらのコンポーネント、ポート、およびプロトコル間の関係の視覚的に豊かな図については、<https://techzone.vmware.com/resource/vmware-horizon-cloud-service-microsoft-azure-network-ports-diagrams> にある VMware Digital Workspace Tech Zone のネットワーク図と説明を参照してください。

第1世代テナント - ポッドのサブスクリプションでの Horizon Cloud アプリケーション登録の作成

第1世代 Horizon Cloud Service on Microsoft Azure デプロイの場合、サービスは API 呼び出しを使用してポッドを Microsoft Azure サブスクリプションにデプロイし、そのポッドとポッドがプロビジョニングされた VDI デスクトップおよびファームを管理します。第1世代 Horizon Cloud がポッドのサブスクリプションで API 呼び出しを使用できるようにするには、アプリケーション登録を作成します。

重要: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

簡単な紹介

ポッドの初期デプロイの場合、ポッド デプロイヤは、ポッドに使用するよう選択した Microsoft Azure サブスクリプションの API を呼び出します。これらの API 呼び出しは、ポッドのサブスクリプションでアクションを実行して、ポッド マネージャ仮想マシン、仮想マシンの NIC、これらの NICS のネットワーク セキュリティ グループ (NSG) などのアイテムを作成します。これらのリソースは、Horizon Cloud ポッドが必要とするすべてのリソースです。

その後、ポッドのデプロイ後も、Horizon Cloud がポッドのサブスクリプションで API を引き続き呼び出すことができるようにする必要があります。ポッドのデプロイ後、サービスは API 呼び出しを使用して、ゴールド イメージの基本イメージ仮想マシンの作成、ゴールド イメージでの Sysprep の実行、ファーム ホストと VDI デスクトップ仮想マシンの作成、ポッドのゲートウェイ構成の追加と編集、およびポッドのメンテナンスとアップグレードを行います。

ポッド デプロイヤを実行する前にアプリケーション登録を作成する

ポッドのサブスクリプション内にポッドのリソースをプログラムで作成するために、ポッドのデプロイ プロセスでポッド デプロイヤが API を呼び出す必要があるため、デプロイ ウィザードを開始する前に、アプリケーション登録とクライアント プライベート キーが存在している必要があります。アプリケーションの登録を作成すると、ポッドのサブスクリプションにサービス プリンシパル オブジェクトが自動的に作成されます。

クライアント プライベート キーは、Azure ポータルで生成し、ロールをポッドのサブスクリプションのレベルで動作するように Horizon Cloud アプリケーションの登録に割り当てる必要があります。

外部 Unified Access Gateway 構成がポッドのサブスクリプションとは別に、独自のサブスクリプションでデプロイされる機能を使用する場合、Horizon Cloud は、ウィザードを実行して外部ゲートウェイをデプロイするとき、そのサブスクリプションで API を呼び出す機能も備えている必要があります。この場合、そのサブスクリプションには、ポッドのサブスクリプション用に加えて、アプリケーション登録とクライアント プライベート キーが必要です。

アプリケーション登録へのロールの割り当てについて

Horizon Cloud アプリケーションの登録は、ポッドのサブスクリプションにロールを割り当てる必要があります。通常、組み込みの Contributor ロールは、ポッドのサブスクリプションで Horizon Cloud によって使用されるロールです。Contributor ロールが使用される理由は、Horizon Cloud がポッドの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、アプリケーション登録がそのグループのメンバーとなる）は、現在、サポートされていません。

組織がポッドの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 ロールの使用もサポートします。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、このページの下部にある[カスタム ロールと Horizon Cloud アプリケーションの登録セクション](#)を参照してください。

リソース プロバイダの登録

ポッドのサブスクリプションでは、次のリソース プロバイダがすべて Registered ステータスである必要があります。このリストの一部のリソース プロバイダはすでに Registered ステータスになっていますが、他のプロバイダはそうではありません。これは、標準の Microsoft Azure の動作の結果であり、通常はすべての Azure サブスクリプションに対して登録されたリソース プロバイダのセットがあります。

ポッド デプロイ ウィザードを実行する前に、これらのリストされたリソース プロバイダのステータスが Registered であることを確認します。ウィザードの最後の手順で、これらのリソース プロバイダのステータスが Registered であることを検証し、ポッドのデプロイが登録解除されている場合はポッドのデプロイを開始できなくなります。

- Microsoft.Compute
- microsoft.insights
- Microsoft.Network
- Microsoft.Storage
- Microsoft.KeyVault
- Microsoft.Authorization
- Microsoft.Resources
- Microsoft.ResourceHealth
- Microsoft.ResourceGraph
- Microsoft.Security
- Microsoft.DBforPostgreSQL
- Microsoft.Sql
- Microsoft.MarketplaceOrdering

次のスクリーンショットは、Azure ポータルで [登録済み] ステータスと未登録ステータスを確認する例を示しています。

Provider	Status
Microsoft.AlertsManagement	✓ Registered
microsoft.insights	✗ NotRegistered
Microsoft.PolicyInsights	✓ Registered
Microsoft.Sql	✓ Registered
Microsoft.DBforPostgreSQL	✓ Registered
Microsoft.Network	✓ Registered
Microsoft.Compute	✓ Registered
Microsoft.KeyVault	✓ Registered

ポッドのサブスクリプションでリソース プロバイダを確認するには、次の手順を実行します。

- 1 Azure ポータルにログインし、ポッド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**（[リソース プロバイダ]）が表示されるまで下にスクロールします。
- 3 上記のリストでリソース プロバイダを探し、それぞれが **Registered**（[登録済み]）ステータスを示していることを確認します。

上記のリストから提供された NotRegistered と表示されるリソースについては、ポータルを使用して登録してください。

Horizon Cloud アプリケーション登録の作成

登録アカウントに応じた Microsoft Azure ポータルを使用して、次の手順を行います。たとえば、これらの Microsoft Azure クラウドのための特定のポータル エンドポイントがあります。

- Microsoft Azure Commercial（標準グローバル地域）
- Microsoft Azure China
- Microsoft Azure US Government

外部ゲートウェイがポッドとは別に独自のサブスクリプションを使用する Horizon Cloud 機能を使用する場合は、そのサブスクリプションの手順を繰り返して、アプリケーションを登録します。

Azure ポータルで次の手順をすべて完了するには、ポータル ログインにアプリケーション登録を作成し、ポッドをデプロイする予定のサブスクリプションでそのアプリケーション登録にロールを割り当てるための十分な権限が必要です。そのサブスクリプションの所有者または管理者でない場合は、アプリケーション登録を作成し、そのアプリケーション登録にロールを割り当てるために必要な権限があるかどうかを、所有者または管理者のいずれかに確認します。

- 1 アプリケーションを登録できる認証情報を使用して Microsoft Azure ポータルにログインします。
- 2 ポータルの検索バーで App registrations を検索し、結果リストに表示されたら [アプリケーション登録] をクリックします。



ポータルに [アプリケーション登録] ページが表示されます。

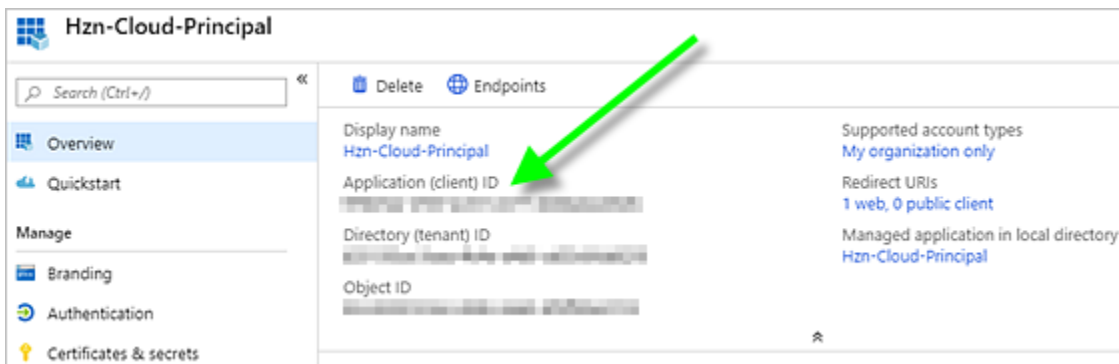
- 3 [アプリケーション登録] ページで、[新規登録] をクリックします。



- 4 この登録が Horizon Cloud で使用されることを思い出させる表示名を入力します。
- 5 [この組織ディレクトリにのみ含まれるアカウント] を選択します。
- 6 オプションの [リダイレクト URI] セクションをデフォルトの空の状態のままにします。
- 7 [登録] ボタンをクリックして、アプリケーション登録の作成を完了します。

新しく作成されたアプリ登録が画面に表示されます。

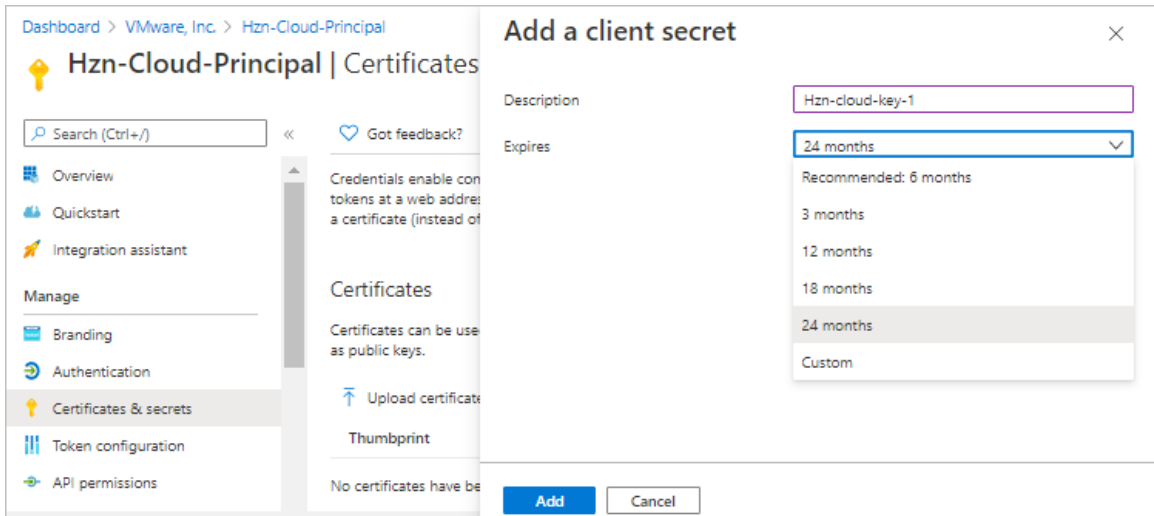
- 8 アプリケーション ID とディレクトリ ID をコピーし、デプロイ ウィザードの実行中に参照できる場所に保存します。次のスクリーンショットは、Hzn-Cloud-Principal という名前のアプリケーション登録と、アプリケーション ID とディレクトリ ID が表示される場所を指す緑色の矢印を示しています。



- 9 次に、アプリケーション登録のクライアント プライベート キーを作成します。

- a 上記のスクリーンショットで、**Certificates & secrets** が表示される場所を参照してください。Azure ポータルの新しく作成した [アプリケーション登録] ページで、[証明書とシークレット] をクリックします。

- b [新しいクライアントのシークレット] をクリックします。
- c 次のスクリーンショットに示すように、ポータルには [クライアント シークレットの追加] 画面が表示されます。説明を入力して有効期限を選択し、[追加] をクリックします。キーの説明は 16 文字以下にしてください。たとえば、Hzn-Cloud-Key1 と入力します。

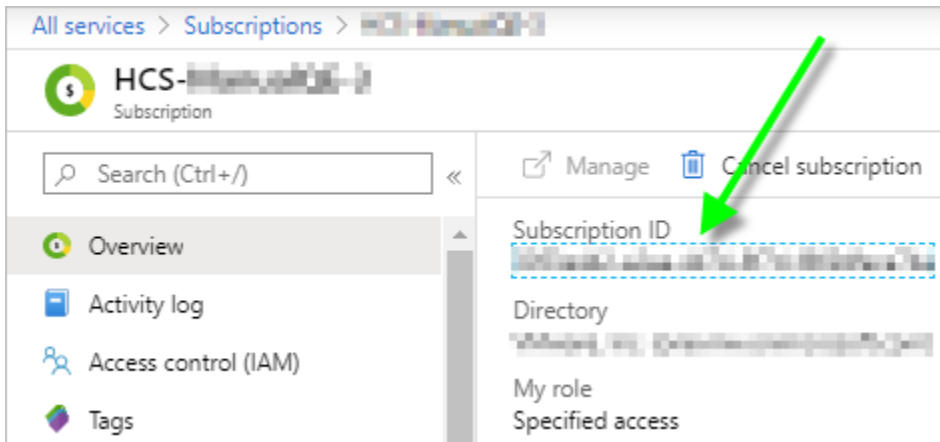



重要： シークレット値をコピーし、後で参照可能な場所に貼り付けるまでは、この画面を開いたままにします。

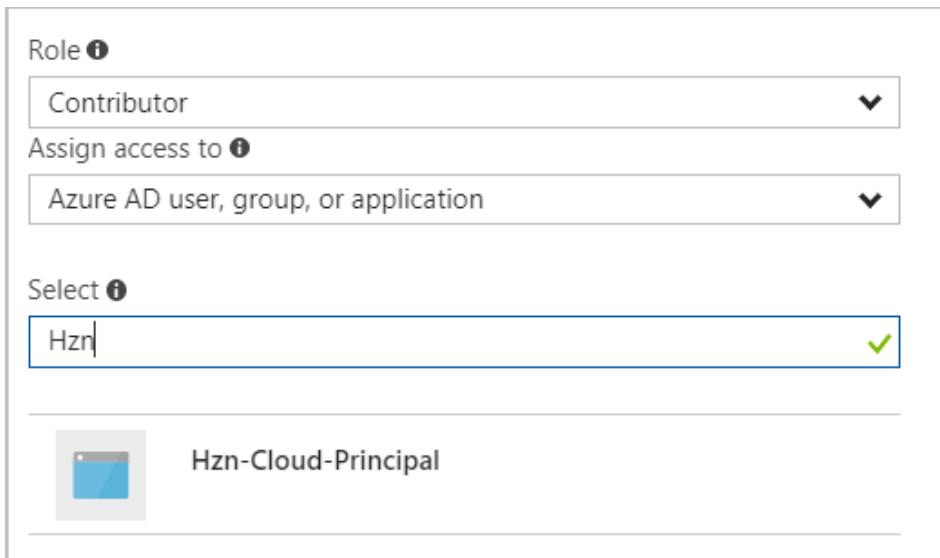
DESCRIPTION	EXPIRES	VALUE
Hzn-cloud-key1	7/1/2022	[REDACTED]

- d デプロイ ウィザードの実行中に参照できる場所にシークレット値をコピーします。ウィザードには、この値を貼り付けるフィールドがあります。
- 10 Horizon Cloud アプリケーション登録にロール割り当てを追加します。サブスクリプション レベルでロールを割り当てます。
- a Microsoft Azure ポータルのメイン ナビゲーション バーで [すべてのサービス] をクリックし、[サブスクリプション] をクリックしてから、ポッド デプロイヤーでポッドをデプロイする予定のサブスクリプションの名前をクリックして、サブスクリプションの設定画面に移動します。

注： ここで、画面に表示されたサブスクリプション ID をメモできます。この ID は、デプロイ ウィザードで必要になります。



- b  アクセス制御 (IAM) ([アクセス制御 (IAM)]) をクリックして、[追加] - [ロール割り当てを追加] の順にクリックし、[ロール割り当てを追加] 画面を開きます。
- c [ロールの割り当ての追加] 画面の [ロール] で Contributor ロールを選択します。
組織が Horizon Cloud にカスタム ロールを使用することを望んでいる場合は、この目的のために組織がセットアップしたカスタム ロールを選択します。
- d [アクセス権の割り当て先] ドロップダウン リストで、[Azure Active Directory ユーザー、グループ、またはアプリケーション] を選択します。
- e [選択] ボックスを使用して、Horizon Cloud アプリケーション登録の名前を検索します。次のスクリーンショットは、この手順を示しています。



- f 作成した Horizon Cloud アプリケーション登録に付ける名前をクリックして、選択したメンバーにし、[保存] をクリックします。

選択 

Hzn 

選択したメンバー:

	Hzn-Cloud-Principal	Remove
---	---------------------	--------

保存 破棄

サマリ

この時点で、Horizon Cloud アプリケーション登録を作成および構成し、Horizon Cloud に必要なリソース プロバイダの登録ステータスを確認し、ポッドのデプロイ ウィザードの最初の手順で入力する必要のあるサブスクリプション関連の値を取得しました。4 つのサブスクリプション関連の値は次のとおりです。

- サブスクリプション ID
- Azure Active Directory ID
- アプリケーション ID
- アプリケーション キーの値

注： Horizon Cloud は、アプリケーション登録のクライアント プライベート キーに設定した有効期限を検出または認識できません。Horizon Cloud がこのアプリケーション登録を引き続き使用してポッドとそのリソースを管理するために必要な API 呼び出しを行えるようにするには、キーの有効期限が切れる前にキーを更新してから、新しいキーを Horizon Cloud 環境に入力する必要があります。現在、Microsoft Azure ポータルを使用して設定できる最長の有効期限は 2 年です。2 年の終わりにキーの有効期限が切れ、ポッドで使用するためにキーを更新したり、Horizon Cloud 環境に新しいキー情報を入力したりしていない場合、期限切れのキーに関連付けられているポッドは動作を停止します。Microsoft Azure ポータルのユーザー インターフェイスで許可される 2 年以上の有効期間を持つプライベート キーを作成する場合、Microsoft Azure は現在、PowerShell、Azure CLI、または Graph API を使用してその機能を提供しています。

カスタム ロールと Horizon Cloud アプリケーションの登録

組織がポッドのサブスクリプションで Contributor ロールを使用しないようにする場合は、代わりにカスタム ロールを作成し、そのロールを Horizon Cloud アプリケーション登録に割り当てることができます。Horizon Cloud で必要な API 呼び出しを許可するように、カスタム ロールを構成する必要があります。組織がポッドのサブスクリプションで Contributor ロールを使用しないようにする場合は、[第 1 世代テナント - 組織が第 1 世代 Horizon Cloud のアプリケーション登録にカスタム ロールを使用することを希望する場合の情報を参照してください](#)。

第 1 世代テナント - 組織が第 1 世代 Horizon Cloud のアプリケーション登録にカスタム ロールを使用することを希望する場合

第 1 世代 Horizon Cloud のアプリケーション登録でポッドのサブスクリプション（またはオプションの外部ゲートウェイのサブスクリプション）で API 呼び出しを行い、その VDI 関連の操作を実行できるようにするには、アプリケーション登録にロールを割り当てる必要があります。通常、この目的には Contributor ロールが使用されます。Contributor ロールの使用を回避することを希望する組織の場合は、カスタム ロールを作成し、カスタム ロールに Horizon Cloud アプリケーション登録に必要な API 呼び出しを実行する機能を付与するという目的を果たすことができます。

重要： この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、[該当記事を参照してください](#)。

ポッドのサブスクリプションでの Horizon Cloud アプリケーション登録のカスタム ロールに加えて、組織がポッドの外部 Unified Access Gateway 構成用に個別のサブスクリプションを使用するアプローチを採用し、その目的のために組織が設定した特定のリソース グループにゲートウェイ リソースをデプロイすることを選択する場合は、そのゲートウェイのサブスクリプションのカスタム ロールは、ポッドのサブスクリプションのカスタム ロールよりもきめ細かく、狭い範囲の権限を持つことができます。

カスタム ロールの概要

包括的な概念として、Horizon Cloud は、ポッドおよびそのゲートウェイ構成を持つために必要なリソースを正常に作成および維持するために、ポッドのサブスクリプションおよびそのリソース グループで特定の操作を実行する必要があります。

単純な例として、ポッドとゲートウェイ アーキテクチャでは NIC を備えた仮想マシンが必要であるため、Horizon Cloud にはサブスクリプション内で仮想マシンと NIC を作成し、それらの NIC をサブスクリプションの VNet のサブネットに接続する機能が必要となります。

Microsoft Azure では、ロールは、アプリケーション登録のサービス プリンシパルによって実行できる一連の管理操作を提供します。管理操作は、リソースとそのリソースに対して実行されるアクションの組み合わせです。

次のルールに従って、ポッドのサブスクリプションおよび（オプションの）ゲートウェイのサブスクリプションの Horizon Cloud アプリケーション登録の機能を、必要な最小限の操作に制限できます。

使用可能な使用事例の概要

サブスクリプションとリソース グループにおいて Horizon Cloud で必要とされる操作については、ここに記載された使用事例で説明できます。

注： 2 サブスクリプションの使用事例では、ポッドのサブスクリプションでのアプリケーション登録のロールは、単一サブスクリプションの使用事例に必要なルールに従う必要があります。

使用事例	説明
<p>ポッドとその外部 Unified Access Gateway 構成の Horizon Cloud によって使用される単一サブスクリプション。</p>	<p>この場合、ポッドのサブスクリプション レベルでサービス プリンシパルにアクセス権を付与する必要があります。そのレベルでサービス プリンシパルに割り当てられたロールは、サブスクリプション内で Horizon Cloud が実行する必要があるアクションによって、そのサブスクリプション内で必要なリソースが正常に作成され、時間の経過とともにそれらのリソースを操作できるようにする必要があります。たとえば、この場合、このロールはデフォルトのリソース グループ、ネットワーク セキュリティ グループ、仮想マシンなどを作成可能である必要があります。</p>
<p>2 つのサブスクリプションを使用していて、外部ゲートウェイの指定されたサブスクリプションで、ゲートウェイに必要なリソース グループとリソースを、ポッドのサブスクリプションの場合と同様に Horizon Cloud が自動作成することを望んでいる場合。</p> <ul style="list-style-type: none"> ■ 外部 Unified Access Gateway 構成のリソースに対して使用するよう指定されたサブスクリプションが 1 つ ■ 残りのポッド リソース用のサブスクリプションが 1 つ 	<p>このオプションを使用する場合、各サブスクリプションのサービス プリンシパルに、サブスクリプション レベルでのアクセス権を、上記で説明した単一サブスクリプションの使用事例と同じアクションを許可する権限とともに付与する必要があります。</p>

使用事例	説明
<p>上記と同様に 2 つのサブスクリプションを使用しているが、外部ゲートウェイの必要なリソース グループおよびリソースを Horizon Cloud が自動作成するのではなく、その外部ゲートウェイの指定されたサブスクリプションで事前にリソース グループを作成し、Horizon Cloud が外部ゲートウェイのリソースを既存のリソース グループにデプロイすることを望んでいる場合。</p>	<p>外部ゲートウェイのデプロイに使用されるサービス プリンシパルへのアクセス権を付与するためのオプションは次の 2 つです。</p> <ul style="list-style-type: none"> ■ 上記の場合と同じように、サブスクリプション レベルでのアクセス権を付与します。 ■ 次の組み合わせを使用します。 <ul style="list-style-type: none"> ■ サブスクリプション レベルで、組み込みのリーダー ロールを使用してアクセス権を付与します。 ■ 名前付きリソース グループ レベルで、カスタム ロールで定義されている権限を使用してアクセス権を付与します。リソース グループ レベルで付与される権限は、外部ゲートウェイのリソースをデプロイおよび構成するために Horizon Cloud がリソース グループで実行する必要がある操作のために用意する必要があるものです。 <p>Horizon Cloud は、リソース グループの権限に加えて、デプロイ プランに応じて次のアクションを実行するための権限を必要とします。</p> <ul style="list-style-type: none"> ■ このデプロイにおいて、サブスクリプションの VNet で事前に作成したサブネットが使用される場合、Horizon Cloud はそれらのサブネットに NIC およびネットワークセキュリティ グループ (NSG) を作成する機能を必要とします。サブネットが属する VNet で必要な権限は <code>Microsoft.Network/virtualNetworks/subnets/*</code> と <code>Microsoft.Network/networkSecurityGroups/*</code> です ■ このデプロイによって Horizon Cloud がサブネットを生成する場合、Horizon Cloud は上記の <code>Microsoft.Network/virtualNetworks/subnets/*</code> および <code>Microsoft.Network/networkSecurityGroups/*</code> の権限に加えて、サブネットを作成する機能を必要とします。VNet で必要な権限は <code>Microsoft.Network/virtualNetworks/write</code> です ■ 外部ゲートウェイのデプロイでパブリック IP アドレスを使用するように指定されている場合、Horizon Cloud は名前付きリソース グループにパブリック IP アドレスを作成する機能を必要とします。名前付きリソース グループに必要な権限は <code>Microsoft.Network/publicIPAddresses</code> です
<p>VNet にカスタム ルートがある場合。Microsoft Azure Cloud には、カスタム ルートと呼ばれる機能があります。</p>	<p>VNet にカスタム ルートがある場合は、上記の使用事例のすべてに加えて次の権限が必要です：<code>Microsoft.Network/routeTables/join/action</code>。</p>

ポッドとそのゲートウェイ構成に対して単一のサブスクリプションを使用する場合、またはサブスクリプション レベルで設定された権限がある外部 Unified Access Gateway 構成に対して別個のサブスクリプションを使用する場合

これらの使用事例では、サブスクリプション レベルでの権限が割り当てられます。カスタム ロールは、次の表の操作を許可する必要があります。* (ワイルドカード文字) は、リストされている操作内の文字列と一致するすべての操作へのアクセスを許可します。

表 6-25. 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 Azure ドキュメントの説明
Microsoft.Authorization/*/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftauthorization
Microsoft.Compute/*/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/availabilitySets/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/disks/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/images/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute

表 6-25. 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 Azure ドキュメントの説明
Microsoft.Compute/locations/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/snapshots/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/virtualMachines/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/virtualMachineScaleSets/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.DBforPostgreSQL/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftdbforpostgresql

表 6-25. 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 Azure ドキュメントの説明
Microsoft.KeyVault/*/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkeyvault
Microsoft.KeyVault/vaults/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkeyvault
Microsoft.KeyVault/vaults/secrets/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkeyvault
Microsoft.Network/loadBalancers/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.Network/networkInterfaces/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork

表 6-25. 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 Azure ドキュメントの説明
Microsoft.Network/networkSecurityGroups/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.Network/publicIPAddresses/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.Network/virtualNetworks/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.Network/virtualNetworks/write	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork

表 6-25. 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 Azure ドキュメントの説明
Microsoft.Network/virtualNetworks/subnets/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.ResourceHealth/availabilityStatuses/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftresourcehealth
Microsoft.Resources/subscriptions/resourceGroups/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftresources
Microsoft.Resources/deployments/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftresources

表 6-25. 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 Azure ドキュメントの説明
Microsoft.Storage/*/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftstorage
Microsoft.Storage/storageAccounts/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftstorage
Microsoft.Compute/galleries/read Microsoft.Compute/galleries/write Microsoft.Compute/galleries/delete Microsoft.Compute/galleries/images/* Microsoft.Compute/galleries/images/versions/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftmarketplaceordering

次の JSON コード ブロックは、Horizon Cloud Pod という名前のカスタム ロール定義に、一連の事前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、この ID が自動的に生成されます。*mysubscriptionId1* 変数の場合は、カスタム ロールが使用されるサブスクリプション (ポッドのサブスクリプションまたはオプションのゲートウェイ サブスクリプション) の ID を置き換えます。

表 6-26. 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

```

{
  "Name": "Horizon Cloud Pod",
  "Id": "uuid",
  "IsCustom": true,
  "Description": "Minimum set of Horizon Cloud pod required operations",
  "Actions": [
    "Microsoft.Authorization/*/read",
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/availabilitySets/*",
    "Microsoft.Compute/disks/*",
    "Microsoft.Compute/images/*",
    "Microsoft.Compute/locations/*",
    "Microsoft.Compute/virtualMachines/*",
    "Microsoft.Compute/virtualMachineScaleSets/*",
    "Microsoft.Compute/snapshots/*",
    "Microsoft.DBforPostgreSQL/*",
    "Microsoft.KeyVault/*/read",
    "Microsoft.KeyVault/vaults/*",
    "Microsoft.KeyVault/vaults/secrets/*",
    "Microsoft.Network/loadBalancers/*",
    "Microsoft.Network/networkInterfaces/*",
    "Microsoft.Network/networkSecurityGroups/*",
    "Microsoft.Network/publicIPAddresses/*",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/write",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/subnets/*",
    "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read",
    "Microsoft.Resources/subscriptions/resourceGroups/*",
    "Microsoft.ResourceHealth/availabilityStatuses/read",
    "Microsoft.Resources/deployments/*",
    "Microsoft.Storage/*/read",
    "Microsoft.Storage/storageAccounts/*",
    "Microsoft.Compute/galleries/read",
    "Microsoft.Compute/galleries/write",
    "Microsoft.Compute/galleries/delete",
    "Microsoft.Compute/galleries/images/*",
    "Microsoft.Compute/galleries/images/versions/*",
    "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",
    "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/mysubscriptionId"
  ]
}

```

カスタム ルートが VNet とそのサブネットにある場合

Microsoft Azure Cloud には、カスタム ルートと呼ばれる機能があります。

このようなルートが VNet とそのサブネットに追加されている場合は、この追加の権限が必要です。

表 6-27. VNet にカスタム ルートがある場合に許可する必要がある Microsoft Azure リソース操作

操作	Microsoft Azure ドキュメントの説明
Microsoft.Network/routeTables/join/action	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork

外部 Unified Access Gateway 構成に対して別個のサブスクリプションを使用し、カスタム リソース グループにデプロイし、サブスクリプション レベルでのリーダー ロールと、きめ細かいレベルでの追加の必要な権限が割り当てられている場合

この使用事例では、外部ゲートウェイのサブスクリプションのサブスクリプション レベルで、組織は組み込みの Reader ロールを使用して Horizon Cloud アプリケーション登録を使用できます。また、名前付きリソース グループのレベルでカスタム ロールを使用することもできます。

組織は、次の表の権限を指定するカスタム ロールを作成します。そのカスタム ロールは、Horizon Cloud アプリケーション登録に割り当てられ、外部ゲートウェイのサブスクリプション内の特別に指定されたリソース グループと連携します。ユーザーまたはユーザーの組織は、外部ゲートウェイをデプロイするサブスクリプションでその名前付きリソース グループを事前に作成します。

計画したデプロイ オプションによっては、サブネットおよび VNet での特定の権限も必要になります。

- この外部ゲートウェイのデプロイにおいて、事前に作成したサブネットが使用される場合、Horizon Cloud はそれらのサブネットに NIC およびネットワーク セキュリティ グループ (NSG) を作成する機能を必要とします。サブネットが属する VNet で必要な権限は Microsoft.Network/virtualNetworks/subnets/* と Microsoft.Network/networkSecurityGroups/* です。
- この外部ゲートウェイのデプロイによって Horizon Cloud がサブネットを生成する場合、Horizon Cloud は上記の Microsoft.Network/virtualNetworks/subnets/* および Microsoft.Network/networkSecurityGroups/* の権限に加えて、サブネットを作成する機能を必要とします。サブスクリプションの VNet で必要な権限は Microsoft.Network/virtualNetworks/write です
- デプロイで、外部ゲートウェイの構成にパブリック IP アドレスを使用するように指定されている場合、Horizon Cloud は名前付きリソース グループにパブリック IP アドレスを作成する機能を必要とします。名前付きリソース グループに必要な権限は Microsoft.Network/publicIPAddresses です

名前付きリソース グループでは、次の許可された操作が必要となります。* (ワイルドカード文字) は、リストされているリソース プロバイダ操作内の文字列と一致するすべての操作へのアクセスを許可します。

表 6-28. 指定されたリソース グループで許可される必要がある Microsoft Azure リソースの操作

操作	Microsoft Azure ドキュメントの説明
Microsoft.Authorization/*/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftauthorization
Microsoft.Compute/*/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/availabilitySets/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/disks/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/images/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute

表 6-28. 指定されたリソース グループで許可される必要がある Microsoft Azure リソースの操作 (続き)

操作	Microsoft Azure ドキュメントの説明
Microsoft.Compute/locations/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/snapshots/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/virtualMachines/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.Compute/virtualMachineScaleSets/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute
Microsoft.DBforPostgreSQL/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftdbforpostgresql

表 6-28. 指定されたリソース グループで許可される必要がある Microsoft Azure リソースの操作 (続き)

操作	Microsoft Azure ドキュメントの説明
Microsoft.KeyVault/*/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkeyvault
Microsoft.KeyVault/vaults/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkeyvault
Microsoft.KeyVault/vaults/secrets/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkeyvault
Microsoft.Network/loadBalancers/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.Network/networkInterfaces/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork

表 6-28. 指定されたリソース グループで許可される必要がある Microsoft Azure リソースの操作 (続き)

操作	Microsoft Azure ドキュメントの説明
Microsoft.Network/publicIPAddresses/*、デプロイで、外部ゲートウェイのデプロイにパブリック IP アドレスを使用するよう指定されている場合。	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.Network/virtualNetworks/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
Microsoft.ResourceHealth/availabilityStatuses/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftresourcehealth

表 6-28. 指定されたリソース グループで許可される必要がある Microsoft Azure リソースの操作 (続き)

操作	Microsoft Azure ドキュメントの説明
Microsoft.Resources/subscriptions/resourceGroups/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftresources
Microsoft.Resources/deployments/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftresources
Microsoft.Storage/*/read	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftstorage
Microsoft.Storage/storageAccounts/*	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftstorage
Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftmarketplaceordering

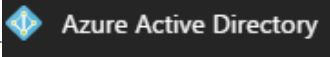

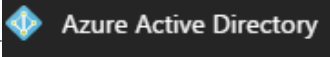

第1世代テナント - Horizon Cloud ポッドのデプロイ ウィザードのためのサブスクリプション関連情報

第1世代 Horizon Cloud ポッドのデプロイ ウィザードでは、Microsoft Azure サブスクリプションから以下の情報を指定する必要があります。外部ゲートウェイをポッドとは別の専用のサブスクリプションにデプロイする場合、デプロイはどちらのサブスクリプションに対してもこの情報を必要とします。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

重要： Microsoft Azure ポータルで生成されたアプリケーション キーは、即座に取得する必要があります。詳細については、[第1世代テナント - ポッドのサブスクリプションでの Horizon Cloud アプリケーション登録の作成](#)を参照してください。その他の情報については、Microsoft Azure アカウントの認証情報を使用して Microsoft Azure ポータルにログインするといつでも入手できます。

ID は UUID で、8-4-4-4-12 の形式です。次の表で説明するこれらの ID とキーは、ポッドのデプロイ ウィザードの最初の手順で使用されます。

要求値	収集方法	値
[環境]	Microsoft Azure サブスクリプションに登録するときに、Microsoft Azure クラウド環境を決定します。その時点で、アカウントとサブスクリプションは特定の Microsoft Azure 環境内で作成されます。	
[サブスクリプション ID]	Microsoft Azure ポータルで、Microsoft Azure ポータルのメイン ナビゲーション バーで [すべてのサービス] をクリックし、[サブスクリプション] をクリックし、ポッドで使用するサブスクリプションの名前をクリックして、サブスクリプションの設定画面に移動します。表示されたサブスクリプション ID を見つけます。	
[ディレクトリ ID]	Microsoft Azure ポータルで、  -  プロパティ] ([管理] の下) をクリックします。	
[アプリケーション ID]	Microsoft Azure ポータルで、  -  アプリの登録] をクリックし、第1世代テナント - ポッドのサブスクリプションでの Horizon Cloud アプリケーション登録の作成 の手順を使用して Horizon Cloud に対して作成した [アプリケーション登録] をクリックします。	
[アプリケーション キー]	Microsoft Azure ポータルでキーを生成して取得します。 第1世代テナント - ポッドのサブスクリプションでの Horizon Cloud アプリケーション登録の作成 を参照してください。	

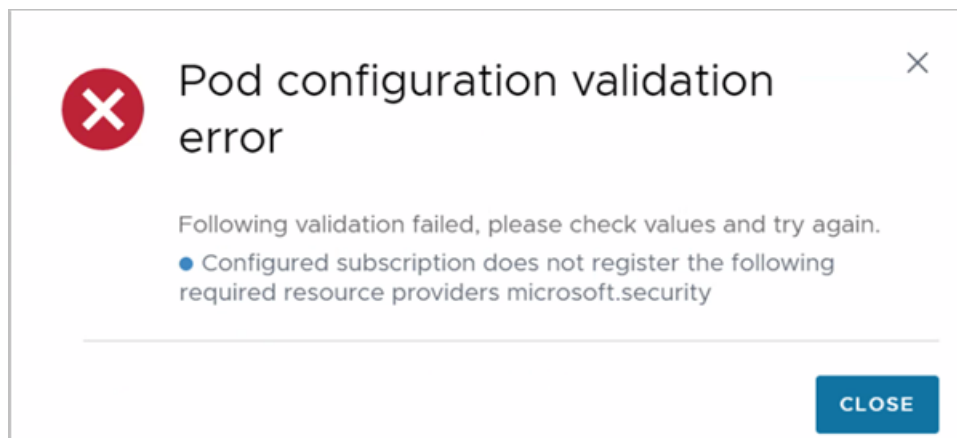
第1世代テナント - 第1世代 Horizon Cloud で Microsoft Azure サブスクリプションにおける状態が登録済みになっている必要があるリソース プロバイダ

Microsoft Azure サブスクリプションで第1世代 Horizon Cloud ポッドを作成および管理するため、第1世代 Horizon Cloud はそのサブスクリプションでさまざまなリソースを作成および管理する機能を必要とします。したがって、サブスクリプションでは特定のリソース プロバイダが [登録済み] 状態になっている必要があります。これにより、Horizon Cloud は最初にポッドをデプロイし、その有効期間にわたってポッドを管理およびアップグレードするのに必要な操作を実行できます。このドキュメントの記事には、第1世代 Horizon Cloud で [登録済み] 状態になっている必要があるリソース プロバイダがリストされています。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、[該当記事を参照してください](#)。

Microsoft Azure のドキュメントによると、[リソース プロバイダ](#)とは、Microsoft Azure リソースを提供するサービスのことで、たとえば Microsoft.KeyVault リソース プロバイダはキー コンテナ タイプのリソースを提供します。Microsoft Azure のドキュメントトピック [Azure リソース プロバイダとタイプ](#)に記載されているとおり、特定のリソースをサブスクリプションで使用する前に、そのタイプのリソースを提供するリソース プロバイダをそのサブスクリプションに登録する必要があります。この Microsoft Azure のドキュメントには、一部のリソース プロバイダはデフォルトで登録され、その他のリソース プロバイダはサブスクリプションでの明示的な手動登録を必要とすることも記載されています。

最も重要なのは、ポッドをデプロイする前に、ここにリストされているすべてのリソース プロバイダが、サブスクリプションで [登録済み] 状態になっていることを確認することです。新しいポッドをデプロイする場合、ポッド デプロイヤーは、さまざまな Microsoft Azure リソース プロバイダにコマンドを発行し、デプロイヤーが作成する必要があるタイプのリソースの作成を要求することにより、サブスクリプションにリソースを作成します。明示的な手動登録を必要とするリソース プロバイダの状態が、ポッドのデプロイが [検証と続行] の手順に進む前に [登録済み] にならない場合、ウィザードはポッドのデプロイがその時点から先に進行するのをブロックします。[第1世代テナント - 検証と続行、およびポッドのデプロイ プロセスの開始](#)で、ポッド デプロイヤーは、必要なリソース プロバイダのセットの状態がサブスクリプションで [登録済み] になっているかどうかを検証します。ポッド デプロイヤーが必要とするリソース プロバイダの状態が [登録済み] でない場合、ウィザードはエラー メッセージを表示します。次のスクリーンショットは、サブスクリプションで Microsoft.Security リソース プロバイダの状態が [登録済み] でない場合の例です。



Horizon Cloud で必要なリソース プロバイダ

- Microsoft.Compute
- microsoft.insights
- Microsoft.Network
- Microsoft.Storage
- Microsoft.KeyVault
- Microsoft.Authorization
- Microsoft.Resources
- Microsoft.ResourceHealth
- Microsoft.ResourceGraph
- Microsoft.Security
- Microsoft.DBforPostgreSQL
- Microsoft.Sql
- Microsoft.MarketplaceOrdering

第1世代テナント - 第1世代 Horizon Cloud ポッドのデプロイに必要な PEM 形式への証明書ファイルの変換

第1世代ポッドの Unified Access Gateway 機能には、クライアント接続のための SSL が必要です。ポッドに対して Unified Access Gateway 構成を作成する場合、ポッド デプロイ ウィザードには、SSL サーバ証明書チェーンをそのポッドの Unified Access Gateway 構成に提供するための PEM フォーマット ファイルが必要になります。1つの PEM ファイルに、SSL サーバ証明書、必要な中間 CA 証明書、ルート CA 証明書、プライベート キーを含む、完全な証明書チェーンが含まれている必要があります。

重要: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

Unified Access Gateway で使用される証明書タイプについて詳しくは、[Unified Access Gateway 製品ドキュメント](#)の「正しい証明書タイプの選択」トピックを参照してください。

ゲートウェイ設定に関するポッド デプロイ ウィザードの手順で、証明書ファイルをアップロードします。デプロイ中、このファイルはデプロイされた Unified Access Gateway インスタンスの構成に送信されます。ウィザードインターフェイスでアップロード手順を実行すると、ウィザードはアップロードしたファイルが次の要件を満たしているかを検証します。

- ファイルを PEM 形式として解析できる。
- 有効な証明書チェーンとプライベート キーが含まれている。
- そのプライベート キーはサーバ証明書のパブリック キーと一致する。

証明書情報に対する PEM 形式のファイルがない場合は、証明書情報を上記の要件を満たすファイルに変換する必要があります。PEM 形式でないファイルを PEM 形式のファイルに変換し、完全な証明書チェーンとプライベート キーを含む単一の PEM ファイルを作成する必要があります。不要な情報が表示される場合は、ファイルの解析中にウィザードで問題が発生しないように、ファイルを編集してその情報を削除する必要があります。手順の概要は次のとおりです。

- 1 証明書情報を PEM 形式に変換し、証明書チェーンとプライベート キーを含む単一の PEM ファイルを作成します。
- 2 ファイルを編集し、-----BEGIN CERTIFICATE----- と -----END CERTIFICATE----- のマーカー間の証明書情報の外部に余分な証明書情報があれば削除します。

次の手順のコード例では、ルート CA 証明書、中間 CA 証明書情報、およびプライベート キーを含む `mycaservercert.pfx` という名前のファイルを使用することを想定します。

前提条件

- 証明書ファイルがあることを確認します。このファイルは PKCS#12 (`.p12` または `.pfx`) 形式や、Java JKS または JCEKS 形式になることができます。

重要： 証明書チェーン内のすべての証明書が有効期限内である必要があります。Unified Access Gateway 仮想マシンでは、任意の中間証明書を含む、チェーン内のすべての証明書が有効期限内である必要があります。チェーン内のいずれかの証明書が期限切れの場合、後で Unified Access Gateway 構成に証明書がアップロードされる際に予期しない障害が発生する可能性があります。

- 証明書を変換するために使用できる `openssl` コマンドライン ツールについて理解しておきます。ドキュメントについては、OpenSSL ソフトウェアを入手したベンダーのサイトを確認するか、[openssl.org](https://www.openssl.org) のマニュアル ページを見つけます。
- 証明書が Java JKS または JCEKS 形式の場合、`.pem` ファイルに変換する前に、最初に証明書を `.p12` または `.pks` 形式に変換するための Java `keytool` コマンドライン ツールについて理解しておきます。

手順

- 1 証明書が Java JKS または JCEKS 形式の場合、`keytool` を使用して証明書を `.p12` または `.pks` 形式に変換します。

重要： この変換中、変換元と変換先で同じパスワードを使用します。

- 2 証明書が PKCS#12 (`.p12` または `.pfx`) 形式の場合、または証明書を PKCS#12 形式に変換した後は、`openssl` を使用して証明書を `.pem` ファイルに変換します。

たとえば、証明書の名前が `mycaservercert.pfx` の場合、次のコマンドを使用して証明書を変換できます。

```
openssl pkcs12 -in mycaservercert.pfx -nokeys -out mycaservercertchain.pem
openssl pkcs12 -in mycaservercert.pfx -nodes -nocerts -out mycaservercertkey.pem
```

上記の最初の行は `mycaservercert.pfx` の証明書を取得し、`mycaservercertchain.pem` に PEM 形式で書き込みます。上記の 2 番目の行は `mycaservercert.pfx` からプライベート キーを取得し、`mycaservercertkey.pem` に PEM 形式で書き込みます。

- 3 (オプション) プライベート キーが RSA 形式でない場合は、プライベート キーを RSA プライベート キー形式に変換します。

Unified Access Gateway インスタンスには、RSA プライベート キー形式が必要です。この手順を実行する必要があるかどうかを確認するには、PEM ファイルのプライベート キー情報が次の行で始まるかどうかを確認します。

```
-----BEGIN PRIVATE KEY-----
```

プライベート キーがこの行で始まる場合は、プライベート キーを RSA 形式に変換する必要があります。プライベート キーが `-----BEGIN RSA PRIVATE KEY-----` で始まる場合は、この手順を実行してプライベート キーを変換する必要はありません。

プライベート キーを RSA 形式に変換するには、次のコマンドを実行します。

```
openssl rsa -in mycaservercertkey.pem -check -out mycaservercertkeyrsa.pem
```

これで PEM ファイルのプライベート キーは RSA 形式 (`-----BEGIN RSA PRIVATE KEY-----` と `-----END RSA PRIVATE KEY-----`) になります。

- 4 証明書チェーン PEM ファイルとプライベート キー PEM ファイルの情報を組み合わせて、1つの PEM ファイルを作成します。

次の例では、`mycaservercertkeyrsa.pem` の内容 (RSA 形式のプライベート キー) が最初にあり、その後にプライマリ SSL 証明書である `mycaservercertchain.pem` の内容が続きます。さらに1つの中間証明書、ルート証明書が続きます。

```
-----BEGIN CERTIFICATE-----
... (your primary SSL certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate CA certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the trusted root certificate)
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
... (your server key from mycaservercertkeyrsa.pem)
-----END RSA PRIVATE KEY-----
```

注： サーバ証明書が最初で、次に中間証明書、その次に信頼されるルート証明書の順番にする必要があります。

- 5 `BEGIN` と `END` マーカーの間に不要な証明書エントリまたは無関係な情報がある場合は、ファイルを編集して削除します。

結果

これで PEM ファイルは、ポッド デプロイ ウィザードの要件を満たすようになります。

第1世代テナント - Microsoft Azure へのポッドの自動デプロイを実行するための第1世代 Horizon Universal Console の使用

ポッド デプロイ ウィザードを実行して、Microsoft Azure のポッド マネージャ ベースのポッドとそのゲートウェイ構成の要素となるコンポーネントをデプロイします。ポッドのコネクタ コンポーネントを第1世代 Horizon Cloud とペアリングし、Microsoft Azure のキャパシティを Horizon Cloud で使用できるようにします。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

重要： このウィザードは、ポッド マネージャ ベースのタイプのポッドを Microsoft Azure にデプロイします。このウィザードでは、Horizon Connection Server のテクノロジーを使用する Azure VMware Solution (AVS) 上の Horizon ポッドはデプロイされません。AVS に Horizon ポッドを手動でデプロイする方法については、Tech Zone の [Horizon on Azure VMware Solution Architecture](#) および [Deploying Horizon with Azure VMware Solution](#) を参照してください。そのタイプのポッドの場合は、該当するポッドを手動でデプロイした後、Horizon Cloud Connector および手動でデプロイされた既存の Horizon ポッドをオンボーディングする場合のワークフローの概要の手順を使用して Horizon Cloud に接続できます。

デプロイヤーは、ウィザードの各手順で入力された情報を使用してポッドを構成する方法を決定します。特定の手順で必要となる情報を提供した後、[次へ] をクリックして次の手順に進みます。

注意： 以下の手順で示す IP アドレスはサンプルです。組織の要件を満たすアドレス範囲を使用してください。IP アドレス範囲の記述がある手順では、組織に適切な IP アドレスに置き換えてください。

前提条件

ポッド デプロイ ウィザードを開始する前に必要な項目を用意しておくことを確認します。ウィザードで指定する必要がある項目は、ポッドの構成オプションによって異なります。前提条件については、[第1世代テナント - 第1世代のポッド デプロイ ウィザードを実行するための前提条件](#)を参照してください。

ポッドの構成オプションには次が含まれます。

- 事前に作成する既存のサブネットを選択するか、ポッド デプロイヤーで自動的にサブネットを作成するか

- 外部または内部の Unified Access Gateway 構成を使用してデプロイする、両方を使用してデプロイする、またはどちらも使用せずにデプロイし、後で追加する。ゲートウェイ構成の1つのタイプだけでデプロイする場合は、後でポッドを編集してもう一方の未構成のタイプを追加できます。

Unified Access Gateway を次のように構成してデプロイする場合	後でポッドを編集して以下を追加することが可能
外部	内部
内部	外部
なし	いずれかのタイプまたは両方のタイプ

- ポッドの VNet とは別の、専用の VNet で外部 Unified Access Gateway 構成を使用してデプロイする。このシナリオには、次のようなバリエーションがあります。
 - ポッドのサブスクリプションとは別の、専用のサブスクリプションで外部 Unified Access Gateway 構成を使用してデプロイする。VNet は複数のサブスクリプションにまたがらないため、このオプションは個別の VNet ケースの特別なシナリオです。外部ゲートウェイが専用のサブスクリプションを使用してデプロイされる場合、それは外部ゲートウェイが専用の VNet にもあることを意味します。
 - 外部 Unified Access Gateway 構成を使用して独自のサブスクリプションにデプロイする場合は、その個別のサブスクリプションの名前付きリソース グループにデプロイすることもできます。この場合、[ポッドの追加] ウィザードを実行する前に、サブスクリプションでそのリソース グループを事前に作成する必要があります。
- ポッドのゲートウェイ構成に設定されている 2 要素認証のオプションを使用してデプロイする。ポッドのゲートウェイ構成に設定されている 2 要素認証設定を使用せずにデプロイする場合は、後でポッドを編集してもう一方の未構成のタイプを追加できます。
- 外部 Unified Access Gateway 構成の場合は、構成のロード バランサでパブリック IP アドレスを使用しないようにすることをオプションで選択できます。ロード バランサにパブリック IP アドレスを持たないようにウィザード オプションを選択する場合は、DNS サーバで FQDN にマッピングした IP アドレス値をウィザードで指定する必要があります。この FQDN は、このゲートウェイへの PCoIP 接続のためにエンド ユーザーの Horizon Client で使用されるものです。デプロイ プロセスでは、デプロイヤーは Unified Access Gateway の Horizon 設定でその IP アドレスを構成します。Unified Access Gateway のドキュメントでは、この IP

アドレス値は PCoIP 外部 URL と呼ばれます。Unified Access Gateway のドキュメントで URL と呼ばれている場合でも、入力した値は IP アドレスである必要があります。この IP アドレスを DNS の FQDN にマッピングします。これは、ポッドの外部 Unified Access Gateway 構成で PCoIP セッションを確立するためにエンド ユーザーの Horizon Client で使用される FQDN です。

注意： デプロイされたポッドを後で編集して、外部ゲートウェイのロード バランサに対するこの IP アドレス設定を変更することはできません。そのため、デプロイ ウィザードで DNS マッピングの FQDN と一致するパブリック IP アドレスを入力し、その FQDN がデプロイ ウィザードでアップロードする証明書の FQDN と一致することを確認してください。

手順

1 第1世代テナント - 第1世代のポッド デプロイ ウィザードを実行するための前提条件

第1世代のポッド デプロイ ウィザードを実行する前に、環境がこ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。ポッド デプロイ ウィザードで要求された値を指定し、ウィザードの指示に従って進めるために、次の項目を用意しておく必要があります。

2 第1世代テナント - ポッド マネージャ ベースのポッドをデプロイするためのポッド デプロイ ウィザードの起動

このウィザードを使用して、ポッド マネージャ ベースのポッドを Microsoft Azure サブスクリプションに自動的にデプロイします。このウィザードを使用して最初のポッドをデプロイする際は、Horizon Universal Console の [はじめに] ページの [Microsoft Azure] 行で、[管理] - [ポッドの追加] 機能を使用してポッド デプロイ ウィザードを開始します。

3 第1世代テナント - 新しい Horizon Cloud ポッドの Microsoft Azure サブスクリプション情報の指定

ポッド デプロイ ウィザードのこの手順で、このポッドで使用する Microsoft Azure サブスクリプション情報を指定します。

4 第1世代テナント - デプロイ ウィザードを使用して Microsoft Azure にデプロイする Horizon Cloud ポッドのポッド構成情報の指定

ポッド デプロイ ウィザードのポッド セットアップの手順で、ネットワーク情報に加えて、ポッドの名前などの詳細を指定します。

5 第1世代テナント - Horizon Cloud ポッドのゲートウェイ構成の指定

ウィザードのこの手順では、1つ以上のゲートウェイが構成されているポッド マネージャ ベースのポッドをデプロイするために必要な情報を指定します。Unified Access Gateway は、このタイプのポッドのゲートウェイ環境を提供します。

6 第1世代テナント - 検証と続行、およびポッドのデプロイ プロセスの開始

[検証と続行] をクリックした後、指定した値がシステムによって検証されます。すべてが検証されると、ウィザードに確認のための情報の概要が表示されます。次にデプロイ プロセスを開始します。

第1世代テナント - 第1世代のポッド デプロイ ウィザードを実行するための前提条件

第1世代のポッド デプロイ ウィザードを実行する前に、環境がこ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。ポッド デプロイ ウィザードで要求された値を指定し、ウィザードの指示に従って進めるために、次の項目を用意しておく必要があります。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

重要： ポッド デプロイ ウィザードを起動してポッドのデプロイを開始する前に、以下の要件に加えて、次の重要な点に注意する必要があります。

- ポッドを正常にデプロイするには、ユーザーまたは IT チームが Microsoft Azure 環境で設定したどの Microsoft Azure ポリシーも、ポッドのコンポーネントの作成をブロック、拒否、または制限しないようにすることが必要です。また、Microsoft Azure ポリシーの組み込みポリシー定義がポッドのコンポーネントの作成をブロック、拒否、または制限しないことを確認する必要があります。許可する必要がある項目の2つの例として、ユーザーと IT チームは、Microsoft Azure ポリシーが Azure ストレージ アカウントでのコンポーネントの作成をブロック、拒否、または制限することがないことを確認し、Microsoft Azure ポリシーで `Microsoft.MarketplaceOrdering/*` の `resourceType` が許可されていることを確認する必要があります。ポッドのデプロイ プロセスは、VMware の `vmware-inc publisherID` からの Azure Marketplace オファアの受け入れに依存します。Azure ポリシーの詳細については、[Azure ポリシーのドキュメント](#)を参照してください。サービスが `Microsoft.MarketplaceOrdering/*` リソース タイプを使用する方法については、[IT またはセキュリティ組織に Azure Marketplace オファアまたはマーケットプレイスの注文の使用に関する制限がある場合](#)を参照してください。
- ポッド デプロイヤでは、Azure ストレージ アカウントでそのデプロイヤがサブスクリプション内のポッドのリソース グループに Azure StorageV2 アカウント タイプを作成できるようにする必要があります。このストレージ アカウントは、ポッドの App Volumes 機能に使用されます。ポッドのデプロイ中は、Microsoft Azure ポリシーが、Azure StorageV2 アカウント タイプを必要とするコンテンツの作成を制限したり、拒否したりしないようにします。
- すべてのクラウド接続されたポッドは、それらのポッドをデプロイするときに、Active Directory ドメインの同じセットに接続されている必要があります。

すべてのデプロイの前提条件

- [第1世代テナント - 第1世代 Horizon Cloud ポッドを Microsoft Azure にデプロイする前の準備](#)に記載されている準備作業がすべて完了していることを確認します。
- サブスクリプション情報が[第1世代テナント - Horizon Cloud ポッドのデプロイ ウィザードのためのサブスクリプション関連情報](#)に記載のとおりであることを確認します。

- [第 1 世代 Horizon Cloud - Microsoft Azure](#) での必要な仮想ネットワークの構成で説明したように、Microsoft Azure サブスクリプションで、ポッドを追加するリージョンに仮想ネットワークがあることを確認します。

重要: 一部の Microsoft Azure リージョンでは、GPU が有効な仮想マシンはサポートされません。GPU 対応のデスクトップまたはリモート アプリケーションでポッドを使用する場合は、使用する NV シリーズ、NVv4 シリーズ、NCv2 シリーズの仮想マシン タイプが、ポッド用に選択した Microsoft Azure のリージョンで提供されていることと、この Horizon Cloud リリースでサポートされていることを確認します。詳細については、<https://azure.microsoft.com/ja-jp/regions/services/> にある Microsoft のドキュメントを参照してください。

- VNet が、外部アドレスを解決できる DNS を参照するように構成されていることを確認します。ポッド デプロイヤーは、ポッド ソフトウェアを Microsoft Azure 環境に安全にダウンロードするために Horizon Cloud 制御プレーンの外部アドレスに到達する必要があります。
- [第 1 世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件](#)、[DNS 名および第 1 世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件](#)の説明どおりに、ポッド デプロイヤーの DNS、ポート、およびプロトコルの要件が満たされていることを確認します。
- アウトバウンド インターネット アクセスでプロキシを使用する必要がある場合は、プロキシ設定のためのネットワーク情報および必要な認証情報（使用する場合）があることを確認します。ポッドのデプロイ プロセスには、アウトバウンド インターネット アクセスが必要です。

重要: ポッドが Microsoft Azure にデプロイされた後にポッドのプロキシ設定を編集または更新することは、現在サポートされていません。また、プロキシ設定なしでデプロイされたデプロイ済みポッドにプロキシ構成を追加することは、現在サポートされていません。

- ポッド マネージャ インスタンスおよび Unified Access Gateway インスタンスで時刻の同期に使用する少なくとも 1 台の NTP サーバの情報があることを確認します。NTP サーバは、パブリック NTP サーバ、またはこの目的で設定する独自の NTP サーバです。指定する NTP サーバは、ポッド マネージャ インスタンスおよび Unified Access Gateway インスタンスをデプロイする予定の仮想ネットワークからアクセスできる必要があります。IP アドレスではなくドメイン名を使用して NTP サーバを使用する場合は、仮想ネットワークに対して構成された DNS が NTP サーバの名前を解決できることも確認してください。

注: ポッド マネージャ インスタンス、Unified Access Gateway インスタンス、および Active Directory サーバに同じ NTP サーバを使用することがベスト プラクティスです。タイム スキューは、これらのインスタンスが異なる NTP サーバを使用する場合に発生する可能性があります。このようなタイム スキューにより、後でゲートウェイがデスクトップおよびアプリケーションに対してエンド ユーザー セッションを認証しようとしたときに、エラーが発生する可能性があります。

- デプロイヤーが必要なサブネットを自動的に作成するようにはしたくない場合は、必要なサブネットが事前に作成されていて VNet 上に存在していることを確認します。必要なサブネットを事前に作成する手順については、[第1世代テナント - ポッドのデプロイの前に、Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成する](#)および[第1世代テナント - Microsoft Azure で Horizon Cloud ポッド用に既存のサブネットを使用する場合](#)を参照してください。

注意： ポッドのデプロイのために VNet 上に事前に手動で作成したサブネットは空のままである必要があります。これらのサブネットの IP アドレスを使用しているアイテムを持つ既存のサブネットを再利用しないでください。IP アドレスがサブネットですでに使用されている場合、ポッドがデプロイに失敗したり、その他のダウンストリーム IP アドレスの競合の問題などの問題が発生する可能性が高くなります。これらのサブネットに何らかのリソースを投入したり、IP アドレスを使用したりしないでください。この警告通知には Horizon Cloud からデプロイされたポッドが含まれています。すでにデプロイされているポッドがあるサブネットを再利用しないでください。

- デプロイヤーが必要なサブネットを作成する場合、ウィザードの管理サブネット、デスクトップ サブネット、および DMZ サブネットに入力するアドレス範囲を把握していることを確認します。外部 Unified Access Gateway 構成を使用する場合は、DMZ サブネットが必要です。また、これらの範囲が重複しないことを確認します。アドレス範囲は、CIDR 表記（クラスレス ドメイン間ルーティング表記）で入力します。入力したサブネット範囲が重複していると、ウィザードがエラーを表示します。管理サブネット範囲の場合、少なくとも /27 の CIDR が必要です。DMZ サブネット範囲の場合、少なくとも /28 の CIDR が必要です。管理および DMZ サブネットの範囲を同じ場所に共存させたいのであれば、IP アドレスを指定して DMZ サブネット範囲を管理サブネットと同様のものに指定することができます。たとえば、管理サブネットが 192.168.8.0/27 の場合、一致する DMZ サブネットは 192.168.8.32/27 になります。

重要： ウィザード フィールドに入力する CIDR は、プリフィックスとビットマスクの各組み合わせが、プリフィックスを開始 IP アドレスとする IP アドレス範囲になるように定義する必要があります。Microsoft Azure では、CIDR プリフィックスを範囲の先頭にする必要があります。たとえば、192.168.182.48/28 という正しい CIDR の場合、IP アドレス範囲は 192.168.182.48 ~ 192.168.182.63 になり、プリフィックスは開始 IP アドレス (192.168.182.48) と同じになります。ただし、192.168.182.60/28 という間違った CIDR の場合、IP アドレス範囲は 192.168.182.48 ~ 192.168.182.63 になり、開始 IP アドレスは 192.168.182.60 のプリフィックスと同じになりません。CIDR は、開始 IP アドレスが CIDR プリフィックスと一致する IP アドレス範囲になるように定義してください。

- デプロイヤーによって必要なサブネットを作成する場合、このアドレス範囲を持つサブネットが VNet 上に存在しないことを確認してください。この場合、デプロイヤー自身がウィザードで指定するアドレス範囲を使用してサブネットを自動的に作成します。ウィザードが既にこれらの範囲が存在するサブネットを検出した場合は、ウィザードにアドレスの重複に関するエラーが表示され、それ以降に進まなくなります。VNet がピアリングされている場合、ウィザードに入力するつもり CIDR アドレス空間がすでに VNet のアドレス空間に含まれていることを確認します。

Unified Access Gateway 構成の前提条件

ポッドで Unified Access Gateway の構成を使用することを計画している場合、次の情報を入力する必要があります。

- サービスへのアクセスでエンド ユーザーが使用する完全修飾ドメイン名 (FQDN)。外部ゲートウェイと内部ゲートウェイの両方の構成に同じ FQDN を使用することを計画している場合は、ポッドをデプロイした後、適切

なゲートウェイ ロード バランサにルーティングするようにエンドユーザー クライアントの受信トラフィックを設定する必要があります。目標は、インターネットからのクライアント トラフィックが外部ゲートウェイの Microsoft Azure パブリック ロード バランサにルーティングされ、イントラネットからのクライアント トラフィックが内部ゲートウェイの Microsoft Azure 内部ロード バランサにルーティングされるようにルーティングを設定することです。このシナリオでは、両方のゲートウェイで同じ FQDN を使用するため、スプリット DNS (スプリット Domain Name System) を構成して、エンド ユーザー クライアントの DNS クエリのオリジン ネットワークに応じて、外部ゲートウェイまたは内部ゲートウェイのいずれかにゲートウェイ アドレスを解決します。次に、エンド ユーザー クライアントで使用されているのと同じ FQDN で、クライアントがインターネット上にある場合は外部ゲートウェイにルーティングし、クライアントが内部ネットワーク上にある場合は内部ゲートウェイにルーティングできます。

重要： この FQDN には、アンダー スコアを含めることはできません。このリリースでは、FQDN にアンダー スコアが含まれていると、Unified Access Gateway インスタンスへの接続が失敗します。

- その FQDN に基づいた署名付きの SSL サーバ証明書 (PEM 形式)。Unified Access Gateway 機能には、Unified Access Gateway 製品マニュアルに記載されているようにクライアント接続のための SSL が必要です。証明書には、信頼された証明書認証局 (CA) の署名が必要です。単一の PEM ファイルに完全な証明書チェーンおよびプライベート キーが含まれている必要があります。たとえば、単一の PEM ファイルに SSL サーバ証明書、必要な中間 CA 証明書、ルート CA 証明書、およびプライベート キーが含まれている必要があります。OpenSSL は、PEM ファイルの作成に使用できるツールです。

重要： 証明書チェーン内のすべての証明書が有効期限内である必要があります。Unified Access Gateway 仮想マシンでは、任意の中間証明書を含む、チェーン内のすべての証明書が有効期限内である必要があります。チェーン内のいずれかの証明書が期限切れの場合、後で Unified Access Gateway 構成に証明書がアップロードされる際に予期しない障害が発生する可能性があります。

- 外部の Unified Access Gateway 構成でデプロイする場合、DMZ (非武装地帯) サブネットを指定する必要があります。2 つの方法で、この DMZ サブネットを指定することができます。
 - DMZ サブネットを VNet で事前に作成する。この方法を使うと、管理サブネットおよびデスクトップ テナント サブネットも事前に作成する必要があります。[第1世代テナント - ポッドのデプロイの前に、Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成するの手順を参照してください。](#)
 - デプロイの際に、デプロイヤに DMZ サブネットを自動的に作成させる。この方法では、ウィザードに入力する DMZ サブネット用のアドレス範囲を決定し、その範囲が管理サブネットおよびデスクトップ テナント サブネットの範囲と重複しないことを確認する必要があります。アドレス範囲は、CIDR 表記 (クラスレスドメイン間ルーティング表記) で入力します。入力したサブネット範囲が重複していると、ウィザードがエラーを表示します。DMZ サブネット範囲の場合、少なくとも /28 の CIDR が必要です。管理および DMZ サブネットの範囲を同じ場所に共存させるには、IP アドレスを指定して DMZ サブネット範囲を管理サブネットと同一のものに指定することができます。たとえば、管理サブネットが 192.168.8.0/27 の場合、一致する DMZ サブネットは 192.168.8.32/27 になります。IP アドレスの範囲に、プリフィックスを開始 IP アドレスとするプリフィックスとビット マスクの組み合わせが必要なことに関する、[すべてのデプロイの前提条件](#)の重要な注意事項も参照してください。

- 外部 Unified Access Gateway 構成でデプロイし、構成のロード バランサにパブリック IP アドレスを使用しないようにする場合、DNS 設定でエンド ユーザーが Horizon Client の PCoIP 接続に使用する FQDN にマッピングした IP アドレスを指定する必要があります。

Unified Access Gateway で必要な PEM ファイルに関する考慮事項の詳細については、[第1世代テナント - 第1世代 Horizon Cloud ポッドのデプロイに必要な PEM 形式への証明書ファイルの変換](#)を参照してください。

ポッドの VNet またはサブスクリプションとは別の専用の VNet またはサブスクリプションを使用して外部 Unified Access Gateway 構成でデプロイする場合の前提条件

注： 専用の VNet を使用して外部ゲートウェイをデプロイすると、ゲートウェイ コネクタ仮想マシンがデプロイされます。[Horizon Cloud ポッドのポートとプロトコルの要件](#)では、ゲートウェイ コネクタ仮想マシンのポートとプロトコルについて説明するセクションに、このゲートウェイ コネクタ仮想マシンの説明も含まれており、ゲートウェイ コネクタ仮想マシンの名前に vmw-hcs-ID のような部分を含む名前が付くことが示されています。この場合、ID はゲートウェイのデプロイ ID、および node 部分になります。

Unified Access Gateway 構成でデプロイする場合の上記の前提条件に加えて、これらの前提条件は、外部ゲートウェイを専用の VNet または専用のサブスクリプションにデプロイする使用事例に固有です。専用のサブスクリプションの使用は専用の VNet の使用の特殊な事例です。それは、VNet の適用範囲はサブスクリプションであるため、個別のサブスクリプションには専用の VNet が必要になるためです。

- ゲートウェイの VNet は、ポッドの VNet とピアリングする必要があります。
- 必要なサブネットが事前に作成されて VNet に存在すること、またはウィザードに入力する予定の CIDR アドレス空間が VNet のアドレス空間にすでに含まれていることを確認します。VNet はピアリングされているため、VNet のアドレス空間にまだ含まれていない CIDR アドレス空間をウィザードに入力すると、デプロイは VNet を自動的に拡張できません。その場合、デプロイ プロセスは失敗します。

ヒント： ベスト プラクティスは、事前にサブネットを作成することです。必要なサブネットを事前に作成する手順については、[第1世代テナント - ポッドのデプロイの前に、Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成する](#)および[第1世代テナント - Microsoft Azure で Horizon Cloud ポッド用に既存のサブネットを使用する場合](#)を参照してください。

- 外部ゲートウェイに個別のサブスクリプションを使用している場合は、[第1世代テナント - Horizon Cloud ポッドのデプロイ ウィザードのためのサブスクリプション関連情報](#)で説明するようにサブスクリプション情報があることを確認します。
- 外部ゲートウェイに別個のサブスクリプションを使用しており、デプロイヤにリソース グループを自動作成させるのではなく、作成した名前付きリソース グループにゲートウェイをデプロイしようとしている場合は、そのサブスクリプションにおいてそのリソース グループが作成済みであることを確認します。そのリソース グループは、ウィザードにおいて名前を選択します。また、[第1世代テナント - 組織が第1世代 Horizon Cloud のアプリケーション登録にカスタム ロールを使用することを希望する場合](#)で説明するように、そのリソースグループに対して、デプロイヤが動作するために必要なアクセス権が付与されていることを確認します。

2 要素認証構成でデプロイする際の前提条件

2 要素認証機能を使用する予定や、それをオンプレミスの 2 要素認証サーバで使用する予定がある場合は、認証サーバの構成からの次の情報があることを確認し、[ポッドの追加] ウィザードの必須フィールドにその情報を指定できるようにします。

使用しているタイプに応じて、次の情報を取得します。

RADIUS

プライマリおよび補助 RADIUS サーバの両方の設定を構成している場合は、それぞれの情報を取得します。

- 認証サーバの IP アドレスまたは DNS 名
- 認証サーバのプロトコル メッセージで暗号化および復号化のために使用される共有シークレット
- 認証ポート番号。通常 RADIUS の場合は 1812/UDP。
- 認証プロトコルのタイプ。認証タイプには、PAP (パスワード認証プロトコル)、CHAP (チャレンジ ハンドシェイク認証プロトコル)、MSCHAP1 および MSCHAP2 (Microsoft チャレンジ ハンドシェイク認証プロトコル、バージョン 1 および 2) があります。

注： RADIUS ベンダーの推奨する認証プロトコルについては、RADIUS ベンダーのドキュメントを確認し、指定したプロトコル タイプに従ってください。RADIUS の 2 要素認証をサポートするポッドの機能は、Unified Access Gateway インスタンスによって提供され、Unified Access Gateway が PAP、CHAP、MSCHAP1、MSCHAP2 をサポートします。PAP のセキュリティは、通常 MSCHAP2 のものよりも低くなっています。また PAP は MSCHAP2 よりシンプルなプロトコルです。結果として、RADIUS ベンダーのほとんどはよりシンプルな PAP プロトコルと互換性がありますが、一部の RADIUS ベンダーはよりセキュリティの高い MSCHAP2 との互換性を有していません。

RSA SecurID

注： RSA SecurID タイプは、マニフェスト 3139.x 以降を実行している Horizon Cloud on Microsoft Azure デプロイでサポートされます。2022 年 3 月中旬以降の [ポッドの追加] ウィザードと [ポッドの編集] ウィザードでは RSA SecurID タイプを指定するユーザー インターフェイス オプションが表示され、選択できるようになります。

- RSA SecurID Authentication Manager サーバのアクセス キー。
- RSA SecurID 通信ポート番号。通常は 5555 で、RSA SecurID 認証 API に対する RSA Authentication Manager システム設定で設定されています。
- RSA SecurID Authentication Manager サーバのホスト名。
- RSA SecurID Authentication Manager サーバの IP アドレス。
- RSA SecurID Authentication Manager サーバまたはそのロード バランサ サーバに自己署名証明書がある場合は、[ポッドの追加] ウィザードで CA 証明書を指定する必要があります。証明書は PEM 形式である必要があります (ファイル タイプ .cer、.cert、または.pem)。

第1世代テナント - ポッド マネージャ ベースのポッドをデプロイするためのポッド デプロイ ウィザードの起動

このウィザードを使用して、ポッド マネージャ ベースのポッドを Microsoft Azure サブスクリプションに自動的にデプロイします。このウィザードを使用して最初のポッドをデプロイする際は、Horizon Universal Console の

[はじめに] ページの [Microsoft Azure] 行で、[管理] - [ポッドの追加] 機能を使用してポッド デプロイ ウィザードを開始します。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

注： クラウドベースのコンソールへのログイン認証は、VMware Cloud Services を使用したアカウント認証情報の認証に依存します。そのサービスが必要な認証要求を完了できない場合、その期間内にコンソールにログインすることはできません。コンソールの最初のログイン画面でログインの問題が発生する場合は、Horizon Cloud システム ステータス ページ (<https://status.workspaceone.com>) で最新のシステム ステータスを確認してください。そのページでは、アップデートを定期受信にすることもできます。

重要： このウィザードは、Azure VMware Solution (AVS) への Horizon ポッドのデプロイをサポートしていません。現在のリリースでは、Azure VMware Solution へのポッドのデプロイを自動化するウィザードはありません。そのタイプのポッドの場合は、まず手動で AVS の Horizon ポッドを立ち上げてから、Horizon Cloud Connector を使用して Horizon Cloud に接続する必要があります。AVS での Horizon ポッドの立ち上げの詳細については、Tech Zone の「Horizon on Azure VMware Solution Architecture」を参照してください。

前提条件

[第1世代テナント - 第1世代のポッド デプロイ ウィザードを実行するための前提条件](#)に記載されている前提条件を満たしていることを確認します。

手順

1 次のいずれかの方法を使用して、管理コンソールにログインします。

- 組織から特に指示がない限り、<https://cloud.horizon.vmware.com> の Horizon Cloud Service アドレスに移動できます。次に、システムは、<https://console.cloud.vmware.com> の標準 VMware Cloud Services ログイン画面に自動的にリダイレクトします。VMware Customer Connect アカウントの認証情報を使用してログインします (VMware Customer Connect アカウントの旧名称は My VMware アカウントでした)。アカウントの認証情報は、`user@example.com` のようなプライマリ メール アドレスと、アカウントのプロファイルで設定されているパスワードです。
- 組織によって VMware Cloud Services を使用して Horizon Cloud テナントにアクセスするように求められた場合は、まず <https://console.cloud.vmware.com> で VMware Cloud Services にログインします。VMware Cloud Services にログインしたら、[マイ サービス] セクションの下に表示される Horizon Cloud カードをクリックします。
- 組織によって Workspace ONE 環境を使用して Horizon Cloud テナントにアクセスするように求められた場合は、まずその Workspace ONE コンソールにログインしてから、サービスのセットに表示される Horizon Cloud カードを使用できます。

次のスクリーンショットは、VMware Cloud Services ログイン画面を示しています。

← → ↻ console.cloud.vmware.com/csp/gateway/discovery

VMware Cloud Services

VMware アカウントを使用してログイン

メールアドレス

name@example.com

次へ

これまでにこれらの認証情報を使用して Horizon Cloud の利用規約に同意していなかった場合、[ログイン] ボタンをクリックした後に利用規約に関する通知ボックスが表示されます。利用規約に合意して続行します。

ログインが正常に認証されると、コンソールがブラウザに表示されます。既存のポッドがない場合、デフォルトでは、[キャパシティ] セクションが展開された状態で、[クラウドのキャパシティを追加] 行で、[はじめに] ウィザードが開きます。

○ ▲ Microsoft Azure®, 0ポッド 管理 ▾

完了していません

注: 第1世代テナント - Horizon Cloud のポッドのデプロイとオンボーディングで説明したように、Horizon Cloud テナント レコードの構成によっては、VMware Cloud Services へのオンボーディングに関する青いバナーが表示されることがあります。この手順は、ポッドのデプロイには必要ありません。後で実行できます。この機能の詳細については、[Horizon Cloud テナントを VMware Cloud Services にオンボーディングする](#)を参照してください。

- 2 [クラウドのキャパシティを追加] 行で、[管理] - [ポッドを追加] の順にクリックします。



[クラウドのキャパシティを追加] ウィザードが開き、最初の手順が表示されます。

- 3 第1世代テナント - 新しい Horizon Cloud ポッドの Microsoft Azure サブスクリプション情報の指定の手順に従ってこのポッドで使用されるサブスクリプションを指定します。

第1世代テナント - 新しい Horizon Cloud ポッドの Microsoft Azure サブスクリプション情報の指定

ポッド デプロイ ウィザードのこの手順で、このポッドで使用する Microsoft Azure サブスクリプション情報を指定します。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

前提条件

- 第1世代テナント - Microsoft Azure へのポッドの自動デプロイを実行するための第1世代 Horizon Universal Console の使用に記載されている前提条件を満たしていることを確認します。
- このウィザードの手順では、第1世代テナント - Horizon Cloud ポッドのデプロイ ウィザードのためのサブスクリプション関連情報に記載されているように、サブスクリプション関連の情報があることを確認します。
- 第1世代テナント - ポッド マネージャ ベースのポッドをデプロイするためのポッド デプロイ ウィザードの起動の手順を完了させます。

手順

- 1 ウィザードの最初の手順で、以前に入力したサブスクリプションの名前を選択するか、新しいサブスクリプション情報を入力して、このポッドで使用するサブスクリプションを指定します。

The screenshot shows a wizard window titled '新規ポッド - Microsoft Azure'. The left sidebar lists steps: 1. サブスクリプション情報 (selected), 2. ポッドのセットアップ, 3. ゲートウェイ設定, 4. サマリ. The main area is 'サブスクリプション情報。' with a close button (X). A note says '*でマークされたフィールドは必須です。'. Below are fields: 'サブスクリプションの詳細', 'タイプ' (radio buttons for '新規' and '既存'), 'サブスクリプション名*' (text input), '環境*' (dropdown menu), 'サブスクリプション ID*' (text input), 'ディレクトリ ID:*' (text input), 'アプリケーション ID*' (text input), 'アプリケーション キー*' (text input with a toggle for visibility), and a toggle for '外部ゲートウェイに別のサブスクリプションを使用'. At the bottom right are 'キャンセル' and '次へ' buttons.

既存のサブスクリプションを選択すると、以前にシステムに入力されたそのサブスクリプションの情報が、この手順で自動入力されます。

注： 最初の [はじめに] ページからポッドをデプロイしているときに、以前入力したサブスクリプション情報が表示されている理由が分からない可能性があります。以前入力したサブスクリプション情報は、次のような事例において表示される可能性があります。

- ウィザードを開始して、最初のウィザード手順でサブスクリプション情報を入力し、[追加] をクリックしてサブスクリプション情報をシステムに送信してから、ウィザードを先に進みます。その後のどこかの手順で、すべての手順を完了する前にウィザードをキャンセルして終了します。この場合、[追加] をクリックしてから最初のウィザードの手順で入力したサブスクリプション情報がシステムによって保存されます。その後の手順でウィザードをキャンセルして終了しても、システムはそれ以前に入力されたサブスクリプション情報を保持します。
- 以前にこの Horizon Cloud 顧客アカウント レコードを使用して、そのアカウント レコードに対して最初とそれ以降のポッドをデプロイし、その後のある時点においてそれらのポッドを削除しました。Horizon Cloud 顧客アカウント レコードに関連付けられている認証情報でログインし直すと、以前に入力したサブスクリプション情報は引き続きその顧客のレコードと関連付けられていて、以前のサブスクリプションの名前がドロップダウン リストに表示されます。

オプション	説明
[サブスクリプションの適用]	以前に入力したサブスクリプションの名前を選択するか、[新規追加] を選択して新しいサブスクリプション情報を入力します。
[サブスクリプション名]	新しいサブスクリプション情報を入力する場合には、前に入力したサブスクリプションと区別できるように、わかりやすい名前を入力します。 名前は、文字から始まり、文字、ダッシュ、および数字のみで構成する必要があります。

オプション	説明
[環境]	<p>次のような、サブスクリプションに関連付けられているクラウド環境を選択します。</p> <ul style="list-style-type: none"> ■ [Azure - Commercial] : 標準的なグローバル Microsoft Azure クラウドの領域の場合 ■ [Azure - 中国] : Microsoft Azure (中国) クラウドの場合 ■ [Azure - US Government] : Microsoft Azure US Government クラウドの場合
[サブスクリプション ID]	クラウド キャパシティのサブスクリプション ID を UUID の形式で入力します。選択した環境で有効なサブスクリプション ID を入力してください。Microsoft Azure では、Microsoft Azure ポータルの [サブスクリプション] 領域でこの UUID を取得できます。
[ディレクトリ ID]	Microsoft Azure Active Directory のディレクトリ ID を UUID 形式 で入力します。Microsoft Azure では、Microsoft Azure ポータルの Microsoft Azure Active Directory プロパティで UUID を取得できます。
[アプリケーション ID]	Microsoft Azure ポータルで作成したサービス プリンシパルのアプリケーション ID を UUID 形式で入力します。Microsoft Azure Active Directory で、アプリケーション登録とそれに関連付けられたサービス プリンシパルを作成することは必須です。
[アプリケーション キー]	Microsoft Azure ポータルで作成したサービス プリンシパル認証キーの値を入力します。このキーの作成は必須です。
[外部ゲートウェイに別のサブスクリプションを使用]	<p>外部の Unified Access Gateway 構成をポッドのサブスクリプションとは別の専用のサブスクリプションにデプロイする場合は、このトグルを有効にします。外部ゲートウェイに個別のサブスクリプションを使用すると、組織はチームの専門分野に応じて、それらのサブスクリプションを制御する個別のチームを柔軟に割り当てることができます。これにより、組織内のどのユーザーがサブスクリプションのリソース グループ内のポッドのアセットにアクセスでき、どのユーザーがゲートウェイのアセットにアクセスできるかについて、よりきめ細かなアクセス制御が可能になります。</p> <p>このトグルをオンにすると、ゲートウェイのサブスクリプション情報を入力するためのフィールドが表示されます。ポッドのサブスクリプションの場合と同様に、これらのフィールドに情報を指定します。</p>

重要： この画面では、特定の [サブスクリプション名] に関連付けられた、以前に入力したサブスクリプション値を削除する方法はありません。これが発生するのはまれなことではありますが、次のような状況を想定できます。

- a Microsoft Azure でサブスクリプション関連の要素を設定します。
- b [クラウドのキャパシティを追加] ウィザードを開始し、最初の手順でこれらのサブスクリプションの値を入力し、次のウィザードの手順に進みます。
- c ただし、ウィザードの次の手順で要求されたネットワークの値の読み取り時に、このウィザードをキャンセルして終了し、新しいブラウザー タブを開いて Microsoft Azure ポータルに移動し、前提条件を満たすようにネットワーク構成を調整します。
- d Microsoft Azure ポータルにいる間に、サービス プロバイダを別の名前を利用するために新しいアプリケーション登録を行うことも決めます。
- e [はじめに] ページがあるブラウザーに戻り、[クラウドのキャパシティを追加] ウィザードを再び開始します。

この時点で、以前に入力したサブスクリプション名は引き続き [サブスクリプションの適用] ドロップ ダウン リストにあります。ただし、その名前を選択すると、すべてのフィールドが古いアプリケーション ID を含む以前の値で自動入力され、この特定の画面内で値を変更することや、そのサブスクリプション名を編集または削除して、同じ名前でもやり直すことはできません。この問題が発生した場合は、まずウィザードをキャンセルします。次に、コンソールの [はじめに] ページに移動し、[管理] - [サブスクリプションの管理] の順にクリックし、[削除] アクションを使用して、以前に入力したサブスクリプション名を削除します。その後、新しいポッド ウィザードを再起動し、使用したい値を入力して続行できます。

次のスクリーンショットは、主なサブスクリプションの詳細の入力が完了した状態の例です。

The screenshot shows a wizard window titled '新規ポッド - Microsoft Azure'. The left sidebar lists steps: 1. サブスクリプション情報 (selected), 2. ポッドのセットアップ, 3. ゲートウェイ設定, 4. サマリ. The main area is 'サブスクリプション情報' with a close button. A note says '*でマークされたフィールドは必須です.' Below are fields for 'サブスクリプションの詳細':

- タイプ: Radio buttons for '新規' (selected) and '既存'.
- サブスクリプション名*: Text input with 'Sub3' and an info icon.
- 環境*: Dropdown menu with '選択' and an info icon.
- サブスクリプション ID*: Text input with an info icon.
- ディレクトリ ID*: Text input with an info icon.
- アプリケーション ID*: Text input with an info icon.
- アプリケーション キー*: Text input with an info icon.
- 外部ゲートウェイに別のサブスクリプションを使用: Toggle switch (off) with an info icon.

 At the bottom right are 'キャンセル' and '次へ' buttons.

2 ウィザードの次の手順に進みます。

次の手順に進むためのボタンをクリックすると、システムは指定されたすべての値の有効性、および値が相互に適切に関連しているかどうかを、以下のように検証します。

- 指定したサブスクリプション ID は選択した環境で有効か。
- 指定したディレクトリ ID、アプリケーション ID、およびアプリケーション キーがそのサブスクリプションで有効か。
- 指定したアプリケーション ID のアプリケーションのサービス プリンシパルに、実行しているデプロイのタイプのためにデプロイ プロセスで必要となるすべての操作を許可するロールが割り当てられているか。サービス プリンシパルとそのロールの要件については、「[アプリケーションの登録と必要なサービス プリンシパルの作成](#)」と「[第1世代テナント - 組織が第1世代 Horizon Cloud のアプリケーション登録にカスタムロールを使用することを希望する場合](#)」のトピックを参照してください。

値の修正に関するエラー メッセージが表示される場合は、少なくとも1つの値が、サブスクリプションに存在しないか、別の値との有効な関係を持っていないかのいずれかの理由で無効になっています。次に、そのエラー メッセージが表示される可能性がある状況を、すべてではありませんが、いくつかリストで示します。

- サブスクリプションにある [ディレクトリ ID] を指定して、別のディレクトリにある [アプリケーション ID] の値を指定した場合。
- 指定されたサービス プリンシパルに割り当てられたロールが、ポッド デプロイヤーで要求される操作を許可しない場合。

重要： このエラー メッセージが表示される場合は、複数の要素が無効である可能性があります。この場合は、収集したサブスクリプション関連情報とサービス プリンシパルの構成を確認します。

3 第1世代テナント - デプロイ ウィザードを使用して Microsoft Azure にデプロイする Horizon Cloud ポッドのポッド構成情報の指定の手順に従ってポッドの詳細とネットワーク情報を指定します。

第 1 世代テナント - デプロイ ウィザードを使用して Microsoft Azure にデプロイする Horizon Cloud ポッドのポッド構成情報の指定

ポッド デプロイ ウィザードのポッド セットアップの手順で、ネットワーク情報に加えて、ポッドの名前などの詳細を指定します。

重要: この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、[該当記事を参照してください](#)。

注意: このウィザードは、ポッド マネージャ ベースのタイプのポッドをデプロイします。現在、コンソールには、Azure VMware Solution (AVS) に Horizon ポッドをデプロイするためのデプロイ ウィザードが用意されていません。AVS での Horizon ポッドのデプロイの詳細については、Tech Zone の [Horizon on Azure VMware Solution Architecture](#) を参照してください。

注意: 以下の手順で示す IP アドレスはサンプルです。組織の要件を満たすアドレス範囲を使用してください。IP アドレス範囲の記述がある手順では、組織に適切な IP アドレスに置き換えてください。

前提条件

[第 1 世代テナント - 第 1 世代のポッド デプロイ ウィザードを実行するための前提条件](#)に記載されている前提条件を満たしていることを確認します。

デプロイ プロセスに必要なサブネットを自動作成する場合、ウィザード フィールドでこれらのサブネット用に指定する CIDR アドレス範囲が、Microsoft Azure 内の VNet 上の既存のサブネットによって使用されていないことを確認します。

このポッドで使用するために事前にサブネットを作成済みである場合は、それらのサブネットにリソースが接続されていないことを確認し、管理サブネットに使用するために作成したサブネットには、そのサブネット用のサービス エンドポイントとして構成された Microsoft .SQL サービスがあることを確認します。ポッド デプロイ ウィザードで、Microsoft .SQL サービスが管理サブネット上のサービス エンドポイントとして構成されていることを検証します。

注意: ポッドのデプロイのために VNet 上に作成するこれらのサブネットは空である必要があります。ポッドをデプロイする前にサブネットを作成することが可能ですが、これらのサブネットにいかなるリソースも配置しないでください。またいかなる IP アドレスも使用しないでください。IP アドレスがサブネットで既に使用されていると、ポッドのデプロイに失敗する可能性があります。

手順

1 ウィザードのこの手順で、ポッドに関する詳細と必要なネットワーク情報を提供します。

次のスクリーンショットは、最初に表示されるときの手順の例です。

Add Microsoft Azure Capacity ×

1. Subscription
2. Pod Setup
3. Gateway Settings
4. Summary

Enter details to configure and connect the pod.

Details

Pod Name: ⓘ

Location: Add New ⓘ Add

Microsoft Azure Region: Select ⓘ

Description:

Azure Resource Tags:

Name	Value
<input type="text"/>	<input type="text"/>

+ ⓘ

Networking

Virtual Network: ▼ ⓘ

Use Existing Subnet: ⓘ

Management Subnet (CIDR): ⓘ

VM Subnet (CIDR) - Primary: ⓘ

NTP Servers: ⓘ

Use Proxy: ⓘ

CANCEL
BACK
NEXT

オプション**説明**

[ポッド名]	このポッドにわかりやすい名前を入力します。管理コンソールでは、他のポッドと区別するために、この名前が使用されます。
[場所]	<p>既存の市区町村名を選択するか、[追加] をクリックして新しい市区町村名を指定します。</p> <p>システムは市区町村名に基づいてポッドをグループ化し、コンソールの [ダッシュボード] ページの [Horizon のグローバルな占有量] マップに表示します。</p> <p>[追加] をクリックして、市区町村の名前を入力します。システムは自動的にバックエンドの地理参照テーブルにある、入力した文字に一致する世界の市区町村名表示するので、そのリストから市区町村を選択できます。</p> <p>注: システムのオートコンプリート リストから市区町村を選択する必要があります。現在、既知の問題により、ローケーション名はローカライズされていません。</p>

オプション	説明
[Microsoft Azure リージョン]	<p>ポッドを展開する実際の地理的な Microsoft Azure リージョンを選択します。利用可能なリージョンは、以前に選択した Microsoft Azure 環境によって決まります。</p> <p>リージョンを選択するときは、このポッドからサービスを利用するエンド ユーザーとの近接性を考慮します。エンド ユーザーがより近接している場合、遅延は少なくなります。</p> <p>重要： 一部の Microsoft Azure リージョンでは、GPU が有効な仮想マシンはサポートされません。GPU 対応のデスクトップまたはリモート アプリケーションでポッドを使用する場合は、使用する NV シリーズ、NVv4 シリーズ、NCv2 シリーズの仮想マシン タイプが、ポッド用に選択した Microsoft Azure のリージョンで提供されていることと、この Horizon Cloud リリースでサポートされていることを確認します。詳細については、https://azure.microsoft.com/ja-jp/regions/services/ にある Microsoft のドキュメントを参照してください。</p>
[説明]	<p>オプション：このポッドの説明を入力します。</p>
[Azure リソース タグ]	<p>オプション：Azure リソース グループに適用するカスタム タグを作成します。Azure リソース タグはリソース グループにのみ適用され、グループ内のリソースには継承されません。</p> <p>最初のタグを作成するには、[名前] と [値] のフィールドに情報を入力します。追加のタグを作成するには、[[+]] をクリックし、既存のフィールドの下に表示される [名前] と [値] のフィールドに情報を入力します。</p> <ul style="list-style-type: none"> ■ 最大 10 個のタグを作成できます。 ■ タグの名前は 512 文字に制限され、タグの値は 256 文字に制限されます。ストレージ アカウントの場合、タグの名前は 128 文字に制限され、タグの値は 256 文字に制限されます。 ■ タグの名前には次の文字を含めることはできません。 <p>< > % & \ ? /</p> ■ タグ名に大文字と小文字を区別しない文字列（「azure」、「windows」、「microsoft」）を含めることはできません。 ■ タグ名とタグ値には、ASCII 文字のみを含めることができます。標準の 128 文字 ASCII セット（拡張 ASCII または拡張 ASCII 文字とも呼ばれる）以外の空白および文字は使用できません。
[仮想ネットワーク]	<p>リストから仮想ネットワークを選択します。</p> <p>[Microsoft Azure リージョン] フィールドで選択されたリージョンに存在する仮想ネットワーク (VNet) のみがここに表示されます。Microsoft Azure サブスクリプションで、そのリージョンで使用する VNet をすでに作成している必要があります。</p>
[既存のサブネットを使用]	<p>ポッドのサブネット要件を満たすよう事前にサブネットを作成済みの場合は、このトグルを有効にします。このトグルを [はい] に設定すると、サブネットを指定するためのウィザード フィールドは、ドロップダウン選択メニューに変わります。</p> <p>重要： このウィザードは、必要なサブネットの 1 つとして既存のサブネットを使用すること、またはその他の必要なサブネットに対して CIDR アドレスを入力することをサポートしません。このトグルを [はい] に設定している場合は、ポッドの必要なサブネットをすべて既存のサブネットから選択する必要があります。</p>

オプション	説明
[管理サブネット] [管理サブネット (CIDR)]	<p>[既存のサブネットを使用] を有効にすると、このメニューに、[仮想ネットワーク] に選択した VNet 上で使用可能なサブネットが一覧表示されます。ポッドの管理サブネットに使用する既存のサブネットを選択します。</p> <hr/> <p>重要：</p> <ul style="list-style-type: none"> ■ サブネットのサービス エンドポイントとして構成された Microsoft.SQL サービスがあるサブネットを選択します。このサービス エンドポイントは、管理サブネットを介した、ポッド マネージャ仮想マシンとポッドの Azure Postgres データベースとの間で必要となる通信をサポートします。 <p>接続されているその他のリソースがない空のサブネットを選択します。サブネットが空でない場合、デプロイ中またはポッドの操作中に予期しない結果が発生する可能性があります。</p> <hr/> <p>[既存のサブネットを使用] がオフになっている場合、サブネットのアドレス範囲を CIDR 表記 (192.168.8.0/27 など) で入力して、ポッドと Unified Access Gateway インスタンスが接続するサブネットをデプロイヤーが作成するようにします。管理サブネットの場合、少なくとも /27 の CIDR が必要です。</p> <hr/> <p>注意： 既存のサブネットを使用するウィザード オプションを選択しない場合、そのサブネットが Microsoft Azure 環境に存在していない必要があります。既に存在している場合は、ウィザードの次の手順に進もうとするとエラーが発生します。</p>
[仮想マシン サブネット - プライマリ] [仮想マシン サブネット (CIDR) - プライマリ]	<p>このフィールドは、ポッドがエンドユーザーのデスクトップとアプリケーションを提供するためにプロビジョニングする仮想マシンに使用するサブネットに関連します。このような仮想マシンには、ゴールド イメージ仮想マシン、ファームの RDSH 対応仮想マシン、VDI デスクトップ仮想マシンなどが該当します。</p> <p>[既存のサブネットを使用] を有効にすると、このメニューに、[仮想ネットワーク] に選択した VNet 上で使用可能なサブネットが一覧表示されます。これらの仮想マシンに使用する既存のサブネットを選択します。</p> <hr/> <p>重要： 接続されているその他のリソースがない空のサブネットを選択します。サブネットが空でない場合、デプロイ中またはポッドの操作中に予期しない結果が発生する可能性があります。</p> <hr/> <p>[既存のサブネットを使用] がオフになっている場合、サブネットのアドレス範囲を CIDR 表記 (192.168.12.0/22 など) で入力して、ポッドのデプロイ時にこのこのサブネットをデプロイヤーが作成するようにします。デスクトップ サブネットの場合、少なくとも /27 の CIDR が必要であり、/22 の CIDR を推奨します。</p> <hr/> <p>重要： ファームの RDSH 対応仮想マシンと VDI デスクトップ仮想マシンをエンド ユーザーに提供できるように、このポッドでプロビジョニングする予定の仮想マシンの台数に十分対応できる範囲を入力します。このデスクトップのサブネットは、ポッドをデプロイした後は拡張できません。</p> <hr/> <p>注意： 既存のサブネットを使用するウィザード オプションを選択しない場合、そのサブネットが Microsoft Azure 環境に存在していない必要があります。既に存在している場合は、ウィザードの次の手順に進もうとするとエラーが発生します。</p>

オプション	説明
[NTP サーバ]	<p>時刻を同期するために使用する NTP サーバのリストをカンマで区切って入力します。</p> <p>ここで入力する NTP サーバは、パブリック NTP サーバ、または時刻同期を指定するために設定する独自の NTP サーバです。ここで指定した NTP サーバは、使用するポッドのために [仮想ネットワーク] フィールドで選択した仮想ネットワークからアクセスできる必要があります。このフィールドでは、各 NTP サーバを IP アドレスまたはドメイン名のいずれかで指定できます。このフィールドに IP アドレスの代わりにドメイン名を入力する場合、仮想ネットワークに対して構成された DNS が指定された名前を解決できることを確認する必要があります。</p> <p>パブリック NTP サーバのドメイン名の例は、time.windows.com、us.pool.ntp.org、time.google.com です。</p>
[プロキシを使用]	<p>アウトバウンド インターネット接続用のプロキシが必要な場合は、このトグルを有効にして、表示される関連フィールドに入力します。</p> <p>ポッド デプロイは、ソフトウェアを Microsoft Azure クラウド環境に安全にダウンロードし、Horizon Cloud クラウド制御プレーンに接続するために、インターネットへのアウトバウンド アクセスを必要とします。ポッドでプロキシ設定を使用するには、トグルを有効にした後、次の情報を提供する必要があります。</p> <ul style="list-style-type: none"> ■ [プロキシ] (必須)：プロキシ サーバのホスト名または IP アドレスを入力します。 ■ [ポート] (必須)：プロキシ サーバの設定で指定されているポート番号を入力します。 <p>プロキシ サーバ設定で認証のためのユーザー名とパスワードが必要な場合は、次の認証情報も入力します。</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>プロキシを使用 <input checked="" type="checkbox"/> ⓘ</p> <p>プロキシ * _____ ⓘ</p> <p>ポート * _____ ⓘ</p> <p>ユーザー名 _____ ⓘ</p> <p>パスワード • _____ ⓘ ⓘ</p> <p>パスワードの検証 ↓ _____ ⓘ ⓘ</p> </div>

次のスクリーンショットは、VNet で事前に作成されたサブネットを使用してこの手順を完了した例です。この例では、アウトバウンド インターネット接続の要件を満たすために、プロキシは必要ありません。

ネットワーク関連の名前が編集されました。

Enter details to configure and connect the pod.

Details

Pod Name:* NorthWestSites ⓘ

Location:* Seattle, WA, United States ⓘ [Edit](#)

Microsoft Azure Region:* West US 2 ⓘ

Description:

Azure Resource Tags:

Environment	dev	🗑️	ⓘ
BU	product	🗑️	+

Networking

Virtual Network:* [Redacted] ⓘ

Use Existing Subnet: ⓘ

Management Subnet:* z [Redacted] m1 [192.168.24.0/27] ⓘ

VM Subnet - Primary:* z [Redacted] t1 [192.168.25.0/27] ⓘ

NTP Servers:* time.windows.com,us.pool.ntp.org ⓘ

Use Proxy: ⓘ

CANCEL
BACK
NEXT

2 [次へ] をクリックして、次の手順に進みます。

3 第1世代テナント - Horizon Cloud ポッドのゲートウェイ構成の指定の手順に従って、ポッドに Unified Access Gateway 構成を作成するための詳細を指定します。エンド ユーザーがインターネット経由で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できるようにするためには、外部 Unified Access Gateway 構成が必要です。

第1世代テナント - Horizon Cloud ポッドのゲートウェイ構成の指定

ウィザードのこの手順では、1つ以上のゲートウェイが構成されているポッド マネージャ ベースのポッドをデプロイするために必要な情報を指定します。Unified Access Gateway は、このタイプのポッドのゲートウェイ環境を提供します。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

外部ゲートウェイ構成

外部ゲートウェイ構成では、企業のネットワークの外部にいる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できるようにすることができます。ポッドにこの外部ゲートウェイ構成がある場合、ポッドには、このアクセスを提供するための [Azure ロード バランサ リソース](#) と Unified Access Gateway インスタンスが含まれています。この場合、各インスタンスには3つのNICがあります：1つは管理サブネット上のNIC、1つはデスクトップ サブネット上のNIC、そしてもう1つはDMZ サブネット上のNICです。デプロイ ウィザードでは、ロード バランサにプライベート IP アドレスを使用するか、パブリック IP アドレスを使用するかに応じて、ロード バランシング タイプをプライベートまたはパブリックのいずれかに指定するためのオプションがあります。ウィザードでこのパブリック IP のトグルをオフに切り替えると、IP アドレスを指定する必要があるフィールドがウィザードに表示されます。このタイプの構成では、Horizon Client からゲートウェイへの PCoIP 接続でこの IP アドレスが使用されます。

外部ゲートウェイ構成の場合、ポッドの VNet とは別の VNet に構成をデプロイするオプションもあります。VNet をピア接続する必要があります。このタイプの構成では、ポッドを [ハブ - スポーク ネットワーク トポロジ](#) など Microsoft Azure のより複雑なネットワーク トポロジにデプロイできます。

注： 最初のウィザードのステップで、外部ゲートウェイが専用のサブスクリプションを使用するトグルを有効にした場合、外部ゲートウェイを専用の VNet (そのサブスクリプションに関連付けられている VNet) にデプロイする必要があります。このトグルを有効にした場合、必要に応じて、外部ゲートウェイのリソース用にそのサブスクリプションの既存のリソース グループを選択できます。このウィザードのステップで選択できるように、事前にそのリソース グループを準備しておく必要があります。

内部ゲートウェイ構成

内部ゲートウェイ構成は、企業のネットワークの内部にいるエンド ユーザーに対して、デスクトップおよびアプリケーションへの信頼される HTML Access (Blast) 接続機能を提供します。内部ゲートウェイ構成を使用してポッドが構成されていない場合、企業のネットワーク内のエンド ユーザーは、ブラウザを使用してデスクトップやアプリケーションに HTML Access (Blast) 接続をする際に標準ブラウザの信頼されていない証明書エラーに遭遇します。ポッドにこの内部ゲートウェイ構成がある場合、ポッドには、このアクセスを提供するための [Azure ロード バランサのリソース](#) と Unified Access Gateway インスタンスが含まれています。この場合、各インスタンスには2つのNICがあります：1つは管理サブネット上のNIC、1つはデスクトップ サブネット上のNICです。デフォルトでは、このゲートウェイのロード バランシング タイプはプライベートです。

次のスクリーンショットは、最初に表示されるときの手順の例です。一部のコントロールは、最初のウィザード手順で外部ゲートウェイ構成に別のサブスクリプションを使用することを選択した場合にのみ表示されます。

Add Microsoft Azure Capacity
✕

1. Subscription
2. Pod Setup
3. Gateway Settings
4. Summary

Set up external and internal Unified Access Gateways for this pod. If Universal Broker two-factor authentication is enabled, an external gateway with two-factor authentication is required.

External Gateway

Enable External Gateway? ⓘ

FQDN:* ⓘ

DNS Addresses: ⓘ

Routes: ⓘ

Inherit Pod NTP Servers: ⓘ

VM Model:* Standard_A4_v2 (4 CPUs, 8 Gi... ⓘ

Certificate:* Upload ⓘ

Blast Extreme TCP Port:* 8443 ⓘ

Cipher Suites:*

- TLS ECDHE RSA WITH AES 128 GCM SH...
- TLS ECDHE RSA WITH AES 256 GCM SH...
- TLS ECDHE RSA WITH AES 128 CBC SH...
- TLS ECDHE RSA WITH AES 256 CBC SH...

 At least one cipher suite should be selected.

Load Balancer

Enable Public IP? ⓘ

Networking

Use a Different Virtual Network: ⓘ

DMZ Subnet:* Select ⓘ

Two-Factor Authentication

Enable two-factor authentication: ⓘ

Internal Gateway

Enable Internal Gateway? ⓘ

Azure Resource Tags ⓘ

Inherit Pod Tags: ⓘ

CANCEL
BACK
VALIDATE & PROCEED

前提条件

第 1 世代テナント - 第 1 世代のポッド デプロイ ウィザードを実行するための前提条件に記載されている前提条件を満たしていることを確認します。

Unified Access Gateway インスタンスに使用する仮想マシン モデルを決定します。このポッドに指定した Microsoft Azure サブスクリプションが、選択したモデルの 2 台の仮想マシンのキャパシティを確実に満たすようにする必要があります。ポッドあたりのセッション数が 2,000 にまで拡大することが想定される環境では、F8s_v2 を使用します。VMware Horizon Cloud Service on Microsoft Azure サービスの制限で説明したように、A4_v2 仮想マシン モデルが十分に機能するのは、ポッド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 (概念実証) 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。

重要： よく考えて、仮想マシン モデルを選択します。現在のサービス リリースでは、ゲートウェイ構成のデプロイ後に、デプロイされたインスタンスで使用される仮想マシン モデルを簡単に変更することはできません。デプロイ後に仮想マシン モデルを変更するには、ゲートウェイ構成を削除して再デプロイする必要があります。

重要： この手順を完了するには、エンド ユーザーがサービスにアクセスするために必要な完全修飾ドメイン名 (FQDN) と、その FQDN に基づく署名付きの SSL 証明書 (PEM 形式) を取得する必要があります。証明書は信頼されている認証局 (CA) によって署名する必要があります。1 つの PEM ファイルに、SSL 証明書の中間証明書、ルート CA 証明書、プライベート キーを含む、完全な証明書チェーンが含まれている必要があります。詳細については、[第1世代テナント - 第1世代 Horizon Cloud ポッドのデプロイに必要な PEM 形式への証明書ファイルの変換](#)を参照してください。

証明書チェーン内のすべての証明書の有効期限が切れていないことを確認します。証明書チェーン内のいずれかの証明書の有効期限が切れている場合、後からポッドのオンボーディング プロセスで予期しない不具合が発生する可能性があります。

この FQDN には、アンダー スコアを含めることはできません。このリリースでは、FQDN にアンダー スコアが含まれていると、Unified Access Gateway インスタンスへの接続が失敗します。

外部ゲートウェイ構成を選択する場合、Horizon Cloud は、外部ゲートウェイ構成に指定された FQDN がパブリックに解決可能であることを想定します。[パブリック IP アドレスを有効にしますか?] トグルをウィザードでオフに切り替えてファイアウォールまたは NAT セットアップから IP アドレスを指定した場合、ファイアウォール内または NAT セットアップ内の IP アドレスにこの FQDN が割り当てられていることを確認する必要があります。この FQDN は、ゲートウェイへの PCoIP 接続に使用されます。

テナントが、2 要素認証が構成されている Universal Broker で構成されている場合は、2 要素認証設定を使用して外部 Unified Access Gateway を構成する必要があります。

手順

1 外部ゲートウェイ構成を使用する場合、[外部ゲートウェイ] セクションのフィールドをすべて入力します。

オプション	説明
[外部ゲートウェイを有効にしますか?]	<p>ポッドに外部ゲートウェイ構成があるかどうかを制御します。外部構成を使用すると、企業のネットワークの外部にいる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できるようになります。ポッドには、このアクセスを提供する Microsoft Azure ロード バランサ リソースと Unified Access Gateway インスタンスが含まれています。</p> <p>注： デフォルトの有効になっている設定にしておくことをお勧めします。</p> <p>このトグルをオフにすると、クライアントは、コネクタ アプライアンスがポッド マネージャに直接統合された Workspace ONE Access を介して接続するか、クライアントがポッド マネージャのロード バランサに直接接続するか、内部ゲートウェイ構成を介して接続する必要があります。これらのうち、クライアントがポッドに統合された Workspace ONE Access を介して接続する、またはクライアントがロード バランサに直接接続する最初の 2 つのシナリオでは、デプロイ後にいくつかの手順が必要になります。これらのシナリオでは、ポッドがデプロイされた後、ポッド マネージャ仮想マシンで SSL 証明書を直接構成するの手順に従って、SSL 証明書をポッド マネージャ仮想マシンにアップロードします。</p>
[FQDN]	<p>ourOrg.example.com のような、必要な完全修飾ドメイン名 (FQDN) を入力します。これは、ポッド デプロイヤーがゲートウェイの Unified Access Gateway インスタンスの構成で指定するドメイン名です。このドメイン名を所有し、その FQDN を検証可能な PEM 形式の証明書を取得する必要があります。</p> <p>Horizon Cloud は、外部ゲートウェイ構成に指定されたこの FQDN がパブリックに解決可能であることを想定します。[パブリック IP アドレスを有効にしますか?] トグルをオフに切り替えてファイアウォールまたは NAT セットアップから IP アドレスを指定した場合、ファイアウォール内または NAT セットアップ内の IP アドレスにこの FQDN が割り当てられていることを確認する必要があります。この FQDN は、ゲートウェイへの PCoIP 接続に使用されます。</p> <p>重要： この FQDN には、アンダー スコアを含めることはできません。このリリースでは、FQDN にアンダー スコアが含まれていると、Unified Access Gateway インスタンスへの接続が失敗します。</p>
[DNS アドレス]	<p>オプションで、Unified Access Gateway が名前解決に使用できる追加の DNS サーバのアドレスを、カンマ区切りで入力します。</p> <p>Unified Access Gateway インスタンスのデプロイ先となる VNet トポロジの外部にある 2 要素認証サーバで 2 要素認証を使用するようにこの外部 Unified Access Gateway 構成を構成する場合は、その認証サーバのホスト名を解決できる DNS サーバのアドレスを指定します。たとえば、2 要素認証サーバがオンプレミスにある場合は、その認証サーバの名前を解決できる DNS サーバのアドレスを入力します。</p> <p>すべてのデプロイの前提条件で説明されているように、Horizon Cloud on Microsoft Azure のデプロイに使用される VNet トポロジは、Unified Access Gateway インスタンスのデプロイ中に、また、その進行中の操作のために、外部の名前解決を提供する DNS サーバと通信する必要があります。</p> <p>デフォルトでは、インスタンスがデプロイされる VNet で構成されている DNS サーバが使用されます。</p> <p>[DNS アドレス] にアドレスを指定すると、デプロイされた Unified Access Gateway インスタンスは、VNet の構成の DNS サーバ情報に加えてこれらのアドレスを使用します。</p>
[ルート]	<p>オプションで、デプロイした Unified Access Gateway インスタンスが、エンド ユーザー アクセス用のネットワークのルーティングを解決するために使用する、追加のゲートウェイへのカスタム ルートを指定します。指定したルートは、Unified Access Gateway が 2 要素認証サーバとの通信などにネットワーク ルーティングを解決できるようにするために使用されます。</p> <p>このポッドをオンプレミスの認証サーバで 2 要素認証を使用するように構成する場合は、Unified Access Gateway インスタンスがそのサーバに接続するための正しいルートを入力する必要があります。たとえば、オンプレミスの認証サーバがその IP アドレスとして 10.10.60.20 を使用している場合、10.10.60.0/24 とデフォルト ルートのゲートウェイ アドレスをカスタム ルートとして入力することになります。この Horizon Cloud on Microsoft Azure デプロイで使用している Express ルートまたは VPN 構成からデフォルト ルートのゲートウェイ アドレスを取得します。</p> <p>形式 <code>ipv4-network-address/bits ipv4-gateway-address</code> で、カンマ区切りリストとしてカスタム ルートを指定します (例: 192.168.1.0/24 192.168.0.1, 192.168.2.0/24 192.168.0.2)。</p>

オプション	説明
[ポッドの NTP サーバの継承]	<p>このトグルはデフォルトで有効になっており、Unified Access Gateway インスタンスは、ポッド マネージャ インスタンスに指定されているのと同じ NTP サーバを使用します。このトグルを有効にしておくことを強くお勧めします。</p> <p>ポッド マネージャ インスタンス、Unified Access Gateway インスタンス、および Active Directory サーバに同じ NTP サーバを使用することがベスト プラクティスです。タイム スキューは、これらのインスタンスが異なる NTP サーバを使用する場合に発生する可能性があります。このようなタイム スキューにより、後でゲートウェイがデスクトップおよびアプリケーションに対してエンド ユーザー セッションを認証しようとしたときに、エラーが発生する可能性があります。</p> <p>このトグルを有効にして、外部ゲートウェイをポッドの VNet とは別の専用の VNet にデプロイする場合は、ポッド マネージャ インスタンスに指定された NTP サーバに、外部ゲートウェイのデプロイ用に選択した仮想ネットワークからアクセスできることを確認します。</p>
[仮想マシン モデル]	<p>Unified Access Gateway インスタンスに使用するモデルを選択します。このポッドに指定した Microsoft Azure サブスクリプションが、選択したモデルの 2 台の仮想マシンのキャパシティを確実に満たすようにする必要があります。</p> <p>重要： 現在のサービス リリースでは、サブスクリプション内でゲートウェイ構成がデプロイされた後、これらのインスタンスで使用される仮想マシン モデルを簡単に変更することはできません。デプロイ後に仮想マシン モデルを変更するには、ゲートウェイ構成を削除して再デプロイする必要があります。ポッドあたりのセッション数が 2,000 にまで拡大することが想定される環境では、F8s_v2 を使用します。VMware Horizon Cloud Service on Microsoft Azure サービスの制限で説明したように、A4_v2 仮想マシン モデルが十分に機能するのは、ポッド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 (概念実証) 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。</p>
[証明書]	<p>Microsoft Azure で実行中の Unified Access Gateway インスタンスへの接続をクライアントが信頼できるようにするために、Unified Access Gateway で使用される PEM 形式の証明書をアップロードします。証明書は、入力した FQDN に基づいたものにして、信頼されている認証局 (CA) によって署名されている必要があります。PEM ファイルに、SSL 証明書、中間証明書、ルート CA 証明書、プライベート キーを含む、完全な証明書チェーンが含まれている必要があります。</p>
[Blast Extreme TCP ポート]	<p>Unified Access Gateway 構成内の Blast Extreme TCP 設定で使用する TCP ポートを選択します。この設定は、クライアントから送信されるデータ トラフィックに対し Unified Access Gateway 上の Blast Secure Gateway 経由の Blast Extreme に関連しています。ポート 8443 は、より効率的で、パフォーマンスが向上し、Unified Access Gateway インスタンスでのリソース使用率が低いため、推奨されます。このような理由により、ウィザードのデフォルト値は 8443 です。もう 1 つの選択肢である 443 は、効率が低く、パフォーマンスが低下して、インスタンスで CPU の輻輳が発生し、エンドユーザー クライアントでトラフィックの遅延が見られる可能性があります。443 の選択肢は、組織でクライアント側の制限が設定されている場合 (組織で 443 送信のみが許可されているなど) にのみ使用する必要があります。</p> <p>注： Blast Extreme に使用される UDP ポートは、この設定の影響を受けず、常に UDP 8443 です。</p>
[暗号スイート]	<p>ほとんどの場合、デフォルト設定を変更する必要はありませんが、Unified Access Gateway には、クライアントと Unified Access Gateway アプライアンス間の通信の暗号化に使用される暗号化アルゴリズムをオプションで指定するためのこの機能が用意されています。</p> <p>画面上のリストから少なくとも 1 つの暗号スイートを選択する必要があります。画面上のリストには、Horizon Cloud on Microsoft Azure 環境で許可されている暗号スイートが表示されます。</p>

このゲートウェイの Microsoft ロード バランサの設定を指定します。

オプション	説明
[パブリック IP アドレスを有効にしますか?]	<p>このゲートウェイのロード バランシング タイプがプライベートとして構成されるか、パブリックとして構成されるかを制御します。オンに切り替えると、デプロイされた Microsoft Azure ロード バランサ リソースがパブリック IP アドレスで構成されます。オフに切り替えると、Microsoft Azure ロード バランサ リソースがプライベート IP アドレスで構成されます。</p> <p>重要： このリリースでは、外部ゲートウェイのロード バランシング タイプを後でパブリックからプライベートに、またはプライベートからパブリックに変更することはできません。この変更を行う唯一の方法は、デプロイされたポッドからゲートウェイ構成を完全に削除してから、ポッドを編集して逆の設定で追加することです。</p> <p>このトグルをオフに切り替えると、[Horizon FQDN のパブリック IP アドレス] フィールドが表示されます。</p>
[Horizon FQDN のパブリック IP アドレス]	<p>デプロイされた Microsoft Azure ロード バランサをパブリック IP アドレスで構成しないことを選択した場合、[FQDN] フィールドで指定した FQDN を割り当てる IP アドレスを指定する必要があります。エンドユーザーの Horizon Client は、ゲートウェイへの PCoIP 接続にこの FQDN を使用します。デプロイは、この IP アドレスを Unified Access Gateway 構成の設定で構成します。</p>

外部ゲートウェイのネットワーク設定を指定します。

オプション	説明
[別の仮想ネットワークを使用]	<p>このトグルは、外部ゲートウェイをポッドの VNet とは別の専用の VNet にデプロイするかどうかを制御します。次の行は、さまざまなケースを示しています。</p> <p>注： ウィザードの最初のステップで外部ゲートウェイに別のサブスクリプションを使用するように指定した場合、このトグルはデフォルトで有効になっています。その場合は、ゲートウェイの VNet を選択する必要があります。</p> <p>このトグルをオンにして、[ポッドの NTP サーバの継承] トグルをオンに切り替える場合は、ポッド マネージャ インスタンスに指定された NTP サーバに、外部ゲートウェイのデプロイ用に選択した仮想ネットワークからアクセスできることを確認します。</p>
[別の仮想ネットワークを使用] - オフ	<p>トグルをオフに切り替えると、外部ゲートウェイがポッドの VNet にデプロイされます。この場合は、DMZ サブネットを指定する必要があります。</p> <ul style="list-style-type: none"> ■ [DMZ サブネット] - ポッドのセットアップ ウィザード手順で [既存のサブネットを使用] を有効にすると、[DMZ サブネット] には [仮想ネットワーク] に対して選択された VNet 上で使用可能なサブネットが表示されます。ポッドの DMZ サブネットに使用する既存のサブネットを選択します。 <p>重要： 接続されているその他のリソースがない空のサブネットを選択します。サブネットが空でない場合、デプロイ中またはポッドの操作中に予期しない結果が発生する可能性があります。</p> <ul style="list-style-type: none"> ■ [DMZ サブネット (CIDR)] - 前のウィザード手順で [既存のサブネットを使用] がオフになっている場合、DMZ (非武装地帯) ネットワークのサブネットを CIDR 表記で入力します。このネットワークは、Unified Access Gateway インスタンスをゲートウェイの Microsoft Azure パブリック ロード バランサに接続するように構成されます。
[別の仮想ネットワークを使用] - 有効	<p>トグルを有効にすると、外部ゲートウェイが専用の VNet にデプロイされます。この場合、使用する VNet を選択してから、必要な 3 つのサブネットを指定する必要があります。[既存のサブネットを使用] トグルを有効にして、指定した VNet で事前に作成したサブネットから選択します。そうでない場合は、サブネットを CIDR 表記で指定します。</p> <p>重要： 接続されているその他のリソースがない空のサブネットを選択します。サブネットが空でない場合、デプロイプロセス中またはポッドの操作中に予期しない結果が発生する可能性があります。</p> <p>この場合、ゲートウェイの VNet とポッドの VNet がピアリングされます。ベスト プラクティスは、サブネットを事前に作成し、ここで CIDR エントリを使用しないことです。ポッドの VNet またはサブスクリプションとは別の専用の VNet またはサブスクリプションを使用して外部 Unified Access Gateway 構成でデプロイする場合の前提条件を参照してください。</p> <ul style="list-style-type: none"> ■ 管理サブネット - ゲートウェイの管理サブネットに使用するサブネットを指定します。少なくとも /27 の CIDR が必要です。このサブネットにはサービス エンドポイントとして Microsoft.SQL サービスが構成されている必要があります。 ■ バックエンド サブネット - ゲートウェイのバックエンド サブネットに使用するサブネットを指定します。少なくとも /27 の CIDR が必要です。 ■ フロントエンド サブネット - Unified Access Gateway インスタンスをゲートウェイの Microsoft Azure パブリック ロード バランサに接続するように構成されるフロントエンド サブネットのサブネットを指定します。

2 (オプション) [外部ゲートウェイ] セクションで、外部ゲートウェイの 2 要素認証をオプションで設定します。
[第1世代テナント - ポッドのための 2 要素認証機能の指定](#) の手順を完了させます。

3 (オプション) [デプロイ] セクションで、トグルを使用して、必要に応じてデプロイヤが外部ゲートウェイ構成のリソースを展開する既存のリソース グループを選択します。

このトグルは、ウィザードの最初のステップで外部ゲートウェイに別のサブスクリプションを使用するように指定した場合に表示されます。トグルを有効にすると、リソース グループを検索して選択するフィールドが表示されます。

4 [内部ゲートウェイ] セクションで、内部ゲートウェイ構成が必要な場合は、[内部ゲートウェイを有効にしますか?] トグルをオンにして、表示されるフィールドに入力します。

オプション	説明
[内部ゲートウェイを有効にしますか?]	ポッドに内部ゲートウェイ構成があるかどうかを制御します。内部構成は、企業のネットワーク内に存在するユーザーが HTML Access (Blast) でデスクトップおよびアプリケーションに接続するときに信頼されたアクセスを提供します。ポッドには、このアクセスを提供する Azure ロード バランサー リソースと Unified Access Gateway インスタンスが含まれています。デフォルトでは、このゲートウェイのロード バランシング タイプはプライベートです。ロード バランサーは、プライベート IP アドレスで構成されます。
[FQDN]	<p>サービスへのアクセスでエンド ユーザーが使用する完全修飾ドメイン名 (FQDN) を入力します (例: ourOrg.example.com)。このドメイン名を所有し、その FQDN を検証可能な PEM 形式の証明書を取得する必要があります。</p> <p>重要: この FQDN には、アンダー スコアを含めることはできません。このリリースでは、FQDN にアンダー スコアが含まれていると、Unified Access Gateway インスタンスへの接続が失敗します。</p>
[DNS アドレス]	<p>オプションで、Unified Access Gateway が名前解決に使用できる追加の DNS サーバのアドレスを、カンマ区切りで入力します。</p> <p>Unified Access Gateway インスタンスのデプロイ先となる VNet トポロジの外部にある 2 要素認証サーバで 2 要素認証を使用するようにこの内部 Unified Access Gateway 構成を構成する場合は、その認証サーバのホスト名を解決できる DNS サーバのアドレスを指定します。たとえば、2 要素認証サーバがオンプレミスにある場合は、その認証サーバの名前を解決できる DNS サーバのアドレスを入力します。</p> <p>すべてのデプロイの前提条件で説明されているように、Horizon Cloud on Microsoft Azure のデプロイに使用される VNet トポロジは、Unified Access Gateway インスタンスのデプロイ中に、また、その進行中の操作のために、外部の名前解決を提供する DNS サーバと通信する必要があります。</p> <p>デフォルトでは、インスタンスがデプロイされる VNet で構成されている DNS サーバが使用されます。</p> <p>[DNS アドレス] にアドレスを指定すると、デプロイされた Unified Access Gateway インスタンスは、VNet の構成の DNS サーバ情報に加えてこれらのアドレスを使用します。</p>
[ルート]	<p>オプションで、デプロイした Unified Access Gateway インスタンスが、エンド ユーザー アクセス用のネットワークのルーティングを解決するために使用する、追加のゲートウェイへのカスタム ルートを指定します。指定したルートは、Unified Access Gateway が 2 要素認証サーバとの通信などにネットワーク ルーティングを解決できるようにするために使用されます。</p> <p>このポッドをオンプレミスの認証サーバで 2 要素認証を使用するように構成する場合は、Unified Access Gateway インスタンスがそのサーバに接続するための正しいルートを入力する必要があります。たとえば、オンプレミスの認証サーバがその IP アドレスとして 10.10.60.20 を使用している場合、10.10.60.0/24 とデフォルト ルートのゲートウェイ アドレスをカスタム ルートとして入力することになります。この環境で使用している Express ルートまたは VPN 構成からデフォルト ルートのゲートウェイ アドレスを取得します。</p> <p>形式 ipv4-network-address/bits ipv4-gateway-address で、カンマ区切りリストとしてカスタム ルートを指定します (例: 192.168.1.0/24 192.168.0.1, 192.168.2.0/24 192.168.0.2)。</p>
[ポッドの NTP サーバの継承]	<p>このトグルはデフォルトで有効になっており、Unified Access Gateway インスタンスは、ポッド マネージャ インスタンスに指定されているのと同じ NTP サーバを使用します。このトグルを有効にしておくことを強くお勧めします。</p> <p>ポッド マネージャ インスタンス、Unified Access Gateway インスタンス、および Active Directory サーバに同じ NTP サーバを使用することがベスト プラクティスです。タイム スキューは、これらのインスタンスが異なる NTP サーバを使用する場合に発生する可能性があります。このようなタイム スキューにより、後でゲートウェイがデスクトップおよびアプリケーションに対してエンド ユーザー セッションを認証しようとしたときに、エラーが発生する可能性があります。</p>

オプション	説明
[仮想マシン モデル]	<p>Unified Access Gateway インスタンスに使用するモデルを選択します。このポッドに指定した Microsoft Azure サブスクリプションが、選択したモデルの 2 台の仮想マシンのキャパシティを確実に満たす必要があります。</p> <p>重要： 現在のサービス リリースでは、サブスクリプション内でゲートウェイ構成がデプロイされた後、これらのインスタンスで使用される仮想マシン モデルを簡単に変更することはできません。デプロイ後に仮想マシン モデルを変更するには、ゲートウェイ構成を削除して再デプロイする必要があります。ポッドあたりのセッション数が 2,000 にまで拡大することが想定される環境では、F8s_v2 を使用します。VMware Horizon Cloud Service on Microsoft Azure サービスの制限で説明したように、A4_v2 仮想マシン モデルが十分に機能するのは、ポッド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 (概念実証) 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。</p>
[証明書]	<p>Microsoft Azure で実行中の Unified Access Gateway インスタンスへの接続をクライアントが信頼できるようにするために、Unified Access Gateway で使用される PEM 形式の証明書をアップロードします。証明書は、入力した FQDN に基づいたものにして、信頼されている認証局 (CA) によって署名されている必要があります。PEM ファイルに、SSL 証明書の中間証明書、ルート CA 証明書、プライベート キーを含む、完全な証明書チェーンが含まれている必要があります。</p>
[Blast Extreme TCP ポート]	<p>Unified Access Gateway 構成内の Blast Extreme TCP 設定で使用する TCP ポートを選択します。この設定は、クライアントから送信されるデータ トラフィックに対し Unified Access Gateway 上の Blast Secure Gateway 経由の Blast Extreme に関連しています。ポート 8443 は、より効率的で、パフォーマンスが向上し、Unified Access Gateway インスタンスでのリソース使用率が低いため、推奨されます。このような理由により、ウィザードのデフォルト値は 8443 です。もう 1 つの選択肢である 443 は、効率が低く、パフォーマンスが低下して、インスタンスで CPU の輻輳が発生し、エンドユーザー クライアントでトラフィックの遅延が見られる可能性があります。443 の選択肢は、組織でクライアント側の制限が設定されている場合 (組織で 443 送信のみが許可されているなど) にのみ使用する必要があります。</p> <p>注： Blast Extreme に使用される UDP ポートは、この設定の影響を受けず、常に UDP 8443 です。</p>
[暗号スイート]	<p>ほとんどの場合、デフォルト設定で十分ですが、Unified Access Gateway には、クライアントと Unified Access Gateway アプライアンス間の通信の暗号化に使用される暗号化アルゴリズムを指定するためのこの機能が用意されています。</p> <p>画面上のリストから少なくとも 1 つの暗号スイートを選択する必要があります。画面上のリストには、Horizon Cloud on Microsoft Azure 環境で許可されている暗号スイートが表示されます。</p>

- 5 (オプション) [内部ゲートウェイ] セクションで、内部 Unified Access Gateway の 2 要素認証をオプションで設定します。

第1世代テナント - ポッドのための 2 要素認証機能の指定 の手順を完了させます。

- 6 (オプション) [Azure リソース タグ] セクションで、必要に応じて、ポッド用に構成したすべての内部および外部の Unified Access Gateway インスタンスを含むリソース グループにカスタム タグを追加します。

オプション	説明
[ポッド タグの継承]	<p>設定したすべての Unified Access Gateway インスタンスを含むリソース グループに、ポッドのリソース タグを追加するには、このトグルを切り替えます。各リソース グループは、ポッドのセットアップ ウィザードの手順で定義したリソース タグを受け取ります。</p> <p>このトグルをオフにして、Unified Access Gateway インスタンスの新しいリソース タグを定義します。</p>
[Azure リソース タグ]	<p>この設定は、[ポッド タグの継承] トグルをオフに切り替えると表示されます。この設定を使用して、Unified Access Gateway インスタンスを含むリソース グループに、ポッドのリソース タグを追加するには、このトグルを切り替えます。</p> <p>最初のタグを作成するには、[名前] と [値] のフィールドに情報を入力します。追加のタグを作成するには、[[+]] をクリックし、既存のフィールドの下に表示される [名前] と [値] のフィールドに情報を入力します。</p> <ul style="list-style-type: none"> ■ 最大 10 個のタグを作成できます。 ■ タグの名前は 512 文字に制限され、タグの値は 256 文字に制限されます。ストレージ アカウントの場合、タグの名前は 128 文字に制限され、タグの値は 256 文字に制限されます。 ■ タグの名前には < > * & \ ? / の文字を含めることはできません。 ■ タグの名前に大文字と小文字を区別しない文字列 ([azure]、[windows]、[microsoft]) は使用できません。 ■ タグ名とタグ値には、ASCII 文字のみを含めることができます。標準の 128 文字 ASCII セット (拡張 ASCII または拡張 ASCII 文字とも呼ばれる) 以外の空白および文字は使用できません。

結果

選択したオプションに関連付けられている必要な情報を提供した場合、[検証と続行] をクリックしてウィザードの最後の手順まで続行することができます。第 1 世代テナント - 検証と続行、およびポッドのデプロイ プロセスの開始を参照してください。

第 1 世代テナント - ポッドのための 2 要素認証機能の指定

Unified Access Gateway 構成を指定するためのポッドのデプロイ ウィザードの手順で、エンド ユーザーがこれらのゲートウェイ構成を介してデスクトップおよびアプリケーションにアクセスする際の 2 要素認証の使用を指定することもできます。

重要: この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。KB-92424 で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

The screenshot shows a wizard window titled "Add Microsoft Azure Capacity". On the left, a navigation pane lists four steps: 1. Subscription, 2. Pod Setup, 3. Gateway Settings (highlighted), and 4. Summary. The main content area is titled "Two-Factor Authentication" and contains the following settings:

- Enable two-factor authentication:** A toggle switch is turned on.
- Two-factor Authentication Type:** A dropdown menu is set to "Radius".
- Two-factor Authentication Configuration:** A dropdown menu is set to "New Radius".
- Configuration Name:** An empty text input field.

Below these settings, a "Properties" section is partially visible.

ゲートウェイ構成のためにウィザードで 2 要素認証の詳細が指定されている場合、ポッドのデプロイ プロセス中にポッド デプロイヤーが、指定した 2 要素認証の詳細を使用してゲートウェイ構成の対応するデプロイ済みの Unified Access Gateway アプライアンスを構成します。

Unified Access Gateway のドキュメントに記載されているように、2 要素認証のために Unified Access Gateway アプライアンスが構成されている場合、Unified Access Gateway アプライアンスは、指定した 2 要素認証ポリシーに従って受信ユーザー セッションを認証します。Unified Access Gateway が指定された認証ポリシーに従ってユーザー セッションを認証した後、Unified Access Gateway はデスクトップまたはアプリケーションの起動を求めるエンド ユーザーのクライアント要求をデプロイされたポッド マネージャに転送し、クライアントと使用可能なデスクトップまたはアプリケーション間の接続セッションを確立します。

重要： ポッドがデプロイされた後、2 要素認証を使用するようにテナントの Universal Broker 設定を構成し、外部ゲートウェイ構成と内部ゲートウェイ構成の両方を使用してポッドをデプロイした場合、Universal Broker が外部エンド ユーザーと内部エンド ユーザーを区別できるように、デプロイ後の追加の手順が必要になる場合があります。これは、Universal Broker に指定された 2 要素認証設定を適切に適用するために必要です。詳細については、[Universal Broker 環境で 2 要素認証を実装する際のベスト プラクティスを参照してください](#)。

前提条件

第1世代テナント - 第1世代のポッド デプロイ ウィザードを実行するための前提条件に記載されている前提条件を満たしていることを確認します。

2 要素認証の詳細を入力する外部または内部 Unified Access Gateway 構成で、[第1世代テナント - Horizon Cloud ポッドのゲートウェイ構成の指定](#)に記載されているとおりに、ウィザードにおける Unified Access Gateway 構成用のフィールドの指定が完了していることを確認します。オンプレミス認証サーバに対して 2 要素認証を構成するときに、Unified Access Gateway インスタンスがそのオンプレミス サーバにルーティングを解決できるようにするために次のフィールドにも情報を提供します。

オプション	説明
[DNS アドレス]	オンプレミス認証サーバの名前を解決できる DNS サーバの 1 つ以上のアドレスを指定します。
[ルート]	<p>ポッドの Unified Access Gateway インスタンスがネットワークのルーティングをオンプレミス認証サーバに解決できるようにする、1 つ以上のカスタム ルートを指定します。</p> <p>たとえば、オンプレミスの RADIUS サーバがその IP アドレスとして 10.10.60.20 を使用している場合、10.10.60.0/24 とデフォルト ルートのゲートウェイ アドレスをカスタム ルートとして使用することになります。この環境で使用している Express ルートまたは VPN 構成からデフォルト ルートのゲートウェイ アドレスを取得します。</p> <p>形式 <code>ipv4-network-address/bits ipv4-gateway-address</code> で、カンマ区切りリストとしてカスタム ルートを指定します (例: 192.168.1.0/24 192.168.0.1, 192.168.2.0/24 192.168.0.2)。</p>

次の情報が、ポッド デプロイ ウィザードの適切なフィールドに指定できるように、認証サーバの構成で使用されていることを確認します。RADIUS 認証サーバを使用していて、プライマリおよびセカンダリ サーバの両方がある場合は、それぞれの情報を取得します。

RADIUS

プライマリおよび補助 RADIUS サーバの両方の設定を構成している場合は、それぞれの情報を取得します。

- 認証サーバの IP アドレスまたは DNS 名
- 認証サーバのプロトコル メッセージで暗号化および復号化のために使用される共有シークレット
- 認証ポート番号。通常 RADIUS の場合は 1812/UDP。
- 認証プロトコルのタイプ。認証タイプには、PAP (パスワード認証プロトコル)、CHAP (チャレンジ ハンドシェイク認証プロトコル)、MSCHAP1 および MSCHAP2 (Microsoft チャレンジ ハンドシェイク認証プロトコル、バージョン 1 および 2) があります。

注： RADIUS ベンダーの推奨する認証プロトコルについては、RADIUS ベンダーのドキュメントを確認し、指定したプロトコルタイプに従ってください。RADIUS の 2 要素認証をサポートするポッドの機能は、Unified Access Gateway インスタンスによって提供され、Unified Access Gateway が PAP、CHAP、MSCHAP1、MSCHAP2 をサポートします。PAP のセキュリティは、通常 MSCHAP2 のものよりも低くなっています。また PAP は MSCHAP2 よりシンプルなプロトコルです。結果として、RADIUS ベンダーのほとんどはよりシンプルな PAP プロトコルと互換性がありますが、一部の RADIUS ベンダーはよりセキュリティの高い MSCHAP2 との互換性を有していません。

RSA SecurID

注： RSA SecurID タイプは、マニフェスト 3139.x 以降を実行している Horizon Cloud on Microsoft Azure デプロイでサポートされます。2022 年 3 月中旬以降の [ポッドの追加] ウィザードと [ポッドの編集] ウィザードでは RSA SecurID タイプを指定するユーザー インターフェイス オプションが表示され、選択できるようになります。

- RSA SecurID Authentication Manager サーバのアクセス キー。
- RSA SecurID 通信ポート番号。通常は 5555 で、RSA SecurID 認証 API に対する RSA Authentication Manager システム設定で設定されています。
- RSA SecurID Authentication Manager サーバのホスト名。

- RSA SecurID Authentication Manager サーバの IP アドレス。
- RSA SecurID Authentication Manager サーバまたはそのロード バランサ サーバに自己署名証明書がある場合は、[ポッドの追加] ウィザードで CA 証明書を指定する必要があります。証明書は PEM 形式である必要があります（ファイル タイプ .cer、.cert、または.pem）。

手順

- 1 [2 要素認証を有効にする] トグルをオンに切り替えます。

トグルが有効になっていると、ウィザードに追加の構成フィールドが表示されます。すべてのフィールドにアクセスするには、スクロール バーを使用します。

次のスクリーンショットは、[外部 UAG] セクションのトグルをオンに切り替えた後に表示される内容の例です。

- 2 2 要素認証タイプとして、[Radius] または [RSA SecurID] を選択します。

現在、サポートされている使用可能なタイプは RADIUS と RSA SecurID です。

タイプを選択すると、[2 要素認証構成] メニューに、選択したタイプの構成を追加していることが自動的に反映されます。たとえば、[RSA SecurID] タイプを選択した場合、[2 要素認証構成] メニューには [新規の RSA SecurID] が表示されます。

- 3 [構成名] フィールドで、この構成の識別名を入力します。

- 4 [プロパティ] セクションで、アクセスの認証に使用するログイン画面でのエンド ユーザーの操作に関連する詳細を指定します。

ウィザードには、Horizon Cloud on Microsoft Azure デプロイがゲートウェイ構成での使用をサポートする構成に基づいてフィールドが表示されます。フィールドは、選択した 2 要素認証タイプによって異なります。選択したタイプ（RADIUS または RSA SecurID）に対応する以下の表を参照してください。

RADIUS

フィールドに入力するときに、プライマリ認証サーバの詳細を指定する必要があります。セカンダリ認証サーバがある場合は、[補助サーバ] トグルを有効にして、そのサーバの詳細も指定します。

オプション	説明
[表示名]	このフィールドは空白のままにできます。このフィールドはウィザードに表示されますが、Unified Access Gateway 構成の内部名のみを設定します。この名前は Horizon クライアントによって使用されません。
[表示に関するヒント]	<p>必要に応じて、ユーザーに RADIUS ユーザー名とパスワードの入力を要求するときにエンドユーザー クライアントのログイン画面に表示されるメッセージに、エンドユーザーに対して表示されるテキスト文字列を入力します。指定されたヒントは、Enter your <i>DisplayHint</i> user name and passcode としてエンドユーザーに表示されます。ここで、<i>DisplayHint</i> はこのフィールドで指定するテキストです。</p> <p>このヒントを参考にして、ユーザーは正しい RADIUS パスコードを入力することができます。たとえば、Example Company user name and domain password below のようなフレーズを指定すると、Enter your Example Company user name and domain password below for user name and passcode というプロンプトがエンドユーザーに表示されます。</p>
[名前 ID のサフィックス]	この設定は、ポッドがシングル サインオンのために TrueSSO を使用するよう構成されている、SAML シナリオで使用されます。オプションとして、ポッド マネージャへの要求で送信される SAML アサーション ユーザー名の後に追加される文字列を指定します。たとえば、ユーザー名が user1 としてログイン画面に入力され、@example.com の名前 ID のサフィックスがここで指定された場合、user1@example.com の SAML アサーション ユーザー名が要求で送信されます。
[反復回数]	この RADIUS システムを使用してログインを試行する場合に、ユーザーに対して許可される認証の失敗試行の最大数を入力します。
[ユーザー名を維持]	<p>このトグルを有効にすると、クライアント、Unified Access Gateway インスタンス、および RADIUS サービス間で発生する認証フローの実行中に、ユーザーの Active Directory ユーザー名が維持されます。有効になっている場合：</p> <ul style="list-style-type: none"> ■ ユーザーは、Active Directory 認証の場合と同じユーザー名認証情報を RADIUS でも利用できる必要があります。 ■ ユーザーは、ログイン画面でユーザー名を変更することができません。 <p>このトグルがオフに切り替わると、ユーザーはログイン画面で別のユーザー名を入力することができます。</p> <p>注： [ユーザー名を維持] の有効化と Horizon Cloud のドメイン セキュリティ設定との関係については、[全般設定] ページでのドメイン セキュリティ設定トピックを参照してください。</p>
[ホスト名/IP アドレス]	認証サーバの DNS 名または IP アドレスを入力します。
[共有シークレット]	認証サーバと通信するため、シークレットを入力します。この値は、サーバで構成されている値と同じである必要があります。
[認証ポート]	認証トラフィックを送受信するために認証サーバで構成されている UDP ポートを指定します。デフォルトは 1812 です。
[アカウント ポート]	オプションとして、アカウントングトラフィックを送受信するために認証サーバで構成されている UDP ポートを指定します。デフォルトは 1813 です。
[メカニズム]	指定した認証サーバでサポートされている、デプロイされたポッドが使用する認証プロトコルを選択します。
[サーバ タイムアウト]	ポッドが認証サーバからの応答を待機する秒数を指定します。この秒数が経過した後、サーバが応答しない場合は再試行が送信されます。
[最大再試行回数]	ポッドが認証サーバへの失敗した要求を再試行する最大回数を指定します。

オプション	説明
[レルムのプリフィックス]	オプションとして、名前が認証サーバに送信されるときに、システムによってユーザー名の先頭に付加される文字列を指定します。ユーザー アカウントの場所はレルムと呼ばれます。 たとえば、ユーザー名が user1 としてログイン画面に入力され、DOMAIN-A\ のレルムのプリフィックスがここで指定された場合、システムは認証サーバに DOMAIN-A\user1 を送信します。レルムのプリフィックスを指定しないと、入力したユーザー名だけが送信されます。
[レルムのサフィックス]	オプションとして、名前が認証サーバに送信されるときに、システムによってユーザー名の後に追加される文字列を指定します。たとえば、ユーザー名が user1 としてログイン画面に入力され、@example.com のレルムのサフィックスがここで指定された場合、システムは認証サーバに user1@example.com を送信します。

RSA SecurID

オプション	説明
[アクセス キー]	システムの RSA SecurID 認証 API 設定で取得した RSA SecurID システムのアクセス キーを入力します。
[サーバ ポート]	通信ポートに対するシステムの RSA SecurID 認証 API 設定で構成した値を指定します。通常はデフォルトで 5555 です。
[サーバ ホスト名]	認証サーバの DNS 名を入力します。
[サーバ IP アドレス]	認証サーバの IP アドレスを入力します。
[反復回数]	ユーザーが 1 時間ロックアウトされるまでに許可される認証試行の最大失敗回数を入力します。デフォルトは、5 回です。
[CA 証明書]	この項目は、RSA SecurID Authentication Manager サーバまたはそのロード バランサが自己署名証明書を使用する場合に必須です。この場合は、CA 証明書をコピーしてこのフィールドに貼り付けます。このページで説明したように、証明書情報は PEM 形式で指定する必要があります。 サーバにパブリック認証局 (CA) によって署名された証明書がある場合、このフィールドはオプションです。
[認証タイムアウト]	タイムアウトになるまでに、認証の試行を Unified Access Gateway インスタンスと RSA SecurID 認証サーバの間で有効にする秒数を指定します。デフォルト値は 180 秒です。

第1世代テナント - 検証と続行、およびポッドのデプロイ プロセスの開始

[検証と続行] をクリックした後、指定した値がシステムによって検証されます。すべてが検証されると、ウィザードに確認のための情報の概要が表示されます。次にデプロイ プロセスを開始します。

重要: この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

手順

- 1 [検証と続行] をクリックします。

次のような指定した値がシステムによって検証されます。

- これから作成されるサブネットのために指定したアドレス範囲が有効で、サブスクリプション内で選択したリージョンの他のアドレスと重複していないか。
- サブスクリプションのクォータに、ポッドを構築するための十分な仮想マシン (VM) とコアがあるか。

- アップロードされた証明書ファイルは正しい PEM 形式か。
- 既存の管理サブネットを使用することを選択した場合、そのサブネットで Microsoft.Sql サービス エンドポイントが有効になっていますか。

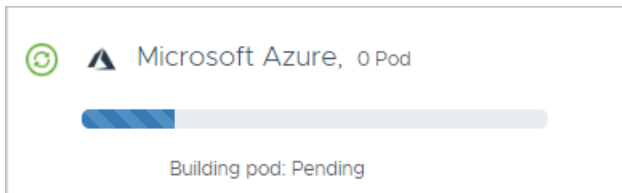
重要： 2019 年 9 月のサービス リリース以降、ポッドの Microsoft Azure PostgreSQL データベースの使用をサポートするために、新しいポッドのデプロイでは管理サブネットで Microsoft.Sql サービス エンドポイントが有効になっている必要があります。管理サブネットでエンドポイントを有効にする必要があることを示す検証エラーが表示された場合は、Microsoft Azure ポータルにログインし、サブネットで Microsoft.Sql サービス エンドポイントを有効にする必要があります。その後、ウィザードを再送信してポッドをデプロイできます。エンドポイントを有効にする方法の詳細については、[第1世代テナント - ポッドのデプロイの前に、Microsoft Azure の VNet で Horizon Cloud ポッドに必要なサブネットを作成する](#)を参照してください。

すべてが検証されると、[サマリ] ページが表示されます。

ネットワーク アドレスの重複に関するエラー メッセージが表示される場合は、サブスクリプションに同じ値を使用している既存のサブネットがあるかどうかを確認します。

- 2 ウィザードの最終手順で、概要情報を確認して、[送信] をクリックします。

Microsoft Azure 環境へのポッドのデプロイを開始します。



結果

Microsoft Azure Cloud と Horizon Cloud 制御プレーン間のネットワーク トラフィックによっては、デプロイに 30 ~ 45 分かかることがあります。

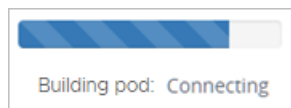
ポッドが正常にデプロイされるまで、進捗状況のアイコンがコンソールの [はじめに] 画面に表示されます。進捗状況を確認するときに、ブラウザ画面の更新が必要になる場合があります。ブラウザ ベースのユーザー インターフェイスは、約 30 分後にタイムアウトして、ログインし直すよう要求することができます。

重要： Microsoft Azure China クラウドにポッドをデプロイする場合、デプロイのプロセス全体が完了するまでに最大で 7 時間かかることがあります。このプロセスは、[第 1 世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名](#) ページに記載されているように、デプロイヤーがアクセスする必要があるホスト名へのトラフィックが遅くなる可能性がある、地理的なネットワークの問題の影響を受けます。

20 分後にポッドが Pending から Downloading の状態に変化せず、またデプロイ先が Microsoft Azure China ではない場合、システムはポッドを自動的に Error 状態に設定します。また、ポッドをクラウド サービスに接続できないため、Microsoft Azure 環境のネットワーク接続状態を確認するように促すメッセージが表示されます。

ポッドが Error 状態であることが表示される場合、環境のネットワーク構成またはファイアウォールが、[第 1 世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名](#) ページに記載されている 1 つ以上の必須ロケーションへのアクセスを拒否していることが原因であると思われます。たとえば、VNet の設定済み DNS が内部名または外部名を解決していない、必要なアウトバウンド ポートが開いていない、またはファイアウォールによってブロックされている可能性があります。*.azure.com ホスト名への接続が一時的に失われることがあります。いくつかのテストを実行し、ポッドの要件に対して環境ネットワークが適切に構成されているかどうかを検証することができます。[ポッドのデプロイまたは初めてのドメイン バインドで問題が発生した場合のトラブルシューティング](#)で始まるページのコンテンツを参照してください。

ポッドのデプロイ プロセス全体を通して、[はじめに] ページの [キャパシティ] セクションには、プロセスの現在のステージ（保留中、ダウンロード中、構築中、接続中など）が示されます。



次の表は、ポッドを構築するステージについての、およその期間の例をいくつか示しています。

重要： デプロイの進行状況で発生する実際の期間は、その時点で存在するネットワーク遅延によって異なります。

ステージ	期間の例
保留中	1 分または 2 分
ダウンロード中	1 分または 2 分
構築中	20 分
接続中	10 分

ポッドが正常にデプロイされた場合：

- Horizon Cloud が、対応する Horizon Cloud 顧客アカウント レコードで識別されるアカウント所有者に通知 E メールを送信します。この E メールには、ポッドのオンボーディングが完了したことが記載されています。
- [はじめに] 画面に緑色のチェックマークが表示されます。



この時点では、Active Directory ドメインがポッドにまだ登録されていないため、[管理] メニューで [ポッドを削除] オプションを使用できます。何らかの理由でデプロイ プロセスが失敗する場合、または使用した値が好ましくないため Active Directory ドメインを登録する前に再びやり直したい場合、[管理] - [ポッドを削除] の順にクリックしてデプロイされたアーティファクトを削除することができます。ポッドが正常に削除されたことが画面に示されたら、[管理] - [ポッドを追加] の順に再度クリックしてプロセスを再開することができます。次のスクリーンショットは、[管理] - [ポッドを削除] オプションの場所を示しています。



ネットワーク遅延のため、この時点でポッドを削除することを選ぶと、すべてポッド関連のアーティファクトが完全に Microsoft Azure 環境から削除される前に、[はじめに] ページでポッドが完全に削除されたことが示される可能性があります。新しいポッドを削除した後、ポッドのデプロイ ウィザードを再び実行する前に、次の手順を行います。

- 1 Horizon Cloud ユーザー インターフェイスからログアウトします。
- 2 Microsoft Azure ポータルにログインします。
- 3 作成した VNet に移動します。
- 4 デプロイヤを使用してポッドのサブネットを自動作成した場合は、ポッドにより作成されたサブネットがないこと、およびそのポッドのサブネットに対して指定したアドレス範囲が VNet のアドレス空間から削除されていることを確認してください。

次に、Horizon Cloud にログインし直して、ポッドのデプロイ ウィザードを再び実行します。

次のステップ

[はじめに] 画面の [全般的なセットアップ] を展開し、Active Directory ドメインの登録に必要な作業を完了します。次に必要な作業は Active Directory の登録です。ドメインを登録し、ドメイン グループのスーパー管理者ロールを設定すると、システムではすべてのコンソールにアクセスできるようになります。続いて、コンソールでこのポッドの管理を続行します。『Horizon Cloud 管理ガイド』の [はじめに](#) を参照してください。Active Directory ドメインを登録したら、[はじめに] ウィザードに従って、次に完了するタスクを確認します。

指定したゲートウェイのタイプに応じて、DNS サーバに適切な CNAME レコードを設定する必要があります。[DNS サーバでマッピングする Horizon Cloud ポッドのゲートウェイのロード バランサ情報の取得方法](#)に記載された CNAME の情報を参照してください。

外部および内部ゲートウェイ構成の両方に同じ FQDN を使用する場合は、ポッドのデプロイ後に、受信するエンドユーザー クライアントのトラフィックを、ゲートウェイのリソース グループ内の適切なロード バランサ リソースにルーティングするための設定を行う必要があります。目標は、インターネットからのクライアント トラフィックが外部ゲートウェイの Microsoft Azure パブリック ロード バランサにルーティングされ、イントラネットからのクラ

クライアント トラフィックが内部ゲートウェイの Microsoft Azure 内部ロード バランサにルーティングされるようにルーティングを設定することです。両方のゲートウェイで同じ FQDN を使用する場合、スプリット DNS (スプリット Domain Name System) を構成して、エンド ユーザー クライアントの DNS クエリのオリジン ネットワークに応じて、外部ゲートウェイまたは内部ゲートウェイのいずれかにゲートウェイ アドレスを解決します。

ポッドのゲートウェイ構成に 2 要素認証を指定した場合は、次のタスクを実行する必要があります。

- ポッドの外部ゲートウェイに 2 要素認証が構成され、ゲートウェイの Unified Access Gateway インスタンスがデプロイされているのと同じ VNet トポロジ内で 2 要素認証サーバにアクセスできない場合は、外部ゲートウェイのロード バランサの IP アドレスからの通信を許可するようにその 2 要素認証サーバを構成します。

このシナリオでは、ゲートウェイ展開と同じ VNet トポロジ内で 2 要素認証サーバにアクセスできないため、Unified Access Gateway インスタンスは、そのロード バランサ アドレスを使用してそのサーバとの接続を試みます。その通信トラフィックを許可するには、その外部ゲートウェイのリソース グループにあるロード バランサ リソースの IP アドレスが、確実に 2 要素認証サーバの構成でクライアントまたは登録されたエージェントとして指定されているようにします。この通信を許可する方法の詳細については、お使いの 2 要素認証サーバのドキュメントを参照してください。

- 同じ VNet トポロジ内で 2 要素認証サーバにアクセスできる場合は、Microsoft Azure でのデプロイの Unified Access Gateway インスタンス用に作成された適切な NIC からの通信を許可するように 2 要素認証サーバを構成します。

ネットワーク管理者が、展開に使用される Azure VNet トポロジとそのサブネットに対する 2 要素認証サーバのネットワーク可視性を決定します。2 要素認証サーバは、ネットワーク管理者が 2 要素認証サーバにネットワークの可視性を与えたサブネットに対応する Unified Access Gateway インスタンスの NIC の IP アドレスからの通信を許可する必要があります。

Microsoft Azure のゲートウェイのリソース グループには、そのサブネットに対応する 4 つの NIC があり、そのうち 2 つが 2 個の Unified Access Gateway インスタンスに対して現在アクティブです。もう 2 つはアイドル状態で、ポッドとそのゲートウェイが更新を完了した後にアクティブになります。

実行中のポッド操作のため、および各ポッドの更新後のために、ゲートウェイと 2 要素認証サーバ間の通信トラフィックをサポートするには、これらの 4 つの NIC の IP アドレスがそのサーバ構成でクライアントまたは登録されたエージェントとして指定されていることを確認します。この通信を許可する方法の詳細については、お使いの 2 要素認証サーバのドキュメントを参照してください。

これらの IP アドレスを取得する方法については、[必要な Horizon Cloud ポッド ゲートウェイ情報での 2 要素認証システムの更新トピック](#)を参照してください。

第1世代テナント - 第1世代 Horizon Cloud ポッドのデプロイまたは初めてのドメインバインドで問題が発生した場合のトラブルシューティング

Microsoft Azure の第1世代 Horizon Cloud ポッドで使用する環境のネットワークが正しく構成されていないと、ポッドを構築するプロセスが PENDING 状態のままになる場合や、デプロイ後の Active Directory 環境へのドメインバインドのアクションが失敗する可能性があります。必要な送信ポートを開くことができないことと、DNS が内部アドレスと外部アドレスの両方を解決できないことの 2 つが、最も一般的なネットワーク関連の原因で

す。ここで説明するトラブルシューティングの手順を実行することで、必要な送信ポートが開いていることと、DNS が内部アドレスと外部アドレスの両方を解決できることを確認するためのテストを実行できます。

重要： この情報は、第1世代の制御プレーンで第1世代のテナント環境にアクセスできる場合にのみ適用されます。[KB-92424](#) で説明されているように、第1世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

ポッドを正常にデプロイするためのネットワーク全体の要件は、[前提条件のチェックリスト](#)に示されていて、[第1世代テナント - Microsoft Azure の Horizon Cloud ポッドに使用する VNet トポロジに必要な DNS サーバの設定](#)および[第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名に記載されています](#)。環境のネットワークがこれらの要件を満たしていない場合は、次のいずれかまたは両方の問題が発生します。

問題	一般的な原因
<ul style="list-style-type: none"> ■ [はじめに] ページにポッドが保留状態であることが示され、接続状態にならない。通常、ポッドは約 10 分間保留状態になります (Microsoft Azure China クラウドにポッドを展開する場合は例外で、さらに時間がかかります)。 ■ ポッドが正常にデプロイされた場合でも、Active Directory を登録しようとすると、ドメインバインドの手順がエラー [Unable to register Active Directory] で失敗する。 	<ul style="list-style-type: none"> ■ 必要な送信ポートが開いていないか、ファイアウォール環境によってブロックされています。必要な送信ポートが開いていない、またはファイアウォールによってブロックされている場合、ポッド ソフトウェアは Microsoft Azure クラウド環境に安全にダウンロードされず、Horizon Cloud クラウド制御プレーンに接続できません。その結果、保留状態のままになる問題が発生します。 ■ VNet DNS サーバが、内部マシン名と外部マシン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適切に構成されていません。 ■ VNet DNS サーバは DNS サーバを正しく参照していますが、DNS サーバは内部マシン名と外部マシン名の両方を解決できません。 <p>外部マシン名の DNS 解決が VNet に提供されない場合、保留状態が続く問題とドメインバインドの問題が発生する可能性があります。たとえば、DNS がドメイン コントローラの Active Directory に解決できない場合、ドメインバインドの手順は失敗します。VNet の DNS 構成の詳細については、第1世代テナント - Microsoft Azure の Horizon Cloud ポッドに使用する VNet トポロジに必要な DNS サーバの設定を参照してください。</p>

DNS 構成が内部名と外部名を解決できること、および必要な送信ポートが開いていることを確認するためのいくつかのテストを実行するには、Microsoft Azure サブスクリプションに小さなテスト用仮想マシン (VM) をデプロイし、その仮想マシンを使用してこれらのネットワーク テストを実行します。トラブルシューティング手順の概要は次のとおりです。

- 1 SSH キー ペアを作成します。
- 2 Microsoft Azure サブスクリプションにテスト用仮想マシンを作成します。
- 3 テスト用仮想マシンに接続します。
- 4 ネットワーク テストを実行します。

- 5 テストが完了したら、テスト用仮想マシンと、このトラブルシューティングを行うために Microsoft Azure 環境で作成されたすべてのテスト関連のアーティファクトを削除します。

注： テスト関連のアーティファクトを削除せず、後でポッドを削除するためにコンソールの [削除] アクションを使用すると、予期しない結果が発生する可能性があります。ポッドを削除するときに、システムはサブネットに接続されているすべてのものがポッドの ID に応じてポッド自体に属していることを確認するために、ポッドのサブネットをチェックします。追加の仮想マシン、仮想マシンのディスク、IP、またはその他のアーティファクトがポッドのサブネットに接続されているとシステムによって判断された場合は、システムがポッドをクリーンに削除することはできません。

トラブルシューティング テストの実行の詳細については、次のセクションを参照してください。

重要： これらの手動テストはすべて成功しても、オンプレミス ネットワークを介してすべてのトラフィックを送信し、認証されたトラフィックのみを通過させ、ポッド デプロイ ウィザードでプロキシを使用するための値を指定しなかった場合、ポッドのデプロイは保留状態のままになることがあります。この説明が状況に一致する場合は、[はじめに] ページからポッドを削除し、ポッド デプロイ ウィザードを再実行し、必要なプロキシ情報を指定する必要があります。

手順

1 Horizon Cloud ポッドのデプロイのトラブルシューティング - SSH キー ペアを作成する

このトラブルシューティングの一環として、テスト用 Linux 仮想マシンが Microsoft Azure サブスクリプションにデプロイされます。テスト用 Linux 仮想マシンに対して認証するには、SSH キー ペアが必要です。キー ペアはテスト用仮想マシンに SSH 接続するために使用するシステムで作成します。そのシステム上にすでにキー ペアがある場合、この手順はオプションです。

2 Microsoft Azure サブスクリプションにテスト用仮想マシンを作成する

Microsoft Azure 環境でテスト用 Linux 仮想マシン (VM) を使用して、Horizon Cloud ポッドが構成されているネットワーク接続を確認するテストを実行します。

3 SSH を使用してテスト用仮想マシンに接続する

Microsoft Azure 環境でネットワーク接続テストを実行できるように、テスト用仮想マシンに対して SSH (Secure Shell) 接続を実行します。

4 Microsoft Azure 環境でネットワークを確認するためのテストを実行する

ここでのテストを実行することで、DNS が内部アドレスと外部アドレスの両方を解決できる、および必要な送信ポートが開いている、という 2 つのネットワーク関連の領域が適切に設定されていることを確認します。これらのテストは、テスト用仮想マシンを使用して実行します。

5 テストの完了後にテスト用仮想マシンを削除する

Microsoft Azure のネットワーク構成を確認するためのテストを完了し、テスト用仮想マシンが不要になったら、Microsoft Azure 環境からその仮想マシンと関連するすべてのアーティファクトを削除する必要があります。

Horizon Cloud ポッドのデプロイのトラブルシューティング - SSH キー ペアを作成する

このトラブルシューティングの一環として、テスト用 Linux 仮想マシンが Microsoft Azure サブスクリプションにデプロイされます。テスト用 Linux 仮想マシンに対して認証するには、SSH キー ペアが必要です。キー ペアはテスト用仮想マシンに SSH 接続するために使用するシステムで作成します。そのシステム上にすでにキー ペアがある場合、この手順はオプションです。

この SSH キー ペアを作成するには、Microsoft Windows または Linux システムのいずれかを使用できます。ここでは両方のタイプのシステムでの手順を説明します。実際の状況に適した手順を選択してください。

Microsoft Windows システム上で SSH キー ペアを作成する

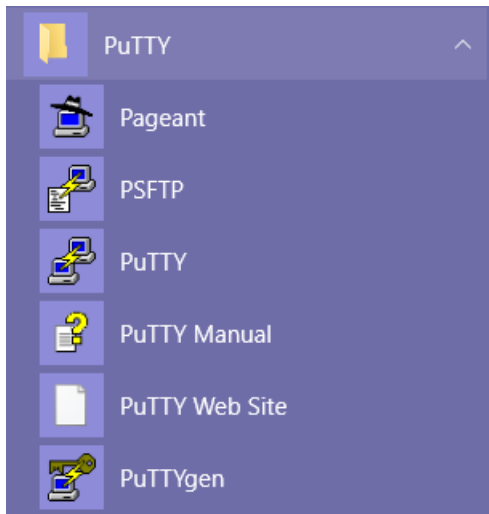
Microsoft Windows システムを使用して、Microsoft Azure サブスクリプションにデプロイするテスト用 Linux 仮想マシン に SSH 接続する場合は、以下の手順を使用します。

Microsoft Azure でテスト用仮想マシンを作成する場合、生成されたパブリック キー ファイルの内容を使用します。テスト用仮想マシンに接続するために使用する Microsoft Windows システム上に既存の SSH キー ペアがある場合は、この手順をスキップし、[Microsoft Azure サブスクリプションにテスト用仮想マシンを作成する](#)での説明に従ってテスト用仮想マシンの作成に進むことができます。

次の手順に従って、SSH キー ペアを生成し、パブリック キー ファイルの内容をコピーしてテスト用仮想マシンの作成時に使用できるようにし、プライベート キーを PuTTY Pageant ツールにロードします。Pageant は、プライベート キーをメモリに保持できる SSH 認証エージェントです。プライベート キーをメモリに保持することで、プライベート キーはその Microsoft Windows システムから SSH セッションに対して自動的に適用されるので、簡単に使用できるようになります。

前提条件

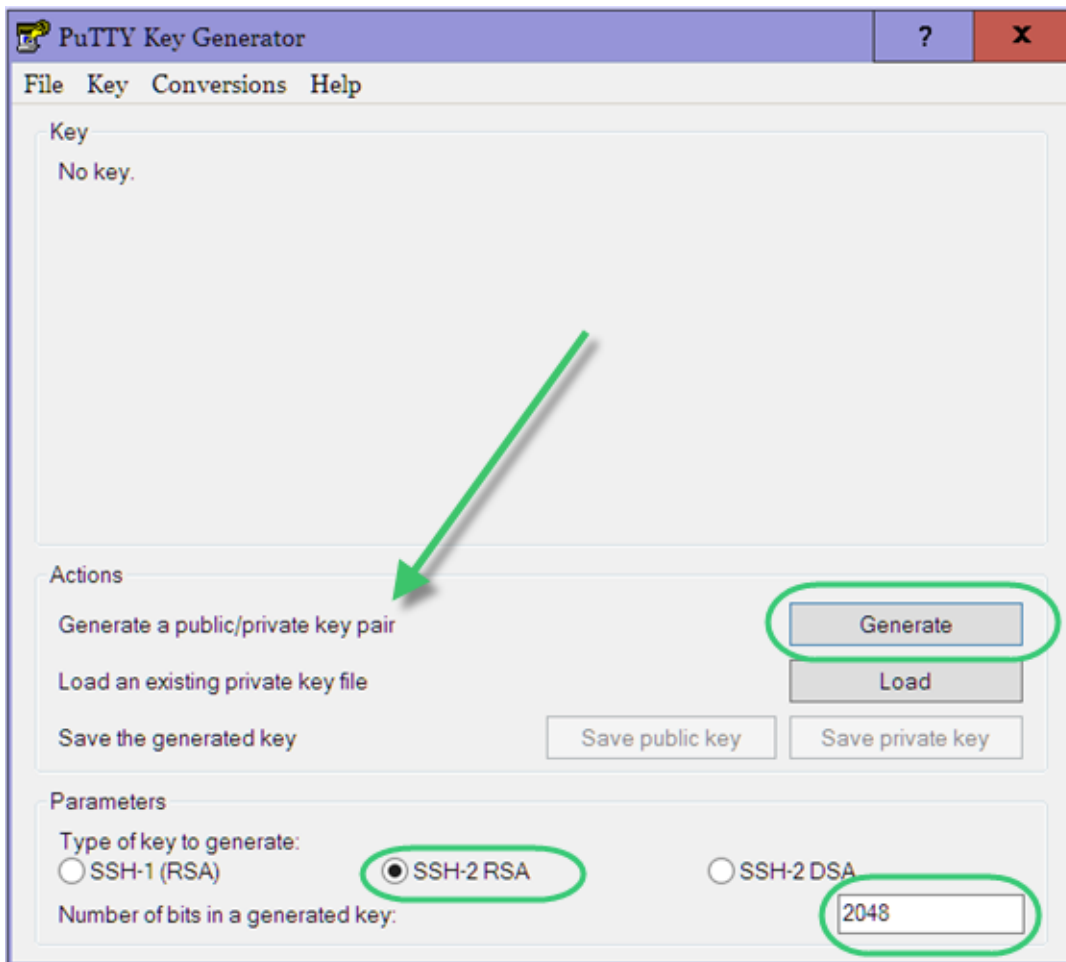
デフォルトでは、Microsoft Windows システムには、SSH キー ペア ソフトウェアがインストールされていません。使用する予定があるシステムに SSH キー ペア生成ソフトウェアがインストールされていることを確認します。任意の SSH キー ペア生成ソフトウェアを使用できます。以下の手順では、Microsoft Windows 上で PuTTY ソフトウェアを使用して SSH キー ペアを作成する方法について説明します。PuTTY ソフトウェアは、www.putty.org から取得できます。インストール後、PuTTY の一連のツールを使用できます。次のスクリーンショットは、[スタート] メニューの PuTTY ツールの例を示します。



手順

- 1 Microsoft Windows システムで、PuTTYgen (PuTTY キー ジェネレータ) を起動します。

[PuTTY キー ジェネレータ] ウィンドウが表示されます。次のスクリーンショットで強調されているように、目標は SSH-2 RSA タイプで 2048 ビットのパブリック - プライベート キー ペアを生成することです。



- 2 [SSH-2RSA] が選択され、ビット数に **2048** が設定されていることを確認し、[生成] をクリックします。ウィンドウは、進行状況バーを示す [キー] ウィンドウに変わります。
- 3 画面に表示される指示に従い、カーソルを進行状況バーの下の空白領域でランダムに動かします。PuTTY ユーザー インターフェイスで示すように、領域内でカーソルを移動すると、必要なランダム性がプロセスに追加されます。
- 4 キーのパスフレーズを入力してシステムにプライベート キーを保存し、[プライベート キーを保存] をクリックします。

注： キー パスフレーズを使用することは、オプションとしてのベスト プラクティスです。ただし、キーのパスフレーズを入力せずに [プライベート キーを保存] をクリックすると、キーのパスフレーズなしでプライベート キーを保存するかを確認するポップアップ ウィンドウが表示されます。

プライベート キーが PPK ファイルとして保存されます。[プライベート キーを保存] をクリックした後、ローカル システムのディレクトリを参照し、ファイル名を入力して、ファイルを保存することができます。

- 5 [パブリック キーを保存] ボタンを使用して、テスト用仮想マシン の作成時にパブリック キーをコピーできる場所に保存します。
- 6 PuTTY の SSH 認証エージェントである Pageant を起動します。
Windows 10 システムでは、Pageant アイコンがシステム トレイにロードされます。
- 7 プライベート キーを Pageant に追加するには、システム トレイ アイコンを右クリックし、[キーを追加] をクリックし、ファイル選択ウィンドウを使用して、保存されたプライベート キー (PPK) ファイルに移動して選択します。

注： 以前にプライベート キー ファイルを保存したときにキーのパスフレーズを指定した場合は、そのパスフレーズを入力するためのボックスが表示されます。

結果

この時点では、プライベート キーは Pageant にロードされます。アクション メニューの [キーの表示] 項目を使用して、ロードされたキーのリストのキーを表示することができます。PuTTY を使用して SSH セッションを開始すると、PuTTY は Pageant からキーを自動的に取得し、そのキーを使用して認証するので、パスフレーズを入力する必要はありません。後で、SSH セッションの実行を終了して Pageant をシャットダウンするときには、Pageant システムのトレイ アイコンの右クリックメニューから [終了] を選択します。

次のステップ

[Microsoft Azure サブスクリプションにテスト用仮想マシンを作成する](#)の手順に従って、テスト用の仮想マシンを作成します。

Linux システム上で SSH キー ペアを作成する

Linux システムを使用して、Microsoft Azure サブスクリプションにデプロイするテスト用 Linux 仮想マシン に SSH 接続する場合は、以下の手順を使用します。

Microsoft Azure でテスト用仮想マシンを作成する手順では、生成されたパブリック キー ファイルの内容を使用します。テスト用仮想マシンに接続するために使用する Linux システム上に既存の SSH キー ペアがある場合は、この手順をスキップし、「[Microsoft Azure サブスクリプションにテスト用仮想マシンを作成する](#)」での説明に従ってテスト用仮想マシンの作成に進むことができます。

前提条件

これらの手順を実行する前に、別の目的で保持しておく既存の SSH キー ペアが上書きされないことを確認してください。Linux システムでは、SSH のパブリックおよびプライベート キー ファイルは、デフォルトで Linux の `~/.ssh/id_rsa` ディレクトリに作成されます。このディレクトリに SSH キーペアが存在し、次のコマンドを実行するときに同じファイル名を使用する場合、またはコマンド内で別の場所を指定し、その場所に SSH キー ペアがすでに存在する場合は、既存の SSH キー ペアが上書きされます。

手順

- 1 Linux システムで、Bash シェルを開きます。
- 2 Bash シェルで、次のコマンドを入力します。

```
ssh-keygen -t rsa -b 2048
```

- 3 画面の指示に従い、キーを保存するファイルを入力し、パスフレーズを入力し、パスフレーズを確認します。

ここに画面の指示のサンプルを示します。ここでは、キーを保存するファイルとして `mykey` が入力されました。

```
-bash-4.1$ ssh-keygen -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/mts-cm/home/user1/.ssh/id_rsa): mykey
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

注： キー パスフレーズを使用することは、オプションのベスト プラクティスです。

プライベート キーは指定したファイルに保存され、パブリック キーは同じ名前で拡張子が `.pub` のファイルに保存されます。ファイルとして `mykey` を入力する上記の例を使用した場合、出力サンプルは次のようになります。

```
Your identification has been saved in mykey.
Your public key has been saved in mykey.pub.
```

次のステップ

[Microsoft Azure サブスクリプションにテスト用仮想マシンを作成する](#)の手順に従って、テスト用の仮想マシンを作成します。

Microsoft Azure サブスクリプションにテスト用仮想マシンを作成する

Microsoft Azure 環境でテスト用 Linux 仮想マシン (VM) を使用して、Horizon Cloud ポッドが構成されているネットワーク接続を確認するテストを実行します。

前提条件

Horizon Cloud ポッドのデプロイのトラブルシューティング - SSH キー ペアを作成するでの説明に従って作成した SSH パブリック キーを持っていることを確認します。仮想マシンの作成ウィザードでこのパブリック キーを指定し、対応するプライベート キーを持つシステムからの SSH 接続を仮想マシンが信頼するようにします。

第 1 世代 Horizon Cloud - Microsoft Azure での必要な仮想ネットワークの構成での説明に従って、仮想ネットワーク (VNet) の名前が、ポッドのデプロイで使用しているものと同じであることを確認します。

[ポッドの追加] ウィザードのオプションを使用してポッドに独自の名前付きサブネットを使用せず、代わりにサブネットの CIDR を入力した場合、ポッド デプロイヤーはポッドの管理サブネットを作成します。デプロイ プロセスが失敗した時点で、プロセスは VNet でポッドの管理サブネットをすでに作成している可能性があります。

- デプロイヤーがすでにその管理サブネットを作成している場合は、そのサブネットにテスト用仮想マシンをデプロイすることをお勧めします。VNet 上にポッドの管理サブネットが存在するかどうかを確認するには、Microsoft Azure ポータルにログインし、該当の VNet に移動してサブネットのリストを調べます。ポッド デプロイヤーがポッドのサブネットを自動的に作成した場合（ポッドに独自の名前付きサブネットを使用するオプションを使用しなかった場合）、ポッドの管理サブネットの名前のパターンは `vmw-hcs-podID-net-management` になります。ここで `podID` はポッドの UUID です。それ以外の場合、ポッドの管理サブネットは、ポッドのデプロイ用に作成したサブネットになります。
- 失敗したデプロイ プロセスで VNet 上にポッドの管理サブネットが作成されなかった場合は、VNet 上で使用可能なサブネットを選択するか、新しいサブネットを作成して、テスト用仮想マシンで使用することができます。

手順

- 1 Microsoft Azure ポータルにログインします。
- 2 ポータルで、Azure Marketplace からコンピューティング仮想マシンを作成し、その仮想マシンを Ubuntu Server LTS モデル タイプ ベースにします。

本書の執筆時点では、Ubuntu Server 20.04 LTS は Azure Marketplace から選択できました。

- 3 このテスト用 Linux 仮想マシンを作成する場合は、ウィザードのユーザー インターフェイスに従って、必要なオプションを構成します。以下に示すように、次の項目を構成してください。

オプション	説明
[サブスクリプション]	ポッドの [ポッドの追加] ウィザードで選択したサブスクリプションと一致します。
[リソース グループ]	テスト用仮想マシンに新しいリソース グループを作成することをお勧めします。画面上的プロンプトに従って、新しいリソース グループを作成します。 このテスト用仮想マシンには既存のリソース グループを使用することができますが、テストの実行が終了したときにリソース グループ全体を削除した方が、より簡単に仮想マシンおよび関連するアーティファクトを削除できるので、テスト用仮想マシンに固有のリソース グループを使用することをお勧めします。
[リージョン]	ポッドの [ポッドの追加] ウィザードで選択したサブスクリプションと一致します。
[サイズ]	ここでは検証テストを完了するために使用される一時的な仮想マシンを想定しているため、任意のサイズを選択できます。ただし、通常はサイズが小さいほど Microsoft Azure の関連コストが低くなるため、テスト用仮想マシンには 2 vCPU モデルなど小さなサイズを選択するのが一般的です。

オプション	説明
[ユーザー名]	この名前は、後で必要になるためメモしておきます。
[認証タイプ]	[SSH パブリック キー] を選択します。
[SSH パブリック キー ソース]	[既存のパブリック キーを使用する] を選択します。SSH パブリック キー フィールドがその選択とともに表示され、SSH パブリック キーを貼り付けることができます。
[SSH パブリック キー]	このフィールドには、SSH キー ペアを作成したときに作成した SSH パブリック キーを貼り付けます。貼り付けられた内容は、パブリック キーの ---- BEGIN SSH2 PUBLIC KEY ---- 行で始まり、---- END SSH2 PUBLIC KEY ---- 行で終わる必要があります。
[パブリック受信ポート]	選択した SSH (22) ポートを許可して、このテスト用仮想マシンでテストを実行できるようにします。
[仮想ネットワーク]	失敗したポッドのデプロイに使用されたのと同じ VNet を選択します。
[サブネット]	<p>ポッドをデプロイしようとしてプロセスが失敗した場合は、ポッドの管理サブネットが仮想ネットワークで作成されている可能性があります。サブネットがある場合は、このテスト用仮想マシンにそのサブネットを選択することをお勧めします。選択された仮想ネットワークに存在するサブネットに移動するには、[サブネット] をクリックします。サブネット上にマウスを移動すると、ツールチップにサブネットの完全名が表示されます。</p> <p>ポッドのデプロイ プロセスで VNet 上にポッドの管理サブネットが作成されなかった場合は、テスト用仮想マシンに使用するよう識別された VNet 上のサブネットを選択します (上記の前提条件を参照)。</p> <p>注： ポッドが正常に展開された後、ドメイン参加の問題のトラブルシューティングが発生した場合は、ドメイン参加の操作はそのデスクトップ サブネットに接続されたデスクトップイメージで 사용되는ため、管理サブネットの代わりにポッドのデスクトップ サブネットをテスト用仮想マシンのために選択することができます。</p>
[パブリック IP アドレス]	<p>この項目を選択すると、作成されたテスト用仮想マシンにはパブリック IP アドレスが割り当てられます。パブリック IP アドレスが割り当てられたテスト用仮想マシンには Wide Area Network (WAN) 経由で接続できます。</p> <p>注： パブリック IP アドレスは、ネットワーク構成によっては使用できない場合があります。パブリック IP アドレスを持つテスト用仮想マシンを作成できない場合は、ローカル システムから、[サブネット] フィールドで選択したサブネットにネットワーク接続する必要があります。あるいは、ネットワーク上の他のマシンに接続してから、テスト用仮想マシンにインバウンド接続する必要があります。</p>

- 4 ウィザードの最終手順では、重要な情報 (サブスクリプション、リージョンの場所、仮想ネットワーク、サブネット) がポッドに使用しているものと一致することを確認し、仮想マシンの作成を送信します。

SSH を使用してテスト用仮想マシンに接続する

Microsoft Azure 環境でネットワーク接続テストを実行できるように、テスト用仮想マシンに対して SSH (Secure Shell) 接続を実行します。

Microsoft Windows システムからテスト用仮想マシンに SSH 接続する

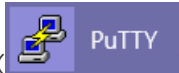
この接続は、テスト用仮想マシンの作成時に指定したパブリック キーに対応するプライベート キーを持つ Microsoft Windows システムから行います。

前提条件

テスト用仮想マシンの IP アドレスと、仮想マシンの作成時に指定したユーザー名があることを確認します。

Microsoft Windows システムでは、通常 PuTTY が使用されます。SSH セッションを開始するときに PuTTY がプライベート キーを簡単に読み込むことができるように、PuTTY を起動する前に、[Microsoft Windows システム上で SSH キー ペアを作成する](#)での説明に従って Pageant を起動し、SSH プライベート キーを Pageant キーリストに追加します。SSH プライベート キーは、テスト用仮想マシンの作成時に指定したパブリック キーと一致する必要があります。プライベート キーが Pageant に読み込まれると、PuTTY の SSH セッションはそのプライベート キーを自動的に使用します。

手順

- 1 PuTTY を起動します ()。
[PuTTY 構成] ウィンドウが開きます。
- 2 [PuTTY 構成] ウィンドウでホスト名を指定し、[SSH] を選択してから [開く] をクリックします。
[PuTTY 構成] ウィンドウの [ホスト名] フィールドに、次のパターンで文字列を入力します。

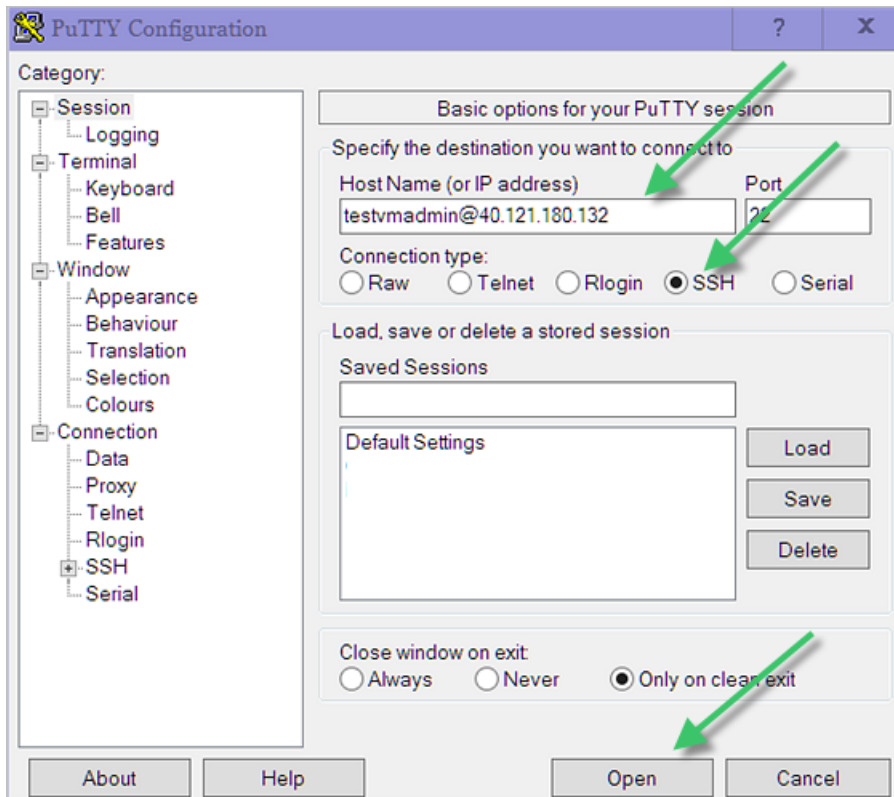
```
testvm_username@testvmip
```

テスト用仮想マシンのユーザー名と IP アドレスを、それぞれ文字列の *testvm_username* と *testvmip* に代入します。

重要： [開く] をクリックした後、初めてテスト用仮想マシンに接続するときに、サーバのホスト キーがキャッシュされていないことを示す PuTTY セキュリティ メッセージが表示され、サーバの rsa2 キー フィンガープリントが表示されます。接続を続行する場合は、[はい] をクリックしてサーバのホスト キーを PuTTY のキャッシュに追加するか、[いいえ] をクリックしてキーを PuTTY のキャッシュに追加せずに接続することができます。テスト用仮想マシンへの接続がされていない可能性がある場合は、[キャンセル] をクリックして接続を破棄し、[PuTTY 構成] ウィンドウに戻り、ホスト名の入力を確認します。

次のスクリーンショットは、このサンプルを使用したウィンドウを示します。

```
testvmadmin@40.121.180.132
```

結果

SSH 接続が確立されると、コマンドライン ウィンドウが表示されます。

次のステップ

テスト用仮想マシンに接続したら、テストを実行して Microsoft Azure 環境内のネットワーク接続をチェックできます。Microsoft Azure 環境でネットワークを確認するためのテストを実行するで説明する手順を実行します。

Linux システムからテスト用仮想マシンに SSH 接続する

この接続は、テスト用仮想マシンの作成時に指定したパブリック キーに対応するプライベート キーを持つ Linux システムから行います。

前提条件

テスト用仮想マシンの IP アドレスと、仮想マシンの作成時に指定したユーザー名があることを確認します。

手順

- 1 Bash シェルを開きます。
- 2 Bash シェルの \$ プロンプトで、次のように ssh コマンドを入力し、テスト用仮想マシンの IP アドレスとユーザー名を、それぞれコマンドの *testvmip* と *testvm_username* に代入します。

```
ssh testvm_username@testvmip
```

たとえば、[Microsoft Azure サブスクリプションにテスト用仮想マシンを作成する](#)の例にあるテスト用仮想マシンの詳細を使用すると、サンプル コマンドは次のようになります。

```
ssh testvmadmin@40.121.180.132
```

結果

SSH 接続が確立されると、次のスクリーンショットのようなコマンドライン ウィンドウが表示されます。

```
testvmadmin@HCS-testingVM: ~
Authenticating with public key "rsa-key-20180323" from agent
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-1011-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

testvmadmin@HCS-testingVM:~$
```

次のステップ

テスト用仮想マシンに接続したら、テストを実行して Microsoft Azure 環境内のネットワーク接続を確認できます。[Microsoft Azure 環境でネットワークを確認するためのテストを実行する](#)で説明する手順を実行します。

Microsoft Azure 環境でネットワークを確認するためのテストを実行する

ここでのテストを実行することで、DNS が内部アドレスと外部アドレスの両方を解決できる、および必要な送信ポートが開いている、という 2 つのネットワーク関連の領域が適切に設定されていることを確認します。これらのテストは、テスト用仮想マシンを使用して実行します。

ポッドは DNS によって内部アドレスと外部アドレスの両方を解決します。ここでの最初の 2 つのテストでは、ネットワーク環境で設定された DNS が、内部アドレスと外部アドレスの既知の FQDN を解決できるかを確認します。

重要： これらの手動テストはすべて成功しても、オンプレミス ネットワークを介してすべてのトラフィックを送信し、認証されたトラフィックのみを通過させ、ポッド デプロイ ウィザードでプロキシを使用するための値を指定しなかった場合、ポッドのデプロイは保留状態のままになることがあります。この説明が状況に一致する場合は、[はじめに] ページからポッドを削除し、ポッド デプロイ ウィザードを再実行し、必要なプロキシ情報を指定する必要があります。

前提条件

これらのテストを実行する前に、[Microsoft Azure サブスクリプションにテスト用仮想マシンを作成する](#)および[SSH を使用してテスト用仮想マシンに接続する](#)での説明に従って、Microsoft Azure サブスクリプションでテスト用仮想マシンを作成し、SSH 接続があることを確認します。

Active Directory ドメイン コントローラなど、VNet からアクセス可能であると考えられるネットワークの内部にあるサーバの IP アドレスと完全修飾ドメイン名 (FQDN) を取得します。この情報は、DNS 検証テストで使用します。

手順

- 1 `dig` コマンドを使用して Microsoft Azure の VNet の内部にある既知のドメイン名をクエリすることにより、DNS が環境内で動作し、内部 FQDN を解決できることを確認します。

SSH 接続ウィンドウで、`dig` コマンドを実行し、Active Directory ドメイン コントローラなどネットワークの内部にあることがわかっているサーバのドメイン名をクエリします。

```
dig internal-domain-name
```

ここで、*internal-domain-name* は、ネットワークの内部にあることがわかっているサーバの完全修飾ドメイン名です。

`dig` (Domain Information Groper) は、ネットワークトラブルシューティングのためのコマンドライン ツールです。内部ホスト名を使用してこのコマンドを実行した結果により、DNS 構成が内部アドレスを適切に解決できるかどうかを検証されます。DNS 構成がコマンドで使用される *internal-domain-name* を解決できる場合、コマンド出力はそのドメイン名に関連付けられた正しい IP アドレスを返します。

たとえば VNet が、DNS エントリが `skylo.local` で IP アドレスが `192.168.0.15` の Active Directory ドメイン コントローラを持つ内部 Active Directory サーバで構成されているとします。`dig skylo.local` を発行すると、VNet の DNS 構成がその内部の `skylo.local` サーバ名を解決できるかどうかチェックされます：

```
testvmadmin@HCS-testingVM:~$ dig skylo.local

; <<>> DiG 9.10.3-P4-Ubuntu <<>> skylo.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64899
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;skylo.local.                IN      A

;; ANSWER SECTION:
skylo.local.                600     IN      A      192.168.0.15

;; Query time: 1 msec
;; SERVER: 192.168.0.15#53(192.168.0.15)
```

```
;; WHEN: Mon Mar 26 20:58:01 UTC 2018
;; MSG SIZE rcvd: 56

testvmadmin@HCS-testingVM:~$
```

ANSWER SECTION が、指定したホスト名がそのホスト名に対して予測される IP アドレスに解決されたことを示している場合は、テストは成功です。

注： 場合によっては DNS が完全に信頼できるものではなく、一部の要求は正常に解決され、他の要求は失敗することがあります。コマンドの最初の発行が失敗する場合は、コマンドを 10 ~ 20 回繰り返して実行し、信頼できる応答が毎回得られるかどうかを確認します。

- 2 dig コマンドを使用して既知の外部ドメイン名をクエリすることにより、DNS が環境内で動作し、外部 FQDN を解決できることを確認します。

SSH 接続ウィンドウで、dig コマンドを発行し、vmware.com または microsoft.com などの外部の業界標準ドメイン名をクエリします。

```
dig external-domain-name
```

ここで、*external-domain-name* は、VNet の外部にある完全修飾ドメイン名です。たとえば、dig vmware.com を発行すると VNet の DNS 構成がその外部名を解決できたかどうかチェックします。

```
testvmadmin@HCS-testingVM:~$ dig vmware.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> vmware.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38655
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;vmware.com.                IN      A

;; ANSWER SECTION:
vmware.com.                 150     IN      A       107.154.105.19
vmware.com.                 150     IN      A       107.154.106.19

;; Query time: 28 msec
;; SERVER: 192.168.0.15#53(192.168.0.15)
;; WHEN: Mon Mar 26 21:14:29 UTC 2018
;; MSG SIZE rcvd: 71

testvmadmin@HCS-testingVM:~
```

上記の例では、ANSWER SECTION は外部ドメイン名 `vmware.com` が2つのIPアドレスに適切に解決されたことを示しています。

注： このテストを `azure.com` や `microsoft.com` などのさまざまな外部ドメイン名を使用して繰り返し、DNS が異なる外部名を解決できることを確認できます。

DNS テストが機能しない場合は、ネットワーク構成および DNS サーバを確認してください。DNS サーバを VNet に追加したことを確認します。

重要： DNS サーバを VNet に追加する必要がある場合、または VNet の DNS サーバ構成を変更する必要がある場合は、VNet に接続されているすべての仮想マシンを再起動して変更を反映する必要があります。VNet の DNS サーバ設定を変更した後、その VNet に接続されたすべての仮想マシンを再起動しないと、変更は VNet 上で正しく伝達されません。

- 3 netcat コマンドを使用して、必要な送信ポートが使用可能であることを確認します。

Horizon Cloud ではいくつかの送信ポートを開く必要があります。それによって、ポッド ソフトウェアを Microsoft Azure 環境に安全にダウンロードすることができ、またポッドを Horizon Cloud 制御プレーンに戻すことができます。第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名で説明するように、以下の送信 TCP ポートをポッドの管理サブネットから開く必要があります：port 80、443、および 11371。以下に示すように netcat コマンドを実行すると、それらの送信ポートが要求されるとおりに開いていることを確認できます。

SSH 接続ウィンドウで、次のコマンドを発行します（ポートごとに1つ）。

注： ポート 11371 をテストする以下のコマンドは `packages.microsoft.com` を指定してその接続をテストし、他の2つの行は Horizon Cloud 制御プレーンへの送信接続をテストします。

```
testvmadmin@HCS-testingVM:~$ netcat -v -w 3 cloud.horizon.vmware.com 80
Connection to cloud.horizon.vmware.com 80 port [tcp/http] succeeded!
testvmadmin@HCS-testingVM:~$ netcat -v -w 3 cloud.horizon.vmware.com 443
Connection to cloud.horizon.vmware.com 443 port [tcp/https] succeeded!
testvmadmin@HCS-testingVM:~$ netcat -v -w 3 packages.microsoft.com 11371
Connection to packages.microsoft.com 11371 port [tcp/hkp] succeeded!
```

ポートが正常に開くと、netcat コマンドはそのテストに対して `succeeded!` 行を返します。

netcat コマンドが失敗を返す場合は、Microsoft Azure のネットワーク接続、サブスクリプションのネットワークセキュリティグループ、および使用しているファイアウォールを確認します。第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名で説明されているように、ポッドがデプロイのために必要とする DNS、ポート、およびプロトコルの要件を、ネットワーク構成が確実に満たすようにします。

結果

上記のテストが成功した場合は、ポッドを正常にデプロイすることができます。

注： True SSO または認証サーバを使用する 2 要素認証など、ポッドで使用するオプションの機能を構成している場合は、それらの目的に応じて追加のポートが必要になることがあります。上記の送信ポートのテスト方法を使用して、それらのポートが適切に開いていることを確認することができます。

次のステップ

テストを完了したら、Microsoft Azure 環境からテスト用仮想マシンと、その仮想マシンのディスク、IP アドレス、NIC などの関連するアーティファクトのすべてを削除する必要があります。理想的には、テスト仮想マシンのリソース グループを作成してあり、単純にそのリソース グループを削除することで仮想マシンのすべてのアーティファクトを削除できることが望ましいです。[テストの完了後にテスト用仮想マシンを削除する](#) の手順に従います。

重要： Microsoft Azure 環境からすべてのテスト用仮想マシンのアーティファクトを削除しないで、仮想マシンをポッドのサブネットの 1 つに接続した場合、後でポッドの [削除] アクションを使用して Horizon Cloud 環境からポッドを削除しようとしても、システムはこれらの残りの接続されているアーティファクトのためにポッドを完全に削除できない可能性があります。デフォルトでは、[削除] アクションを使用してポッドを削除する場合に、Horizon Cloud はポッドのために作成したこれらのリソース グループおよびサブネットを削除します。Microsoft Azure は、継続して使用中であるサブネットの削除を防止します。テスト用仮想マシンのアーティファクトがポッドのサブネットに接続されている場合は、これらのサブネットは削除できず、ポッドの削除は完了しません。この状況を回避するには、ポッドを正常にデプロイした後に、テスト用仮想マシンのすべてのアーティファクトが確実に削除されるようにします。

テストの完了後にテスト用仮想マシンを削除する

Microsoft Azure のネットワーク構成を確認するためのテストを完了し、テスト用仮想マシンが不要になったら、Microsoft Azure 環境からその仮想マシンと関連するすべてのアーティファクトを削除する必要があります。

重要： Microsoft Azure 環境からすべてのテスト用仮想マシンのアーティファクトを削除しないで、仮想マシンをポッドのサブネットの 1 つに接続した場合、後でポッドの [削除] アクションを使用して Horizon Cloud 環境からポッドを削除しようとしても、システムはこれらの残りの接続されているアーティファクトのためにポッドを完全に削除できない可能性があります。デフォルトでは、[削除] アクションを使用してポッドを削除する場合に、Horizon Cloud はポッドのために作成したこれらのリソース グループおよびサブネットを削除します。Microsoft Azure は、継続して使用中であるサブネットの削除を防止します。テスト用仮想マシンのアーティファクトがポッドのサブネットに接続されている場合は、これらのサブネットは削除できず、ポッドの削除は完了しません。この状況を回避するには、ポッドを正常にデプロイした後に、テスト用仮想マシンのすべてのアーティファクトが確実に削除されるようにします。

手順

- 1 Microsoft Azure ポータルにログインします。

2 テスト用仮想マシンは、そのデプロイ方法に応じて次のいずれかの方法で削除します。

- テスト用仮想マシンを独自のリソース グループにデプロイし、そのグループを他の目的で使用していない場合は、リソース グループ全体を削除できます。

注意： 誤って他のアイテムを削除するのを回避するため、リソース グループを削除する前に、リソース グループにはテスト用仮想マシンと、ディスクやネットワーク アダプタなどの関連オブジェクトのみが含まれるようにします。

- リソース グループ全体を削除せずにテスト用仮想マシンを削除する必要がある場合は、ポータルを検索ボックスを使用してテスト用の仮想マシンの名前を検索できます。検索結果には、仮想マシンとそのすべての関連オブジェクト（ディスク、ネットワーク インターフェイス、パブリック IP アドレスなど）が一覧表示されます。各オブジェクトを個別に削除します。

第 1 世代テナント - 最初のポッドのデプロイが完了し、第 1 世代 Horizon Cloud に接続されました

7

おめでとうございます。最初の Horizon Cloud ポッドをのデプロイが完了しました。

重要: この情報は、第 1 世代の制御プレーンで第 1 世代のテナント環境にアクセスできる場合にのみ適用されます。KB-92424 で説明されているように、第 1 世代の制御プレーンは提供終了 (EOA) となりました。詳細については、該当記事を参照してください。

コンソールの [はじめに] ページには、クラウド接続ポッドが正常に作成されたことが表示されます。

次のスクリーンショットは、最初のポッドが Microsoft Azure に展開されている場合のページの外観を示しています。



この時点で、このポッドで使用したい Active Directory ドメインに Horizon Cloud を登録するための手順を実行する必要があります。Horizon Cloud 管理ガイド に、これらの詳細な手順を示します。Horizon Cloud 環境 の使用を開始するという名称のトピックおよびそのサブトピックを参照してください。

リビジョン履歴 - 変更ログ - Microsoft Azure および Horizon ポ ッドの Horizon Cloud へのオンボー ディング

8

このドキュメントのトピックでは、『Onboarding to Horizon Cloud for Microsoft Azure and Horizon Pods — Deployment Guide』への大幅な変更の履歴について説明します。

注： 2019年9月17日以降にガイドのトピックに加えられた大幅な変更についてのみ説明します。それ以前の改訂の詳細情報は提供されません。また、誤字・脱字の修正、リストを表形式にするなどの形式の変更、その他の重要な変更は提供されません。

2023年11月

リビジョン	説明
2023年11月14日	新しいアイテムの更新については、『Horizon Cloud リリース ノート』の「2023年11月」のセクションで紹介しています。

2023年10月

リビジョン	説明
2023年10月26日	新しいアイテムの更新については、『Horizon Cloud リリース ノート』の「2023年10月」のセクションで紹介しています。

2023年5月

リビジョン	説明
2023年5月4日	2023年5月の新機能の更新については、Horizon Cloud リリース ノートの「新機能」で紹介しています。

2023年4月

リビジョン	説明
2023年4月27日	2023年4月の新機能の更新については、Horizon Cloud リリース ノートの「新機能」で紹介しています。
2023年4月17日	Horizon Edge 仮想アプライアンス デプロイの DNS 名の表に、Horizon インフラストラクチャの監視に必要な2つの新しい宛先 URL を追加しました。

2023年2月

リビジョン	説明
2023年2月21日	Horizon Cloud on Microsoft Azure デプロイの DNS 名の表の [プロキシ トラフィック] 列のデータの一部を更新しました。
2023年2月13日	Horizon Cloud on Microsoft Azure デプロイの構成にプロキシが含まれている場合にネットワーク トラフィックがプロキシを通過するかどうかを示すため、DNS 名の表に [プロキシ トラフィック] 列を追加しました。

2023年1月

リビジョン	説明
2023年1月11日	Horizon Cloud Connector に関する既知の問題が [既知の問題] ページに追加されました。

2022年10月

リビジョン	説明
2022年10月20日	Horizon Cloud リリース ノートの「2022年10月の新機能」 に応じて新機能を更新しました。

2022年8月

リビジョン	説明
2022年8月30日	Syslog サーバを有効にする機能に関する問題が、 Horizon Cloud - 既知の問題 ページに追加されました。
2022年8月9日	Horizon Cloud リリース ノートの「2022年8月の新機能」 に応じて新機能を更新しました。

2022年6月

リビジョン	説明
2022年6月28日	Microsoft の Horizon Cloud ポッドおよび関連サービス機能の DNS 要件に、Horizon Edge 仮想アプライアンスの新たな必須 DNS 名を追加しました。
2022年6月26日	Horizon Universal Console へのログインについて説明するドキュメント ページを更新しました。これらの更新は、 Horizon Cloud リリース ノートの 2022年6月26日の更新 に対応しています。コンソール ログインに、VMware Cloud Services を使用した認証が組み込まれるようになりました。
2022年6月23日	Microsoft の Horizon Cloud ポッドおよび関連サービス機能の DNS 要件に新しい必須 DNS 名を追加しました。

2022年4月

リビジョン	説明
2022年4月26日	2022年4月の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2022年3月

リビジョン	説明
2022年3月9日	2022年3月の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2022年2月

リビジョン	説明
2022年2月8日	コンソールが Azure Marketplace 以外のオリジンから取得したイメージの使用を妨げない方法に関する制限事項を、 Horizon Cloud - 既知の制限 に追加しました。Horizon Cloud on Microsoft Azure での使用がサポートされている場合でも、インポートされたすべての基本イメージは、Azure Marketplace をソースとする Windows ベースの仮想マシンから構築する必要があります。
2022年2月3日	2022年2月の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2021年11月30日

リビジョン	説明
2021年11月30日	2021年11月30日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2021年10月12日

リビジョン	説明
2021年10月12日	2021年10月12日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2021年9月7日

リビジョン	説明
2021年9月7日	2021年9月7日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2021年8月18日

リビジョン	説明
2021年8月18日	プライベート キーの有効期限を2年以内に制限する Microsoft Azure ポータルの新しい動作に合わせて 第1世代テナント - ボットのサブスクリプションでの Horizon Cloud アプリケーション登録の作成に関するトピック を更新しました。

2021年8月10日

リビジョン	説明
2021年8月10日	2021年8月10日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2021年7月15日

リビジョン	説明
2021年7月15日	2021年7月15日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2021年6月29日

リビジョン	説明
2021年6月29日	<p>次のトピックを更新して、ポッドの外部および内部ゲートウェイ構成の Unified Access Gateway アプライアンスに対して選択する仮想マシン モデルに関するガイダンスを追加しました。</p> <ul style="list-style-type: none">■ 第1世代テナント - VMware Horizon Cloud Service on Microsoft Azure サービスの制限■ 3章 第1世代テナント - 2023年11月2日のサービス更新以降の新しいポッド デプロイに対する VMware Horizon Cloud Service on Microsoft Azure 要件チェックリスト■ 第1世代テナント - Horizon Cloud ポッドのゲートウェイ構成の指定

2021年6月9日

リビジョン	説明
2021年6月9日	<p>次のトピックを更新して、Europe-3（ドイツ）の地域別制御プレーン インスタンスに関する情報を追加し、パターン query-prod* の DNS 名の記述を削除しました。query-prod* DNS 名へ到達可能である必要はありません。</p> <ul style="list-style-type: none">■ 第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名■ 第1世代テナント - Horizon Cloud Connector と Horizon ポッドを使用するときの DNS、ポート、およびプロトコルの要件 <p>また、第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件、DNS 名のトピックに修正が加えられました。パターン kinesis.* でのクラウド管理サービスの DNS 名に関する表の行のソース サブネットは、ポッドの管理サブネットです。これまでは、その表の行には、テナント サブネットがソース サブネットとして表記されていました。</p>

2021年5月20日

リビジョン	説明
2021年5月20日	2021年5月20日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2021年4月14日

リビジョン	説明
2021年4月14日	2021年4月14日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2021年3月25日

リビジョン	説明
2021年3月25日	2021年3月25日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2021年3月9日

リビジョン	説明
2021年3月9日	2021年3月9日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2021年3月1日

リビジョン	説明
2021年3月1日	ドメイン参加アカウントをスーパー管理者ロールを持つ Active Directory グループに含めなければならないという要件の削除に関連する更新。この要件は、ポッド フリートに 1600.0 より古いマニフェストを実行している Microsoft Azure の Horizon Cloud ポッドがある場合にのみ適用されます。詳細については、 Horizon Cloud の運用に必要なサービス アカウント を参照してください。

2021年1月7日

リビジョン	説明
2021年1月7日	2021年1月7日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2020年12月15日

リビジョン	説明
2020年12月15日	2020年12月15日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2020年12月2日

リビジョン	説明
2020年12月2日	2020年12月2日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2020年11月24日

リビジョン	説明
2020年11月24日	2020年11月24日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2020年11月4日

リビジョン	説明
2020年11月4日	2020年11月4日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2020年10月8日

リビジョン	説明
2020年10月8日	2020年10月8日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2020年7月9日～2020年10月7日

リビジョン	説明
2020年9月9日	「はじめに」ページの[管理]メニューで提供される機能に合わせて、このガイドのスクリーンショットを更新しました。 Horizon Cloud Connector の既知の考慮事項にも更新があります。
2020年8月18日	このガイドを Horizon のドキュメントに合わせて更新し、各トピックのコンテキストに応じて、基本イメージとゴールドイメージという用語を採用しました。
2020年8月5日	このガイドに従って、日本の新しい地域別クラウド制御プレーンを利用できるようになりました。この地域別制御プレーンのDNS名に関して、ドキュメント第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件 、DNS名および第1世代テナント - Horizon Cloud Connector と Horizon ポッド を使用するときのDNS、ポート、およびプロトコルの要件のトピックが更新されました。
2020年7月13日	高可用性 (HA) 機能を備えたポッドが、Microsoft Azure Government (米国バージニア州政府、米国アリゾナ州政府、米国テキサス州政府) でサポートされるようになりました。
2020年7月9日	2020年7月9日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2020年3月17日～2020年7月8日

リビジョン	説明
2020年6月9日	2020年6月9日の Horizon Cloud リリース ノートの「新機能」 に合わせて、このガイドを更新しました。「ようこそ」Eメールに表示される地域名が、わかりやすい名前を使用するように更新されました。次のドキュメントのトピックも更新され、その変更に合わせて変更されました：第1世代テナント - Horizon Cloud on Microsoft Azure のデプロイ - ホスト名解決の要件 、DNS名
2020年5月27日	2020年5月27日の Horizon Cloud リリース ノートの「新機能」 に合わせて、このガイドを更新しました。
2020年5月12日	2020年5月12日の Horizon Cloud リリース ノートの「新機能」 に合わせて、このガイドを更新しました。エージェントに関連するポートとプロトコルの要件に関する表のエントリも修正しました。
2020年4月14日	2020年4月13日の Horizon Cloud リリース ノートの「新機能」 に合わせて、このガイドを更新しました。
2020年3月17日	2020年3月17日の新機能の更新については、 Horizon Cloud リリース ノートの「新機能」 で紹介しています。

2019年13月12日～2020年3月16日

リビジョン	説明
2020年2月25日	<p>記載されている変更について、次のトピックを更新しました。</p> <ul style="list-style-type: none"> ■ 第1世代テナント - 組織が第1世代 Horizon Cloud のアプリケーション登録にカスタム ロールを使用することを希望する場合のリストに Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read を追加しました。 ■ 第1世代テナント - ポッドのサブスクリプションでの Horizon Cloud アプリケーション登録の作成のリストにリソース プロバイダ Microsoft.Sql を追加しました。 ■ ジャンプ ボックス仮想マシンとポッド マネージャ仮想マシンが第1世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件へのポート 9443/TCP を使用して、Unified Access Gateway 仮想マシンにアクセスするための行を追加しました。このポートは、ポッドのデプロイ中およびポッドを編集して Unified Access Gateway の設定を変更するときに、Unified Access Gateway の設定を構成するために必要です。 ■ 第1世代テナント - Horizon Cloud ポッド - ポートとプロトコルの要件で、ログイン認証トラフィックのためのポッドの Unified Access Gateway 仮想マシンからポッドの Microsoft Azure ロード バランサへのトラフィックのポート要件として、ポート 443 を 8433 に修正しました。
2020年1月13日	<p>Horizon 7 Cloud Connector のプロキシ関連の情報を更新しました。更新されたトピックには第1世代テナント - Horizon ポッドの第1世代の Horizon Cloud 制御プレーンへのオンボーディングおよび第1世代テナント - Horizon ポッドと Horizon Cloud Connector - 第1世代の制御プレーン サービスにオンボーディングする準備が含まれます。</p>
2020年1月6日	<p>コマンドライン インターフェイスの使用による Horizon Cloud Connector への SSH アクセスの有効化、4章 第1世代の Horizon Cloud 制御プレーンを使用する VMware Horizon 8 ポッド - 要件チェックリスト - 2023年11月2日のサービス更新に合わせて適切に更新されましたに関するトピックに新しい情報を追加しました。</p>
2019年13月12日	<p>2020年12月13日の新機能の更新については、Horizon Cloud リリース ノートの「新機能」で紹介しています。</p>

2019年9月17日～2019年12月12日

リビジョン	説明
2019年11月21日	<p>ドキュメントのトピック第1世代テナント - ポッドのサブスクリプションでの Horizon Cloud アプリケーション登録の作成の手順 8で、リソース プロバイダのリストを、最新のポッド アーキテクチャに関連する Microsoft Azure のサブスクリプションに必要な追加のリソース プロバイダで更新しました。</p>
2019年9月17日	<p>2020年9月17日の新機能の更新については、Horizon Cloud リリース ノートの「新機能」で紹介しています。</p>