第 1 世代テナント - Horizon Cloud 管理ガイド

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

目次

第 1 世代テナント - ポッド フリート管理 - Horizon Cloud 10

1 第 1 世代テナント - Horizon Cloud 環境の使用を開始する 15

第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行 18

Horizon Cloud の運用に必要なサービス アカウント 27

Horizon Cloud の Active Directory の登録ワークフローの NETBIOS 名と DNS ドメイン名のフィールドに必要な情報の検索 32

Horizon Cloud on Microsoft Azure - LDAPS (LDAP Over SSL) 用に構成された Active Directory 環境の使用 34

Horizon Cloud LDAP サーバの署名要件がある Active Directory ドメイン コントローラのサポート 42

Horizon Cloud のクラウド接続されたポッドに対する外部およびフォレストの信頼のサポートについて 42

Horizon Universal Console にログインして Horizon Cloud 環境で管理タスクを実行する 43

Horizon Cloud テナント環境への認証について 45

第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアー 49

第 1 世代 Horizon Universal Console のナビゲーション メニューとフィルタ フィールドの使用について 51

追加の Active Directory ドメインの登録 95

追加の補助ドメイン バインド アカウントを追加します。 102

Horizon Universal Console 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 103

Horizon Cloud テナント環境にログインし、Horizon Universal Console を使用してアクションを実行するための管理者ロールを組織内の個人に付与する 109

Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てる 113

第 1 世代のテナント - Horizon Cloud 環境の Cloud Monitoring Service (CMS) の有効化または無効化 118

第 1 世代テナント - Horizon Universal Console を使用して Horizon Cloud テナントを VMware Cloud Services Engagement Platform および VMware Cloud Services にオンボーディングする 119

Active Directory ドメイン登録の削除 122

2 第 1 世代のテナント - 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 124

第 1 世代のテナント - 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 127

Horizon インフラストラクチャの監視 と Horizon Cloud 環境のポッド 132

Horizon Cloud 環境内のヘルプ デスク機能 132

コンソールの検索機能の使用 133

第 1 世代テナント - ユーザー カード機能（別称：Horizon Cloud のヘルプ デスク）について 134

3 第 1 世代テナント - 第 1 世代 Horizon Cloud がサポートするすべてのポッド タイプのクラウド接続ポッドの管理 141

制御プレーン サービスとしての Horizon Console の起動 148

第 1 世代テナント - 第 1 世代 Horizon Universal Console の [キャパシティ] の概要と、Horizon Cloud のポッド フリートへのポッドの追加 150

第 1 世代テナント - Microsoft Azure 上の Horizon Cloud ポッド - 第 1 世代 Horizon Universal Console の [キャパシティ] ページを使用した、ポッド フリートへのポッドの追加 151

Horizon Cloud - [キャパシティ] ページの編集ワークフローを使用した、クラウド接続されたポッドのクラウドに関連するいくつかの特性の変更 186

クラウド接続された Horizon ポッドを Horizon Cloud での使用から削除する 187

プロセス中にオフラインだった Horizon ポッドからクラウド管理プロパティをクリアして Horizon Cloud から切断する 188

4 第 1 世代テナント - Day-2 Horizon Cloud Connector タスク 190

Horizon Cloud Connector 2.0 以降 - 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 192

Horizon Cloud Connector 2.0 以降 - ノード レベルの高可用性の設定 196

Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector クラスタからのワーカー ノードの削除 198

Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector ノード上のサービスのステータスの監視 199

Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector クラスタの管理コマンド 200

Horizon Cloud Connector 仮想アプライアンスの CA 署名付き証明書の構成 201

Horizon Cloud Connector 2.4 以降 - 送信トラフィック用に SSL オフロードを構成している場合は、Horizon Cloud Connector でカスタムの CA 署名証明書を構成して Horizon 制御プレーンへの接続を許可する 204

Horizon Cloud Connector 仮想アプライアンスの固定 IP アドレスの更新 205

Horizon Cloud Connector root ユーザーのパスワード有効期限ポリシーの設定 206

Horizon Cloud Connector の root パスワードまたは ccadmin パスワードのリセット 207

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 209

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 211

Horizon Cloud Connector 2.4 以降：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 214

Horizon Cloud Connector の DNS 設定の変更 215

Horizon Cloud Connector 1.6 以降のプロキシ設定の変更 216

Horizon Cloud Connector 1.5 以前のプロキシ設定の変更 217

Horizon Cloud Connector 仮想アプライアンスと NTP サーバの同期 219

Horizon Cloud Connector 2.0 以降：SNMP を使用したアプライアンスの監視 220

Horizon ユニバーサル ライセンスの監視 224

Horizon Cloud Connector 仮想アプライアンスの手動更新 227

Horizon Cloud Connector 仮想アプライアンスの自動更新の構成 233

Horizon Cloud Connector 仮想アプライアンスの更新のトラブルシューティング 243

Horizon Cloud Connector アプライアンスのログ ファイルの収集 243

Horizon Cloud Connector の既知の考慮事項 245

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　246

5 第 1 世代 Horizon Cloud Universal Broker とマルチクラウド割り当て　253

VMware Horizon Service Universal Broker について　255

Universal Broker のシステム アーキテクチャとコンポーネント　258

Universal Broker - 機能に関する注意事項と既知の制限　262

Universal Broker のシステム要件　265

Horizon ポッド - Universal Broker の DNS、ポートおよびプロトコルの要件　268

Horizon 制御プレーン テナントの Universal Broker サービスのセットアップ　269

Horizon ポッド - Universal Broker で使用する Unified Access Gateway を構成する　270

Horizon ポッド - Connection Server への Universal Broker プラグインのインストール　273

Horizon Universal Console を使用した Universal Broker の有効化の開始　278

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　281

Universal Broker の内部ネットワーク範囲の定義　283

Universal Broker セッションに対するグローバル クライアント制限の構成　284

Universal Broker の設定　287

Universal Broker 環境でのサイトの操作　297

Universal Broker のサイトの構成　298

Universal Broker のホーム サイトの構成　300

View ポッド - マルチクラウド割り当てのためのクラウド接続されたポッドの有効化　302

Horizon Universal Console を使用して、クラウド接続された Horizon ポッドを管理対象状態に変更する　303

Horizon ポッド - ポッドを監視対象状態に変更する　304

Universal Broker 環境での割り当ての作成および管理　305

Horizon ポッド - マルチクラウド割り当てに適したデスクトップ プールの作成　305

Horizon ポッド - マルチクラウド割り当てに使用する既存のデスクトップ プールを準備する　307

Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成　308

Horizon ポッド - Universal Broker 環境用の RDSH デスクトップとアプリケーションの構成　313

Horizon ポッド - マルチクラウド割り当てからのデスクトップ プールの削除　316

Microsoft Azure の Horizon Cloud ポッド - 第 1 世代環境での VDI マルチクラウド割り当ての作成と表示　318

ポッドがオフラインになった場合の Universal Broker 環境での割り当てに関する考慮事項　338

Horizon Cloud テナント環境でのマルチクラウド割り当ての管理　339

6 ユーザーの Horizon Cloud on Microsoft Azure 環境　346

Horizon Cloud on Microsoft Azure 環境の高可用性の特性　353

Microsoft Azure の Horizon Cloud ポッドでの高可用性の有効化　357

Microsoft Azure でのデスクトップ イメージと Horizon Cloud ポッドの作成　358

ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリング　363

インポートされた仮想マシンの Windows オペレーティング システムをカスタマイズ　377

Horizon Cloud ファームとデスクトップから最適なリモート エクスペリエンス パフォーマンスを引き出すためにゴールド イメージで実行すべき 5 つの重要な手順 387
Horizon Cloud on Microsoft Azure - インポートした GPU 対応仮想マシンに適切な GPU ドライバをインストールする 393
構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の割り当て可能なイメージに変換する 395
Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートする 398
Horizon Cloud 環境のファームと VDI デスクトップでの Microsoft Azure Disk Encryption の使用 421
Microsoft Azure の Horizon Cloud ポッドからの仮想デスクトップでのデータディスクの使用 424
Horizon Cloud のイメージ仮想マシンのデータ ディスクの設定 426
Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッド 428
Horizon Cloud のインポートされたイメージ仮想マシンへの NSX Tools のインストール 431
ポッドでプロビジョニングされた仮想マシンに対する NSX Manager で必要となるファイアウォールルール 435
ポッドでプロビジョニングされた仮想マシンに必要な転送ポリシーの NSX Manager への追加 435
Horizon Universal Console でのファームと割り当ての仮想マシン タイプとサイズの管理 436
ネストされた Active Directory ドメイン組織単位の使用についての考慮事項 438
Horizon Cloud のファーム 438
第 1 世代 Horizon Cloud ポッド - ファームの作成と管理 439
ファームのローリング メンテナンスの例 463
Horizon Cloud のファームの電源管理とロード バランシングについて 464
Horizon Cloud ポッド内のネットワーク セキュリティ グループとファームについて 466
Horizon Cloud インベントリ内のアプリケーション 467
Microsoft Azure 上の Horizon Cloud の App Volumes アプリケーション - 概要および前提条件 468
リモート アプリケーション - Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた RDSH ファームからのインポート 495
リモート アプリケーション - Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされたリモート アプリケーションのリモート アプリケーション割り当ての作成 498
Microsoft Azure の Horizon Cloud ポッドに基づくテナントのデスクトップ割り当ての概要 500
Horizon Cloud ポッド - RDS ベースのセッション デスクトップ割り当てを作成して、エンド ユーザーのために RDS ホストからのデスクトップ セッションを提供する 502
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 504
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 518
Horizon Cloud on Microsoft Azure - シングルポッド ブローカの概要 531
シングルポッド ブローカ - Horizon Cloud ポッド - URL リダイレクトのカスタマイズを作成し、ユーザーに割り当てる 531
シングルポッド ブローカ - Horizon Cloud ポッドと URL コンテンツ リダイレクト機能 535
Microsoft Azure での Horizon Cloud ポッドの公開イメージの管理 539
Microsoft Azure の Horizon Cloud ポッドから発行されたイメージに対して実行できるアクション 540
Horizon Cloud でのファームに使用されるイメージの変更 543
VDI デスクトップ割り当てに使用されるイメージの変更 545
Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた割り当ての管理 547
Workspace ONE UEM を使用して Microsoft Azure の Horizon Cloud ポッド内の専用 VDI デスクトップを管理する 553

Horizon Cloud 環境で現在設定されている割り当ての表示　553
Horizon Cloud 環境での割り当ての編集　555
Horizon Cloud 環境からの割り当ての削除　555
Horizon Cloud 環境での VDI デスクトップ割り当てのサイズ変更　556
Microsoft Azure の 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の仮想マシン モデルの変更　558
Horizon Cloud ポッド - VDI 専用デスクトップ割り当ての特定の VDI デスクトップのサイズ変更　560
シングルポッド ブローカ - 専用デスクトップ割り当て間の仮想マシンの移行　562
専用デスクトップ割り当ての削除の防止または削除の許可　564
Horizon Cloud ポッド内のネットワーク セキュリティ グループと VDI デスクトップについて　565
Horizon Cloud ポッド - VDI デスクトップ割り当て、ファーム、公開イメージ、ベース仮想マシンにインストールされたエージェント関連ソフトウェアの更新　567
Horizon Cloud の RDSH イメージのエージェント ソフトウェアをアップデートする　569
専用 VDI デスクトップ割り当て用のエージェント ソフトウェアを更新する　571
Horizon Cloud ポッド - フローティング VDI デスクトップ割り当てによって使用されるイメージのエージェント ソフトウェアを更新する　589
Microsoft Azure にデプロイされた Horizon Cloud ポッドの管理　592
IT またはセキュリティ組織で、Horizon Cloud on Microsoft Azure 環境のサブスクリプションでの Azure Marketplace オファーの使用またはマーケットプレイスでの購入に制限がある場合、または環境で Azure China を使用している場合　592
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　597
Microsoft Azure でデプロイされた Horizon Cloud ポッドのゲートウェイ関連項目の変更　601
ファーム用および VDI 割り当て用 Horizon Cloud ポッドでの複数のテナント サブネットの使用の概要　634
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　638
Horizon Cloud：Microsoft Azure サブスクリプション情報の削除、編集、および追加　641
Horizon Universal Console を使用して、サブスクリプションによる Microsoft Azure 制限の現在の使用率を調べる　645
Horizon Cloud ポッド - メンテナンスと更新　646
Horizon Cloud on Microsoft Azure デプロイのバックアップとリストア　662
Horizon Cloud ポッドの NTP 設定を変更する　663
コネクタがポッド マネージャ仮想マシンへの接続を信頼できるように、Workspace ONE Access コネクタ アプライアンスを Microsoft Azure の Horizon Cloud ポッドと統合する場合には、ポッド マネージャ仮想マシンで SSL 証明書を直接構成します。　663
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　672
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　703
第 1 世代テナント - Microsoft Azure にデプロイされた 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　720
第 1 世代テナント - 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　764

7 シングル ポッド ブローカから Universal Broker への移行について　768

Horizon Cloud - Universal Broker に移行するためのシステム要件　772
シングル ポッド ブローカから Universal Broker への移行をスケジューリングして完了する　775

Universal Broker への移行後のテナント環境の最新情報　786

8 VMware Workspace ONE およびオプションの True SSO 機能を使用した Horizon Cloud 環境の使用について　789

Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合する　790

Universal Broker による Horizon Cloud 環境 - Workspace ONE Access および Intelligent Hub サービスとの統合によるアーキテクチャ　798

Workspace ONE Access を使用する Horizon Cloud - リモート アプリケーション アクセス クライアントの作成　799

Workspace ONE Access を使用する Horizon Cloud：Universal Broker が有効になっている Horizon Cloud テナントと統合するためのユーザー属性の構成　800

Workspace ONE Access を使用する Horizon Cloud - Horizon Cloud との統合のための Intelligent Hub の構成　802

Universal Broker を使用した第 1 世代の Horizon Cloud - ユーザー接続のための Intelligent Hub リダイレクトの構成　803

Universal Broker による Horizon Cloud 環境 - Horizon Cloud Workspace ONE Access の統合の削除　805

シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure の環境の Horizon Cloud ポッドと Workspace ONE Access の統合　806

シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure で関連する Workspace ONE Access テナント情報を使用して Horizon Cloud ポッドを構成する手順　811

シングルポッド仲介を使用した Horizon Cloud 環境：エンド ユーザーによる Workspace ONE Access のデスクトップ割り当てへのアクセスの確認　813

True SSO を Horizon Cloud 環境で使用するために構成する　814

Horizon Cloud - True SSO - Microsoft Windows Server システムを使用したエンタープライズ認証局の設定　815

Horizon Cloud - True SSO - CA での証明書テンプレートの設定　817

Horizon Cloud - True SSO - Horizon Cloud ペアリング バンドルのダウンロード　820

第 1 世代の Horizon Cloud - True SSO - 登録サーバの設定　821

Horizon Cloud - True SSO - Horizon Cloud 環境の True SSO の構成を完了する　823

9 Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた資格のあるデスクトップおよびリモート アプリケーションへのエンド ユーザーの接続　825

RDS デスクトップ セッションと RDS ベースのアプリケーション セッションのタイム ゾーン リダイレクトの有効化　826

Microsoft Azure の Horizon Cloud ポッドによって提供されるデスクトップおよびリモート アプリケーションの複数モニタのサポート　827

Horizon Cloud on Microsoft Azure - Microsoft Teams のメディア最適化のサポート　828

デスクトップおよびアプリケーションへのアクセス　829

Horizon Client を使用したデスクトップまたは RDS ベースのリモート アプリケーションへのログイン　829

ブラウザを使用したデスクトップおよび RDS ベースのリモート アプリケーションへのログイン　830

ファイルのリダイレクトを使用したリモート アプリケーションによるローカル ファイルへのアクセス　831

Universal Broker を使用した Horizon Cloud 環境では、エンド ユーザーが Workspace ONE Intelligent Hub を使用して、使用資格が付与されたデスクトップやアプリケーションにアクセスすることを強制します。　832

シングルポッド仲介を使用した Horizon Cloud 環境では、エンド ユーザーが Workspace ONE Access を使用して、使用資格が付与されたデスクトップやアプリケーションにアクセスすることを強制します。 833

10 Horizon Cloud 環境の管理者向けトラブルシューティング 836

Horizon Cloud - Horizon Universal Console を使用したエージェント ログの収集 836

ファームまたは VDI デスクトップ割り当てのディスク サイズが増加した場合に必要な管理者のアクション 838

Horizon Universal Console の最初のログイン画面で正常にログインできない 839

ログに記録された Microsoft Windows Sysprep エラーを解決した後でも、イメージへの変換タスクがタイムアウト エラーで失敗する 839

Windows Server 2012 イメージの場合に、イメージ タスクへの変換がタイムアウト エラーで失敗する 840

プライマリ ドメイン バインド アカウントがロックアウトされているときの通知 841

新しいファームが進行中のままになる 841

フローティング VDI デスクトップ割り当てからデスクトップへの接続を試みると Windows のエラー メッセージが表示される 842

True SSO が構成され、ユーザーに証明書の失効ステータスに関するメッセージが表示される場合 842

ポッドがマニフェスト 1230 以降に更新されていないときに、インポートしたイメージにリモート接続するためのドメイン アカウントの機能を設定する方法 843

11 リビジョン履歴 - 変更ログ - Horizon Cloud のテナント環境とオンボーディングされたポッドの管理 846

第 1 世代テナント - ポッド フリート管理 - Horizon Cloud

このページの管理コレクションでは、第 1 世代のテナント環境のフリートに 1 つ以上のポッドがある場合の操作について説明します。このドキュメント ページは、ここでは主に管理コレクションのエントリ ページとして機能します。このコレクションには、Horizon Universal Console を使用して第 1 世代の制御プレーンにオンボーディングしたポッドを管理する Day-1 タスクと Day-2 タスクの両方に関するページが含まれています。

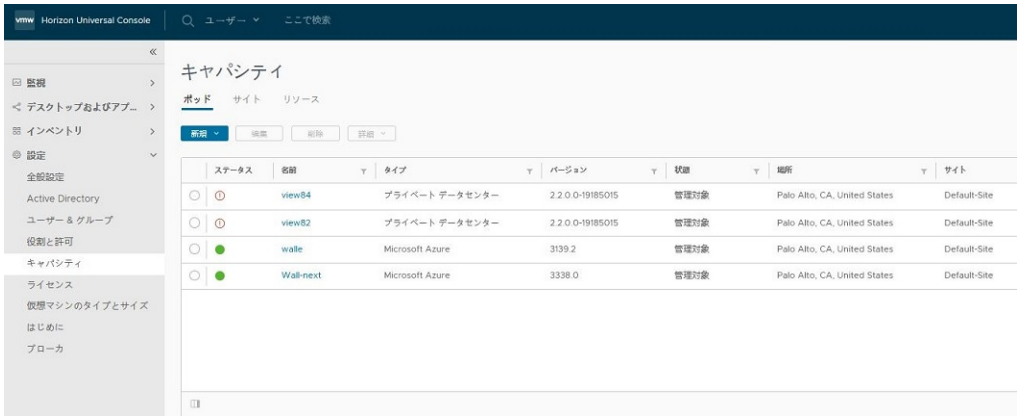
このページについて

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。

第 1 世代テナント管理の簡単な紹介



テナント環境全体は、VMware がホストするサービスと、適切にデプロイされ、サービスの制御プレーンに接続されたポッドのフリートで構成されます。

ポッド フリートと、制御プレーンが提供するクラウド ホスト型管理機能を使用するには、Horizon Universal Console（略して、コンソール）という名前のテナント環境の Web ベースの管理ポータルを使用します。主な概念の詳細については、サービス、クラウド制御プレーン、クラウド接続されたポッド、および関連概念の概要のページを参照してください。

ポッド フリート

テナントのポッド フリートは、次のいずれか 1 つ以上で構成されます。

Horizon ポッド

Horizon Connection Server ソフトウェアに基づくポッドです。

Horizon Cloud ポッド

Microsoft Azure での実行に特化した VMware Horizon Cloud のポッド マネージャ テクノロジーに基づくポッドです。

このドキュメント内の情報は、テナントのポッド フリート内に少なくとも 1 つのポッドがある場合の、Horizon Cloud 機能の使用方法について説明するものです。最初のポッドをテナントに追加する方法については、『デプロイ ガイド』の 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トピックとそのサブトピックを参照してください。

ここで機能について読み、実際の環境で機能を表示されない場合

このドキュメントに記載された機能が実際にコンソールに表示されない場合、次の理由が考えられます。

- これらのドキュメント ページには、サービスおよび制御プレーンの現在のリリースが反映されています。現在サポートされているリリース レベルに更新されていないポッド コンポーネントがあり、特定の機能が最新レベルに依存している場合、実際の環境ではこのガイドに記載されている内容が反映されないことがあります。
- 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が含まれている場合があります。お持ちのライセンスにそのような機能の使用が含まれる場合のみ、Horizon Universal Console にその機能に関連する要素が反映されます。
- サービスには、テナントごとの要求によってのみ有効になる機能が含まれる場合があります。すべてのテナントに同じ機能が自動的に表示されるわけではありません。

Horizon Cloud ドキュメントに記載されている機能が環境内で表示されない場合は、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。

これらの管理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、11 章 リビジョン履歴 - 変更ログ - Horizon Cloud のテナント環境とオンボーディングされたポッドの管理を参照してください。

対象読者

このドキュメントは、システム管理者としての経験があり、仮想マシン テクノロジーおよびデータセンターの運用に詳しい方を対象としています。

組織のニーズおよび動作しているポッドのタイプに応じて、次のソフトウェア製品、ソフトウェア コンポーネント、およびそれらの機能について理解しておくことは有用です。

- VMware Horizon
- VMware Horizon® Cloud Connector™
- VMware Unified Access Gateway™
- VMware Workspace ONE® Access™
- VMware Workspace ONE Hub Services
- VMware Workspace ONE® UEM
- VMware Horizon® Client™
- VMware Horizon® HTML Access™
- 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)
- Microsoft Active Directory
- VMware Dynamic Environment Manager™

このドキュメントで使用する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。

- 説明に対応するユーザー インターフェイスの部分のみが表示されます。完全なユーザー インターフェイスが表示されるとは限りません。
- 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。

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。

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

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

- My VMware® 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。
- 少なくとも 1 つのクラウド接続ポッドを構成した後、クラウドベースのコンソールにログインし、[] - [サポート] をクリックするとサポート リクエストを発行できます。

これらの管理ガイドのドキュメント トピックで使用されているポッド関連の用語の選択

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。

VMware Information Experience 用語集

VMware Information Experience 用語集は、専門的な用語などを集約した用語集です。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。

VMware のプライバシー通知

VMware がこの製品を介して収集した情報をどのように処理するかについては、https://www.vmware.com/help/privacy.html を参照してください。

第 1 世代テナント - Horizon Cloud 環境の使用を開始する

1

第 1 世代 Horizon Cloud 環境全体は、VMware がホストするクラウド サービス、提供されるキャパシティ、およびそのキャパシティにデプロイされクラウド サービスに接続される VMware ソフトウェアで構成されます。上記のキャパシティでインストールされた VMware ソフトウェアが適切に構成されクラウド サービスに接続されると、構成されたエンティティはクラウド接続されたポッドになります。クラウド接続されたポッドを 1 つ以上使用し、Active Directory の登録プロセスを完了すると、健全性の監視、ヘルプ デスク サービスなど、これらのポッドに関連する管理や管理タスクに、クラウドベースおよび Web ベースの Horizon Universal Console 使用が可能になります。

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。

このページについて

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。

簡単な紹介

第 1 世代のテナント環境の概要については、「Horizon Cloud の紹介およびポッドをクラウド接続するためのオンボーディングの概要」を参照してください。サポートされているキャパシティ環境とは、Microsoft Azure クラウドや、VMware がサポートする SDDC などです。これらのキャパシティ環境には、それぞれ特定のポッド タイプが用意されています。

- Microsoft Azure クラウドのポッド
- Horizon Cloud Connector を使用して接続された Horizon ポッド - VMware がサポートする SDDC にデプロイされた Horizon ポッド

クラウド接続されたポッドが 1 つ以上あり、Active Directory の登録プロセスが完了すると、環境で管理タスクを実行するためにコンソールが使用されるようになります。コンソールは、Horizon Cloud が提供するクラウドベースのサービスを統合的に表示し、集中管理できるようにします。Web ベースのコンソールは、業界標準の Web ブラウザで動作します。サポート対象の Web ブラウザのタイプとバージョンの一覧については、第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアーを参照してください。

アクセス可能なキャパシティ タイプに応じて、同じコンソールを使用してそのキャパシティ内にポッドを自動でデプロイし、ポッドの Horizon Cloud への接続を設定できます。一部のタイプのポッドでは、自動的なデプロイおよび構成はできませんが、いくつかの必要な接続手順を実行した後に、それらのポッドをクラウドに接続して、同じ管理コンソールで操作できます。

概要レベルの手順を開始する

クラウドホスト型サービスまたは Horizon Cloud ポッドを備えたコンソールを使用するには、次のことを行う必要があります。

- 最初のポッドを Horizon Cloud に接続します。最初にデプロイするポッドのタイプに応じて、次を参照してください。
  - Horizon ポッド — Horizon ポッドの高度なワークフロー
  - Microsoft Azure への Horizon Cloud ポッド — ポッドを Microsoft Azure にデプロイするための高度なワークフロー
- 第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行します。

  ドメインの登録には、以下の両方が含まれます。

  - Horizon Cloud が Active Directory 内の検索を実行するために使用する、プライマリ ドメイン バインド アカウントおよび補助ドメイン バインド アカウント。最初にドメインを登録するときに補助ドメイン バインド アカウントを指定することで、プライマリ バインド アカウントがアクセスできない場合に管理者ユーザーがコンソールからロックアウトされないようにします。
  - Microsoft Azure Marketplace からの仮想マシンのインポート、ファーム RDSH インスタンスの作成、VDI デスクトップ インスタンスの作成など、仮想マシンをドメインに参加させる必要のあるポッド操作で Horizon Cloud が使用するドメイン参加アカウント。

  注： このリリースでは、ドメイン結合アカウントは主に Microsoft Azure のポッドを使用したシステム操作で使用されます。クラウド接続された Horizon ポッドは、Active Directory ドメイン登録手順で指定したドメイン参加アカウントを使用しません。ただし、クラウド接続された Horizon ポッドのみを環境で使用している場合でも、後でスーパー管理者ロールを割り当てるプロンプトがアクティブになるよう、ドメイン参加アカウントの手順を完了しておくことが賢明です。Active Directory ドメイン グループへのこのロールの割り当ては、すべてのタイプのクラウド接続ポッドで必要な手順です。

  これらのドメイン バインドおよびドメイン参加アカウントの要件については、Horizon Cloud の運用に必要なサービス アカウントを参照してください。

ドメイン登録ワークフローの詳細については、第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行を参照してください。

その後、ベスト プラクティスとして、[はじめに] ウィザードに表示される推奨されているアクションを実行します。

重要： また、既知の問題により、Horizon Cloud Connector を使用して Horizon ポッドを接続するときに、最初のポッドの Active Directory ドメイン登録プロセスを完了せずに後続のポッドでコネクタのクラウド ペアリング ワークフローを実行しようとすると、予期しない結果が発生する可能性があります。コネクタのクラウド ペアリング ワークフローは、Horizon Cloud への最初の Active Directory ドメイン登録を完了する前に複数のポッドに対して実行することができますが、最初のドメイン登録を完了する前に次のポッドでそのクラウド ペアリング プロセスを実行しようとすると、このドメイン登録プロセスが失敗することがあります。その場合は、以下を実行する必要があります。

1 Web ベースの Horizon Cloud Connector 構成ポータルで [接続解除] アクションを使用し、クラウド接続されたポッドが 1 つになるまでそれらのクラウド接続された各ポッド間の接続を解除します。

2 Active Directory ドメイン登録の削除の手順に従い、Horizon Universal Console を使用して失敗した登録を削除します。

3 そのポッドに関連する、最初の Active Directory ドメイン登録プロセスを完了します。

4 Web ベースの Horizon Cloud Connector 構成ポータルで、他のポッドに対してコネクタのクラウド ペアリング ワークフローを再実行します。

最初の Active Directory ドメインがポッドの使用のために Horizon Cloud に登録された後、追加の Active Directory ドメインをクラウド構成の Active Directory ドメインとして Horizon Cloud テナント環境に登録するできます。追加の Active Directory ドメインを登録すると、管理コンソールを使用して実行するさまざまな Horizon Cloud ワークフロー内でこれらのドメインのユーザー アカウントを指定することができます。たとえば、ポッドでプロビジョニングされたリソースの使用権限をエンド ユーザーに付与したり、管理ユーザーに管理ロールを割り当てたりすることができます。最初の Active Directory ドメインが登録された後で、追加の補助ドメイン バインド アカウントおよび補助ドメイン参加アカウントも構成することができます。

重要： このリリースでは、すべてのポッドがクラウド構成のすべての Active Directory ドメインに対して通信路を確立している必要があります。コンソールで Active Directory ドメインを登録すると、そのドメインはユーザーの Horizon Cloud 環境に対するクラウド構成の Active Directory ドメインのセットに追加されます。

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て、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。

次のトピックを参照してください。

- 第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行

- Horizon Universal Console にログインして Horizon Cloud 環境で管理タスクを実行する
- 第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアー
- 追加の Active Directory ドメインをクラウド構成の Active Directory ドメインとして Horizon Cloud テナント環境に登録する
- Horizon Cloud のクラウド構成の Active Directory ドメイン用に補助バインド アカウントを追加する
- Horizon Universal Console 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
- Horizon Cloud テナント環境にログインし、Horizon Universal Console を使用してアクションを実行するための管理者ロールを組織内の個人に付与する
- Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てる
- 第 1 世代のテナント - Horizon Cloud 環境の Cloud Monitoring Service (CMS) の有効化または無効化
- 第 1 世代テナント - Horizon Universal Console を使用して Horizon Cloud テナントを VMware Cloud Services Engagement Platform および VMware Cloud Services にオンボーディングする
- Active Directory ドメイン登録の削除

第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行

このページは、第 1 世代の Horizon Cloud Service デプロイに適用されます。このページでは、第 1 世代の Horizon Universal Console 管理機能のロックを解除するために必要な Active Directory ドメイン情報を構成するための複数ステップのワークフローについて説明します。

ヒント: この 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。コンソールの「はじめに - キャパシティおよび全般的なセットアップ領域」で使用可能な一部の機能を除き、1 つ以上の Active Directory ドメインが構成されるまで、コンソールはロックされたままになります。

この登録フローを完了することにより、第 1 世代のテナントの環境に適したコンソールのすべての管理機能がロック解除されます。

目的

最初のポッドがテナントのポッド フリートに追加された直後またはすぐ後にこのワークフローを完了することがベスト プラクティスです。そのポッドが Horizon Cloud on Microsoft Azure デプロイであるか、または Horizon Cloud Connector を使用した Horizon ポッドのデプロイであるかは関係ありません。

完了がベスト プラクティスである理由は、このワークフローによってコンソールの管理機能がロック解除されるためです。テナントに少なくとも 1 つの Active Directory ドメインが設定されるまで、コンソールの管理機能のほとんどすべてがグレーアウトされ、ロックされます。

概要

ドメイン登録ワークフロー全体にこの高レベルのシーケンスがあります。

1 cloud.horizon.vmware.com から、画面のプロンプトに従ってコンソールにログインします。次に、コンソールで Active Directory 構成ワークフローを開始します。

2 ドメイン バインド手順では、テナントで Active Directory ドメインのクエリに使用できる Active Directory ドメインの名前関連情報、プロトコル関連情報、およびドメイン バインド サービス アカウントの資格情報を指定します。プライマリ アカウントと補助アカウントの両方を指定する必要があります。そのドメイン バインド アカウントに必要な Horizon Cloud については、ドメイン バインド アカウント - 必須の特性を参照してください。

3 ドメイン参加情報は、Horizon Cloud on Microsoft Azure のデプロイに必要です。この手順では、サービスがテナントのマシン名を解決できるようにする DNS サーバの IP アドレス、ポッドがプロビジョニングされたマルチセッション マシンとシングルセッション マシン（仮想マシン）を作成するデフォルトの組織単位 (OU)、およびテナントがそれらの仮想マシンを Active Directory ドメインに参加させるために使用できるドメイン参加サービス アカウントの認証情報を指定します。このような仮想マシンには、インポートされた仮想マシン、ファーム RDSH インスタンス、および VDI デスクトップ インスタンスなどが含まれます。テナントでそのドメイン参加アカウントに必要なものについては、ドメイン参加アカウント - 必須の特性を参照してください。

   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、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、これを選択し、後でこの同じテナントに Horizon Cloud ポッド デプロイを追加し、そのポッドが同じ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ありません。

4 ワークフローの最後の [管理者の追加] の手順では、Active Directory ドメイン グループに Horizon Cloud スーパー管理者ロールを割り当てます。

5 管理者情報を保存すると、コンソールから自動的にログアウトされます。この手順により、前の手順で特定したドメイン グループの管理者のみがコンソールの管理機能にアクセスできるようになります。

1 つの Active Directory ドメインのワークフローが完了したら、組織のニーズに応じて、後で追加の Active Directory ドメインを構成できます。

重要な考慮事項

- コンソール内の他のページに移動するには、少なくとも 1 つのドメインでこのワークフロー全体を完了する必要があります。これらのタスクを完了しないと、主要なサービスを利用できません。
- コンソールの機能をサポートするには、スーパー管理者ロールを Active Directory ドメイン グループに割り当てるワークフロー手順を完了する必要があります。この手順を完了する前にウィザードをキャンセルした場合は、コンソールの [はじめに] ページで [構成] ボタンをクリックして Active Directory の登録ウィザードを再度開き、そのロールの割り当てを完了します。

- v2202 サービス リリース以降では、LDAPS の使用が Horizon Cloud on Microsoft Azure デプロイ環境でサポートされます。これを使用するためには、テナントを明示的に有効にし、テナントの最初のポッドと後続のポッドで v2201 リリース マニフェスト レベルを実行する必要があります。詳細については、Horizon Cloud on Microsoft Azure - LDAPS (LDAP Over SSL) 用に構成された Active Directory 環境の使用を参照してください。
- 配布グループは、セキュリティ グループにネストされていてもサポートされません。Active Directory グループを作成するときは、常に [グループ タイプ] に [セキュリティ] を選択します。
- プライマリ ドメイン バインド アカウントおよび補助ドメイン バインド アカウントには、常にスーパー管理者ロールが割り当てられます。これにより、コンソールで管理アクションを実行するためのすべての権限が付与されます。スーパー管理者権限を必要としないユーザーは、管理者が指定したドメイン バインド アカウントにアクセスできないようにする必要があります。
- Active Directory サーバのクロック スキューが 4 分未満であることを確認します。マニフェスト 2474.x 以降では、システムは登録された Active Directory サーバのクロック スキューが 4 分未満かどうかをチェックします。このスキューが 4 分を超えると、「クロック スキューが大きすぎます」という例外が発生し、システムのドメイン サーバの検出に失敗します。システムのドメイン サーバの検出に失敗すると、エンド ユーザーのデスクトップ接続要求が影響を受ける可能性があります。
- 今後の検討のために、後でこのテナントのポッド フリートに追加のポッド デプロイを追加する予定の場合、これらのポッドを接続またはデプロイするときに、これらのポッドはこの同じ Active Directory ドメインを認識できる必要があることに注意してください。
- また、既知の問題により、Horizon Cloud Connector を使用して Horizon ポッドを接続するときに、この最初のポッドの Active Directory ドメイン登録プロセスを完了せずに後続のポッドでコネクタのクラウド ペアリング ワークフローを実行しようとすると、予期しない結果が発生する可能性があります。クラウド ペアリング ワークフローは、Horizon Cloud への最初の Active Directory ドメイン登録を完了する前に複数のポッドに対して実行することができますが、最初のドメイン登録を完了する前に次のポッドでそのクラウド ペアリング プロセスを実行しようとすると、このドメイン登録プロセスが失敗することがあります。その場合、まず、Horizon Cloud Connector 構成ポータルで [接続解除] を使用し、クラウド接続されたポッドが 1 つになるまでそれらのクラウド接続された各ポッド間の接続を解除します。次に、失敗した Active Directory の登録を削除し、そのクラウド接続された単一のポッドのドメイン登録プロセスを完了してから、後続のポッドで Horizon Cloud Connector ワークフローを再実行します。

コンソールでワークフローを実行する前に

- 最初のポッドが正常にデプロイされていることを確認します。コンソールの [はじめに] ウィザードでは、最初のポッドが正常にデプロイされたことを緑色のチェックマーク アイコン ( ) で示します。
- 登録しているドメインの Active Directory ドメインの NetBIOS 名と DNS ドメイン名を取得します。これらの値は、このワークフローの最初のステップでコンソールの [Active Directory の登録] ウィンドウに入力します。これらの値を特定する方法の例については、Horizon Cloud の Active Directory の登録ワークフローの NETBIOS 名と DNS ドメイン名のフィールドに必要な情報の検索を参照してください。ドメイン名なしのユーザー ログイン名（`ouraccountname` など）のように、アカウント名自体をフィールドに入力することに注意してください。

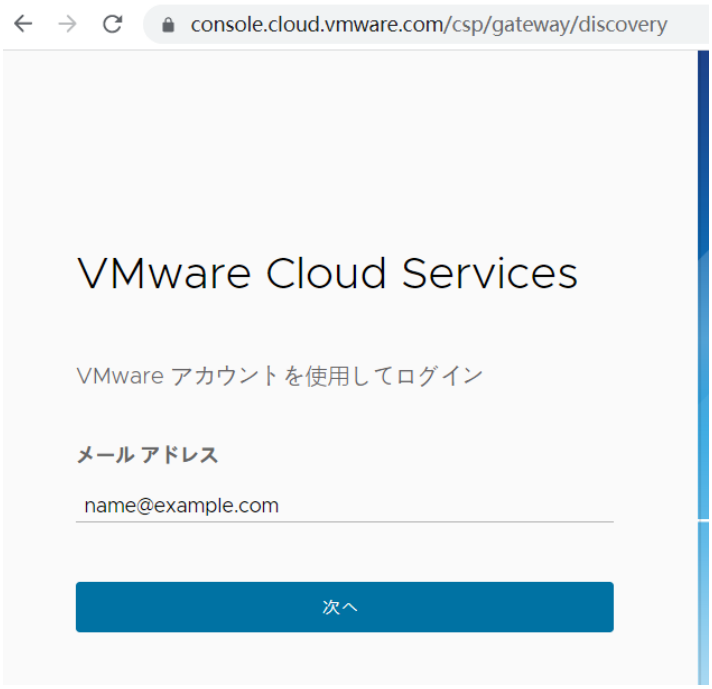
- 必須のプライマリ ドメイン バインド アカウントと補助ドメイン バインド アカウント、およびドメイン参加アカウントの、コンソールの必須フィールドに入力する準備ができている有効な情報を取得します。これらのアカウントがドメインに存在し、Horizon Cloud の運用に必要なサービス アカウントに記載されている要件を遵守していることを確認します。コンソールのワークフローの一部として、サービスは入力されたアカウント情報を検証します。
- ドメイン参加アカウントの手順が失敗しないようにするには、Active Directory インフラストラクチャが正確な時間のソースと同期していることを確認します。失敗した場合は、VMware のサポートに問い合わせる必要があります。[ドメイン バインド] 手順は成功したが、ドメイン参加の手順に失敗した場合、ドメインをリセットし、時間のソースを調整する必要があるかどうかを確認してみてください。ドメインをリセットするには、Active Directory ドメイン登録の削除の手順を参照してください。

注： テナントの最初のポッド デプロイが Horizon Connection Server および Horizon Cloud Connector デプロイ タイプで、このワークフローの実行中に問題が発生する場合は、デプロイでサポートされているバージョンの Horizon Connection Server および Horizon Cloud Connector が実行されていることを確認してください。

ログインしてワークフローを開始する

1 https://cloud.horizon.vmware.com/ の Horizon Universal Console ポータル URL に移動して、コンソールにログインします。

この URL は、以下のスクリーンショットに示すように、VMware Cloud Services ログイン画面にリダイレクトされます。Horizon Cloud テナントに関連付けられている認証情報を使用してログインします。画面に表示されるフローに従います。



これまでにこれらの認証情報を使用してサービス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サービスの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、コンソールが開き、[はじめに] ページが表示されます。

2　[はじめに] ページで、[全般的なセットアップ] セクションがまだ展開されていない場合は展開します。

3　[Active Directory] で [構成] をクリックします。

コンソールに、Active Directory 登録ワークフローの開始ウィンドウが表示されます。このウィンドウの外観は、テナントが Horizon Connection Server タイプのポッドで開始するのか、Horizon Cloud on Microsoft Azure のデプロイで開始するのかによって異なります。

ドメイン バインド - Horizon Connection Server ポッド

コンソール ウィンドウで必要な情報を入力し、[ドメイン バインド] をクリックして保存します。各バインド アカウント名を入力する場合は、ドメイン名を含まないアカウント名（`ouraccountname` のようなユーザー ログイン名など）を入力します。

表 1-1. Horizon ポッド - [Active Directory の登録] フィールド

フィールド	説明
[NETBIOS 名]	Horizon ポッドが認識できるすべての Active Directory ドメインの名前が入力された選択メニューが表示されます。最初に登録する Active Directory ドメインを選択します。
[DNS ドメイン名]	読み取り専用。コンソールに、[NETBIOS 名] で選択した Active Directory ドメインの完全修飾 DNS ドメイン名が自動的に表示されます。
[プロトコル]	このポッド タイプでサポートされているプロトコルである `LDAP` が自動的に表示されます。
[バインド ユーザー名] と [バインド パスワード]	選択したドメインで使用するサービスのドメイン バインド サービス アカウントの認証情報を指定します。
[補助アカウント #1]	[バインド ユーザー名] と [バインド パスワード] フィールドに、補助 LDAP バインド アカウントとして使用するドメイン内のユーザー アカウントとそれに関連するパスワードを入力します。
[詳細プロパティ]	デフォルトを変更しない限り、サービスはコンソールに表示されるデフォルト値を使用します。 ■ [ポート] : デフォルトで 389 （デフォルトの LDAP ポート）に設定されています。ドメインが標準以外の LDAP ポートを使用している場合を除き、この値を保持します。 ■ [ドメイン コントローラの IP アドレス] : この Active Directory ドメインへのテナントのトラフィックで特定のドメイン コントローラを使用する場合は、優先ドメイン コントローラの IP アドレスをカンマで区切って入力します。このテキスト ボックスを空のままにしておくと、サービスではこの Active Directory ドメインに使用可能なドメイン コントローラが使用されます。 ■ [コンテキスト] : DNS ドメイン名に関連する LDAP 命名コンテキスト。このテキスト ボックスは、サービスが [NetBIOS 名] のドメインから抽出した情報に基づいて自動入力され、[DNS ドメイン名] フィールドに自動的に表示されます。

ドメイン バインド：Horizon Cloud on Microsoft Azure デプロイ

コンソール ウィンドウで必要な情報を入力し、[ドメイン バインド] をクリックして保存します。各バインド アカウント名を入力する場合は、ドメイン名を含まないアカウント名（`ouraccountname` のようなユーザー ログイン名など）を入力します。

表 1-2. Horizon Cloud ポッド - [Active Directory の登録] フィールド

フィールド	説明
[NETBIOS 名]	テキスト ボックスが表示されます。ポッドが認識できる Active Directory ドメインの NetBIOS 名を入力します。通常、この名前にはピリオドは含まれません。Active Directory ドメイン環境から使用する値を見つける方法の例については、Horizon Cloud の Active Directory の登録ワークフローの NETBIOS 名と DNS ドメイン名のフィールドに必要な情報の検索を参照してください。
[DNS ドメイン名]	[NETBIOS 名] に指定した Active Directory ドメインの完全修飾 DNS ドメイン名を入力します。
[プロトコル]	このポッド タイプでサポートされているプロトコルである `LDAP` が自動的に表示されます。
[バインド ユーザー名] と [バインド パスワード]	選択したドメインで使用するサービスのドメイン バインド サービス アカウントの認証情報を指定します。
[補助アカウント #1]	[バインド ユーザー名] と [バインド パスワード] フィールドに、補助 LDAP バインド アカウントとして使用するドメイン内のユーザー アカウントとそれに関連するパスワードを入力します。
[詳細プロパティ]	任意。デフォルトを変更しない限り、サービスはコンソールに表示されるデフォルト値を使用します。 ■ [ポート]：デフォルトで 389 （デフォルトの LDAP ポート）に設定されています。ドメインが標準以外の LDAP ポートを使用している場合を除き、この値を保持します。 ■ [ドメイン コントローラの IP アドレス]：この Active Directory ドメインへのテナントのトラフィックで特定のドメイン コントローラを使用する場合は、優先ドメイン コントローラの IP アドレスをカンマで区切って入力します。このテキスト ボックスを空のままにしておくと、サービスではこの Active Directory ドメインに使用可能なドメイン コントローラが使用されます。 ■ [コンテキスト]：DNS ドメイン名に関連する LDAP 命名コンテキスト。このテキスト ボックスは、サービスがドメインの [DNS ドメイン名] フィールドから抽出した情報に基づいて自動入力されます。

次のスクリーン ショットは、Microsoft Azure が、最初のクラウドに接続されたポッドの場合、[Active Directory の登録] ウィンドウを示しています。フィールドには、`ENAUTO` の NetBIOS 名と `ENAUTO.com` の DNS ドメイン名の例 Active Directory ドメインの値があります。

ドメイン参加

ドメイン バインドの手順が成功すると、コンソールに [ドメイン参加] ダイアログ ボックスが自動的に表示されます。アカウントの認証情報には、前提条件に説明されているドメイン参加アカウントのガイドラインに準拠した Active Directory アカウントを使用します。

ベスト プラクティスは、このウィザード手順の必須フィールドに入力することです。このリリースでは、ドメイン参加アカウントは主に Microsoft Azure のポッドにある仮想マシンを含むシステム操作に使用されますが、この手順を完了すると、コンソールから、スーパー管理者ロールを付与する次の手順を完了するように求められます。

重要： ドメイン バインドの手順が失敗し、そのままドメイン参加アカウントの追加を続行してシステムがスーパー管理者ロールの手順に進んだ場合、システムが次のステップに進んだとしても登録プロセスは完了しません。この状況が発生した場合、Active Directory ドメイン登録の削除の手順を実施した後に、ドメイン バインドのフローを再度開始します。

1 [ドメイン参加] ダイアログ ボックスで、必須の情報を入力します。

オプション	説明
[プライマリ DNS サーバ IP アドレス]	Horizon Cloud でマシン名の解決に使用するプライマリ DNS サーバの IP アドレス。 Microsoft Azure のポッドの場合、この DNS サーバは、Microsoft Azure クラウド内のマシン名、および外部名を解決できる必要があります。
[セカンダリ DNS サーバ IP アドレス]	（オプション）セカンダリ DNS サーバの IP アドレス

オプション	説明
[デフォルト OU]	インポートされた仮想マシン、ファーム RDSH 仮想マシン、VDI デスクトップ インスタンスなど、ポッドのデスクトップ関連の仮想マシンで使用する Active Directory 組織単位 (OU)。Active Directory OU の形式は、`OU=NestedOrgName, OU=RootOrgName,DC=DomainComponent` のようになります。システム デフォルトは `CN=Computers` です。`CN=myexample` など、必要に応じてデフォルトを変更できます。 **注：** ネストされた組織の名前の説明については、ネストされた Active Directory ドメイン組織単位の使用についての考慮事項を参照してください。入力した個々の OU は、`OU=` の入力部分を除いて 64 文字以内の長さでなければなりません。Microsoft は、個々の OU を 64 文字以内に制限します。64 文字を超える OU パスは、個々の OU が 64 文字を超えていなければ、有効です。ただし、個々の OU はそれぞれ 64 文字以内である必要があります。
[参加ユーザー名] と [参加パスワード]	その Active Directory ドメインにコンピュータを参加させる権限を持つ Active Directory のユーザー アカウント。ユーザー名と関連するパスワードを入力します。 **注：** ユーザー名のみを指定します。ここにドメイン名を含めないでください。
[補助参加ユーザー名] と [補助参加パスワード]	任意。補助ドメイン参加アカウントを指定します。 指定したプライマリ ドメイン参加アカウントにアクセスできない場合、システムは、Microsoft Azure のポッドで、イメージ仮想マシンのインポート、ファーム RDSH インスタンスの作成、VDI デスクトップ インスタンスの作成など、ドメインに参加する必要がある操作に対して補助ドメイン参加アカウントを使用します。 前提条件に説明されているプライマリ ドメイン参加アカウントの同じガイドラインに準拠した Active Directory アカウントを使用します。両方のアカウントに [Never Expires (有効期限なし)] が設定されている場合を除き、この補助ドメイン参加アカウントの有効期限はプライマリ ドメイン参加アカウントとは異なることを確認します。プライマリおよび補助ドメイン参加アカウントの両方の有効期限が同時に切れる場合、ファーム RDSH 仮想マシンと VDI デスクトップ仮想マシンのプロビジョニングやイメージのシーリングにおけるシステム動作が失敗します。 この時点で補助ドメイン参加アカウントを追加しない場合、後で追加することができます。ここで追加した場合は、後で更新または削除できます。追加できる補助ドメイン参加アカウントは 1 つのみです。

2 [保存] をクリックします。

ドメイン参加の手順が成功すると、[管理者の追加] ダイアログ ボックスが表示されます。この手順を続行して、Active Directory ドメインの管理者グループにスーパー管理者ロールを追加する必要があります。

重要： ドメイン参加の手順が失敗した場合、登録プロセスは完了していません。この状況が発生した場合、Active Directory ドメイン登録の削除の手順を実施した後に、手順 4 を再度実行します。

Active Directory グループへのスーパー管理者ロールの追加

1 [管理者の追加] ダイアログ ボックスで、Active Directory 検索機能を使用し、このコンソールを使用して環境で管理アクションを実行する Active Directory 管理者グループを選択します。この顧客アカウントの Active Directory ドメインが設定されたので、この割り当てにより、少なくとも 1 つの Active Directory ドメインのユーザー アカウントに対して、このコンソールにログインするための権限が付与されます。

2 [保存] をクリックします。

[保存] をクリックすると、システムによって自動的にログアウトされます。ポッドを Active Directory ドメインに登録したので、システムはログインし直すことを要求します。これにより、VMware アカウントの認証情報とともに Active Directory アカウントの使用が強制されます。たとえば、この場合、VMware アカウントの認証情報を使用してログインし、次にスーパー管理者ロールを割り当てた Active Directory グループ内のユーザーの Active Directory アカウントの認証情報を使用してログインします。

重要： Active Directory グループをスーパー管理者ロールに割り当てた後は、Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるで説明するように、このスーパー管理者ロールに別の管理者グループを追加していない限り、指定した管理者グループを Active Directory システムから削除したり、Active Directory システムに表示される GUID を変更したりしないでください。このスーパー管理者ロールは、どの Active Directory ユーザー アカウントが Horizon Cloud テナント アカウントにログインしてコンソールで管理操作を実行できるかを管理します。Active Directory システムからグループを削除したり、Active Directory システム内でその GUID を変更したりしても、その変更は Horizon Cloud 制御プレーンに伝達されないため、Horizon Cloud はスーパー管理者の役割を持つ Active Directory グループを正しく認識できなくなります。そのグループがこのスーパー管理者ロールに割り当てられた唯一のグループである場合、以前はスーパー管理者のアクセス権を持っていた Active Directory アカウントは、管理操作を実行するためのアクセス権を持つ Horizon Cloud テナント アカウントにログインできなくなります。その時点で、ログインしてスーパー管理者ロールにグループを追加するために使用できるのは、ドメイン バインド アカウントと補助ドメイン バインド アカウントの認証情報のみです。

プロセス完了の結果

ウィザードのすべての手順が完了すると、次の項目が配置されます。

- Active Directory ドメインは、この Horizon Cloud 顧客アカウントに関連付けられた最初のクラウド構成の Active Directory ドメインとしてクラウド プレーンに構成されます。
- Horizon Cloud には、Horizon Cloud ポッドに仮想マシンをドメインに参加させるシステム操作に必要なドメイン参加アカウントがあります。
- コンソールでの管理アクティビティにアクセス可能になりました。
- Horizon Cloud テナントには最初に登録された Active Directory ドメインが含まれるようになり、コンソールにログインするときのログイン フローが変更されました。ログイン フローの概要については、Horizon Cloud テナント環境への認証についてを参照してください。
- スーパー管理者ロールが付与されたグループ内のユーザーは、関連付けられた VMware アカウントの認証情報を使用してログインすると、コンソールにアクセスして管理アクティビティを実行できます。これらの管理者が自分の VMware アカウントの認証情報を使用して Horizon Cloud で認証できるようにするには、Horizon Cloud テナント環境にログインし、Horizon Universal Console を使用してアクションを実行するための管理者ロールを組織内の個人に付与するで説明する手順を実行します。
- 登録された Active Directory ドメインからのユーザー アカウントは、Microsoft Azure のポッドからのリソースを含む割り当てに対して選択できます。
- コンソールのヘルプ デスク機能は、その登録された Active Directory ドメインのユーザー アカウントで使用できます。

次の手順

この時点から、通常は次のタスクを実行します。

- 追加の補助バインド アカウントをこの Active Directory ドメイン構成に追加します。指定したプライマリおよび最初のバインド アカウントがアクセス不可になった場合、システムでは次の補助バインド アカウントを使用して Active Directory に接続します。プライマリ バインド アカウントが Active Directory ドメインでアクセス不可になった場合に、補助バインド アカウントを持つことにより、管理者ユーザーがコンソールからロックアウトされないようになります。Horizon Cloud のクラウド構成の Active Directory ドメイン用に補助バインド アカウントを追加するを参照してください。
- 環境を管理する追加ユーザーにアクセス権限を付与します。まず関連付けられた Horizon Cloud ロールがある VMware アカウントを追加してから、それらの Active Directory アカウントに適切な Horizon Cloud ロールを付与します。Horizon Cloud テナント環境にログインし、Horizon Universal Console を使用してアクションを実行するための管理者ロールを組織内の個人に付与するおよび Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるを参照してください。
- [はじめに] ウィザードの手順を続行します。Horizon Cloud の [はじめに] ウィザード - 概要を参照してください。
- コンソールのダッシュボードおよびその他の領域に移動して、他の管理タスクを確認または実行します。第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアーを参照してください。
- コンソールへの管理アクセス権限を付与するユーザー、または割り当てを提供するエンド ユーザーがいる追加の Active Directory ドメインがある場合、これらの Active Directory ドメインも登録できます。追加の Active Directory ドメインをクラウド構成の Active Directory ドメインとして Horizon Cloud テナント環境に登録するを参照してください。
- コンソールへの読み取り専用アクセス権限を付与するこのドメイン内のユーザーにデモ管理者ロールを割り当てます。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 プラクティスおよび Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対してコンソールのどの部分を有効にするかを制御するロールをそのグループに割り当てるを参照してください。

注意： スーパー管理者ロールが割り当てられた Active Directory グループが 1 つしかない場合は、そのグループを Active Directory サーバから削除しないでください。これを行うと、以降のログインで問題が発生する可能性があります。

Horizon Cloud の運用に必要なサービス アカウント

Horizon Cloud は、Active Directory (AD) ドメイン内の 2 つのアカウントをサービス アカウントとして使用する必要があります。このトピックでは、これら 2 つのアカウントが満たす必要がある要件について説明します。

Horizon Cloud では、これらの 2 つのサービス アカウントとして使用する 2 つの AD アカウントを指定する必要があります。

- AD ドメイン内の検索を実行するために使用するドメイン バインド アカウント。

- コンピュータ アカウントをドメインに参加させ、Sysprep 処理を実行するために使用するドメイン参加アカウント。

  注： Microsoft Azure のポッドの場合、システムは Microsoft Azure Marketplace からのイメージのインポート、ファーム RDSH インスタンスの作成、VDI デスクトップ インスタンスの作成など、仮想マシンをドメインに参加させる必要のあるポッド操作でこのドメイン参加アカウントを使用します。

これらのサービス アカウントに指定する Active Directory アカウントは、Horizon Cloud の次の動作要件を満たす必要があります。最初のポッドのテナントへのオンボーディングを行った後、クラウドベースの管理コンソールを使用して、これらのアカウントの認証情報を入力します。

重要：

- これらのサービス アカウントは、Horizon Cloud Active Directory ドメイン登録の構成のみで使用してください。これらのサービス アカウントを他の構成で再利用すると、予期しない結果が発生する可能性があります。たとえば、Workspace ONE Access Connector の構成設定では、同じドメイン バインド アカウントを使用しないでください。さもないと、ドメイン バインド アカウントに関する予期しない通知が Horizon Universal Console に表示されることがあります。
- ここに記述されているとおりに、OU およびオブジェクトのうちユーザーが使用するものや、システムが使用することが予想されるものはすべて、ドメイン バインドやドメイン参加アカウントに引き続き権限が付与されていることを確認する必要があります。Horizon Cloud には、環境においてどの Active Directory グループが使用されるかを事前設定したり、予測する機能はありません。コンソールを使用して、ドメイン バインド アカウントとドメイン参加アカウントを Horizon Cloud に構成する必要があります。

注意： すべての権限を個別に設定する代わりに、アカウントに対してフル コントロールを設定することもできますが、権限を個別に設定することを推奨します。

ドメイン バインド アカウント - 必須の特性

- ドメイン バインド アカウントは、期限切れにしたり、変更やロックアウトをすることができません。このタイプのアカウント設定を使用する必要があります。これは、システムでは Active Directory を問い合わせるためにプライマリ ドメイン バインド アカウントがサービス アカウントとして使用されるためです。何らかの理由でプライマリ ドメイン バインド アカウントにアクセスできない場合、システムは補助ドメイン バインド アカウントを使用します。プライマリ/補助の両方のドメイン バインド アカウントが期限切れかアクセス不能になると、クラウドベースのコンソールにログインして設定を更新することができません。

  重要： プライマリ/補助の両方のドメイン バインド アカウントが期限切れかアクセス不能になると、コンソールにログインして設定を有効なドメイン バインド アカウント情報に更新することができません。プライマリまたは補助ドメイン バインド アカウントで [Never Expires（有効期限なし）] を設定しない場合、両方に異なる有効期限を設定する必要があります。有効期限が近くなったら常に追跡しながら、有効期限の時刻に達する前に Horizon Cloud ドメイン バインド アカウント情報を更新する必要があります。

- ドメイン バインド アカウントには、sAMAccountName 属性が必要です。sAMAccountName 属性は 20 文字以下にする必要があります。また、次の文字を含めることはできません。"/\ []:; |= , + * ?< >

- ドメイン バインド アカウントには常にスーパー管理者ロールが割り当てられます。これにより、コンソールで管理アクションを実行するためのすべての権限が付与されます。スーパー管理者権限を付与しないユーザーは、ドメイン バインド アカウントにアクセスできないようにする必要があります。コンソールで使用されるロールの詳細については、Horizon Universal Console 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。

ドメイン バインド アカウント - 必須の Active Directory 権限

ドメイン バインド アカウントには読み取り権限が付与されている必要があります。Horizon Cloud のサービスとしてのデスクトップ操作でエンド ユーザーへのデスクトップ仮想マシンの割り当てなどの操作を行う際など、AD 組織単位 (OU) の AD アカウントをすべて検索できる機能を使用されることが想定されます。ドメイン バインド アカウントには、Active Directory からオブジェクトを列挙する機能が必要です。ドメイン バインド アカウントには、Horizon Cloud での使用が予想されるすべての OU およびオブジェクトに対する次の権限が必要です。

- コンテンツの一覧表示
- すべてのプロパティの読み取り
- アクセス許可の読み取り
- tokenGroupsGlobalAndUniversal の読み取り（[すべてのプロパティの読み取り] 権限により暗黙に含まれる）

重要： 一般的に、ドメイン バインド アカウントには、Microsoft Active Directory デプロイで認証されたユーザーに通常付与される、設定済みのデフォルトの読み取りアクセス関連の権限が付与されている必要があります。標準の Microsoft Active Directory デプロイでは、Authenticated Users に通常付与されるデフォルト設定により、標準ドメイン ユーザー アカウントは、Horizon Cloud がドメイン バインド アカウントに必要な列挙を行うことができます。ただし、組織の Active Directory 管理者が通常ユーザーの読み取りアクセス権に関連する権限をロックダウンすることを選択した場合は、それらの Active Directory 管理者に、Horizon Cloud に使用するドメイン バインド アカウントの認証済みユーザーの標準デフォルト設定を保持するように要求する必要があります。

ドメイン参加アカウント - 必須の特性

- ドメイン参加アカウントを変更またはロックアウトすることはできません。
- アカウントのユーザー名に空白を含めることはできません。名前に空白が含まれている場合、そのアカウントに依存するシステム操作で予期しない結果が発生します。
- ドメイン参加アカウントには、sAMAccountName 属性が必要です。sAMAccountName 属性は 20 文字以下にする必要があります。また、次の文字を含めることはできません。"/\ [];: |= , + * ?< >
- 次の条件のうち、少なくとも 1 つを満たしている必要があります。
  - Active Directory で、ドメイン参加アカウントを [Never Expires（有効期限なし）] に設定します。

- または、最初のドメイン参加アカウントと有効期限の異なる補助ドメイン参加アカウントを構成します。この方法を選択する場合は、補助ドメイン参加アカウントが、コンソールに設定するメインのドメイン参加アカウントと同じ要件を満たしていることを確認します。

注意： ドメイン参加アカウントの有効期限が切れ、有効な補助ドメイン参加アカウントが構成されていない場合、Horizon Cloud はイメージのシーリングとファーム RDSH の仮想マシンおよび VDI デスクトップ仮想マシンのプロビジョニングに失敗します。

重要： テナントに 1600.0 より古いマニフェストを実行している Microsoft Azure の Horizon Cloud ポッドがある場合は、ドメインの登録時に入力するドメイン参加アカウントが、Horizon Cloud スーパー管理者ロールを割り当てる Active Directory グループの 1 つにも属していることを確認する必要があります。これらの古いマニフェスト バージョンを実行しているポッドでのシステムの操作は、Horizon Cloud スーパー管理者ロールによって付与された権限を持つドメイン参加アカウントに依存します。グループにロールを割り当てる方法の説明については、Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるを参照してください。

ドメイン参加アカウント - 必須の Active Directory 権限

ドメイン参加アカウントは、テナント レベルで構成されます。テナントのフリート内のすべてのポッドで、ドメイン参加関連のすべての操作のために、Active Directory 登録で構成されている同じドメイン参加アカウントがシステムによって使用されます。

システムは、ファームと VDI デスクトップ割り当ての [コンピュータの組織単位 (OU)] テキスト ボックスが Active Directory 登録のデフォルトの OU と異なる場合、Active Directory 登録ワークフロー（そのワークフローの [デフォルトの組織単位 (OU)] テキスト ボックス）で指定する OU 内、および作成するファームおよび VDI デスクトップ割り当てで指定する OU 内のドメイン参加アカウントに対する明示的な権限チェックを実行します。

下位の OU を使用するケースにも対応するため、ベスト プラクティスとして、これらの必須のアクセス権限をコンピュータの組織単位のすべての子孫オブジェクトに適用するように設定します。

重要：

- ここに挙げる AD 権限の一部は通常、Active Directory により、デフォルトで アカウントに割り当てられます。ただし、Active Directory のセキュリティ許可を制限している場合、Horizon Cloud で使用すると予想されるすべての OU およびオブジェクトの権限についての記述を、ドメイン バインド アカウントが必ず読むようにする必要があります。
- Microsoft Active Directory では、新しい組織単位 (OU) を作成するときに、システムは、新しく作成された OU およびすべての子孫オブジェクトの [すべての子オブジェクトの削除] 権限に `Deny` を適用する `Prevent Accidental Deletion` 属性を自動的に設定する場合があります。その結果、ドメイン参加アカウントに [コンピュータ オブジェクトの削除] 権限を明示的に割り当てた場合、新しく作成された OU の場合、Active Directory は、明示的に割り当てられた [コンピュータ オブジェクトの削除] 権限に上書きを適用した可能性があります。[誤削除の防止] フラグをオフにしても、Active Directory が [すべての子オブジェクトの削除] 権限に適用した `Deny` が自動的にオフにならない場合があるため、新しく追加された OU の場合、Horizon 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。

ヒント： 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必須の Active Directory 権限のセットが以前のセットよりも少なくなり、テナントの柔軟性が向上しています。ただし、ドメイン参加アカウントはテナント レベルで構成されているため、システムは、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において同じドメイン参加アカウントを使用します。このため、フリートに 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、ドメイン参加アカウントに、これらのポッドに必要な以前の権限セットが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。

表 1-3. Microsoft Azure のすべての Horizon ポッドがマニフェスト 2474.0 以降を実行している場合

アクセス	適用先
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

表 1-4. 2474.0 以前のマニフェストを実行している Microsoft Azure の Horizon ポッドがある場合

アクセス	適用先
コンテンツの一覧表示	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読み取り	このオブジェクトとすべての子孫オブジェクト

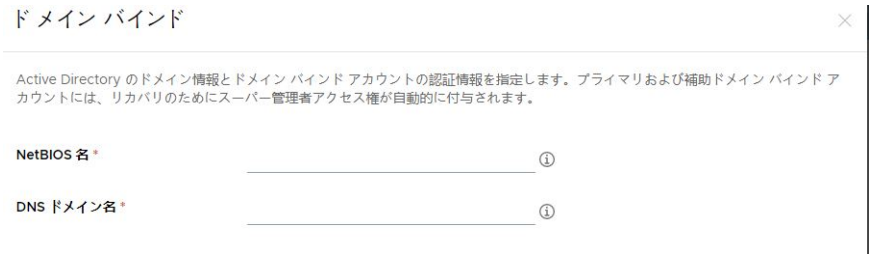
表 1-4. 2474.0 以前のマニフェストを実行している Microsoft Azure の Horizon ポッドがある場合 （続き）

アクセス	適用先
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	すべての子孫オブジェクト
アクセス許可の読み取り	このオブジェクトとすべての子孫オブジェクト
パスワードのリセット	子孫コンピュータ オブジェクト

Horizon Cloud の Active Directory の登録ワークフローの NETBIOS 名と DNS ドメイン名のフィールドに必要な情報の検索

このトピックでは、[NETBIOS 名] および [DNS ドメイン名] の各フィールドに必要な情報を見つける方法の例を示します。これらのフィールドは Horizon Cloud 環境に Active Directory ドメインを登録するためのワークフローで必要です。

Active Directory ドメイン登録のワークフローを開始すると、コンソールに [Active Directory の登録] ウィンドウが表示されます。次のスクリーンショットはウィンドウの上部を示したものです。



[NETBIOS 名] および [DNS ドメイン名] フィールドに必要な情報は Active Directory ドメイン環境から取得できます。一般的な Active Directory ドメイン環境では、NetBIOS 名は、Active Directory 管理ツールのインターフェイスを介して [ドメイン名（Windows 2000 以前）] フィールドに表示されます（たとえば、Microsoft Management Console (MMC) への Active Directory ユーザーおよびコンピュータのスナップインを使用したときなど）。同じスナップインから DNS ドメイン名を取得することもできます。

このトピックでは、Active Directory ユーザーとコンピュータ MMC スナップインを使用して必要な情報を見つけるための 1 つの方法について説明します。スナップインが Active Directory ドメイン サービスまたはリモート サーバ管理ツールがインストールされている Microsoft Windows サーバにインストールされている場合は、`dsa.msc` を実行してスナップインを開くことができます。

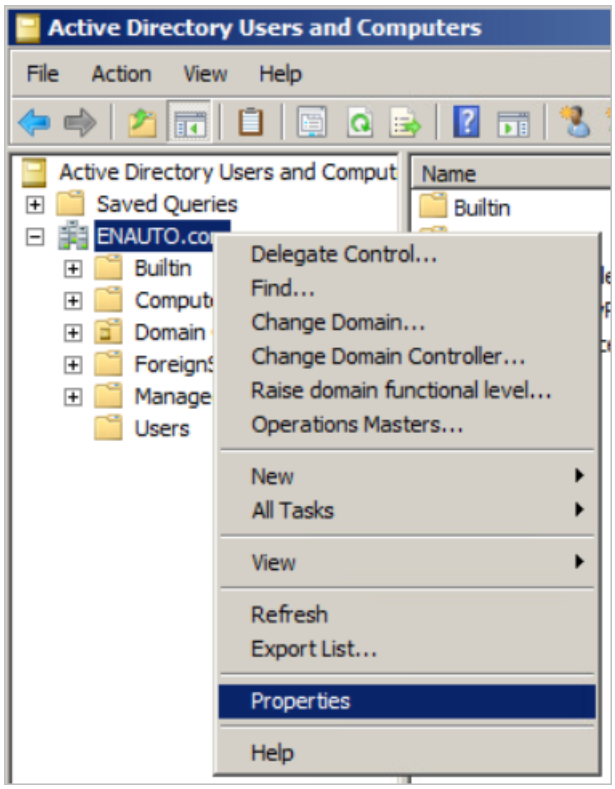
手順

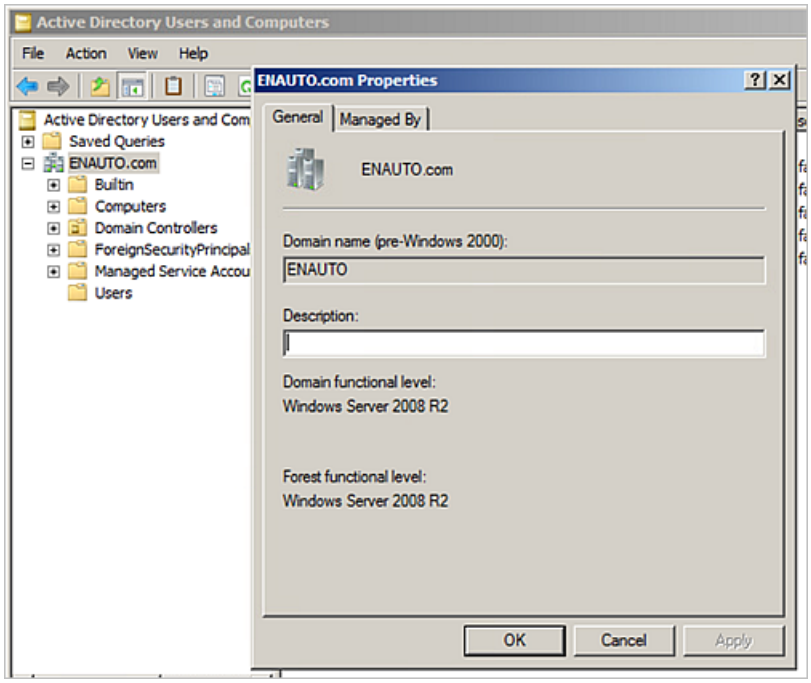
1 [Active Directory ユーザーとコンピュータの設定] ウィンドウを開き、ドメイン構成を確認します。

次のスクリーンショットは、DNS ドメイン名が `ENAUTO.com` の Active Directory ドメインのウィンドウの例です。

2 ドメイン名のアイコンを右クリックし、[プロパティ] をクリックしてドメインのプロパティを表示します。

次のスクリーンショットで例を示します。

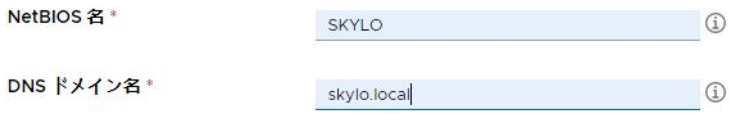




ドメインの NetBIOS 名は、[ドメイン名（Windows 2000 以前)]フィールド内の名前です。通常、この名前にはピリオド (.) は含まれません。この名前は、[Active Directory の登録] ウィンドウの [NETBIOS 名] フィールドに入力します。

プロパティ名の上部にある名前は、ドメインの完全な DNS 名です。通常、この名前には `ENAUTO.com` のようにピリオドが使用されています。この完全な DNS 名は、[Active Directory の登録] ウィンドウの [DNS ドメイン名] フィールドに入力します。

次のスクリーンショットは、上記のスクリーンショットに表示されている ENAUTO.com というドメインの例を登録するときのコンソールの [Active Directory の登録] ウィンドウを示します。このドメインの NetBIOS 名は `ENAUTO` で、DNS ドメイン名は `ENAUTO.com` です。



Horizon Cloud on Microsoft Azure - LDAPS (LDAP Over SSL) 用に構成された Active Directory 環境の使用

このページでは、クラウド プレーン テナントで LDAPS 用に構成された Active Directory 環境を使用するためのサービスのサポートについて説明します。

サービス リリース 2201 以降では、サービスは LDAPS を使用するように構成された Active Directory (AD) ドメイン環境の使用をサポートします。この機能を使用するには、テナントを明示的に有効にする必要があります。また、ポッド フリートのポッドは、v2201 リリースのマニフェスト レベルを実行している Horizon Cloud ポッドのみで構成されている必要があります。この機能の有効化を要求するには、VMware の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。

この機能の概要

VDI 提供サービスとして、このサービスには、ドメイン バインド アカウントを使用して Active Directory ドメインで参照を実行する機能が必要です。Active Directory 環境が LDAPS 用に構成されている場合、サービスにはドメイン コントローラのルート CA 証明書と、必要に応じて中間 CA 証明書が必要です。Horizon Universal Console を使用して、証明書を収集し、システムに保存します。

サービスは、信頼済み CA 証明書をシステムに提供するために、自動検出と手動アップロードの 2 つの方法を提供します。これらの方法については、このページで詳しく説明します。

重要なポイントと要件

LDAPS 構成の Active Directory ドメインを登録する前に、次の重要なポイントと要件を確認してください。

- 自己署名証明書はサポートされていません。
- このサービスでは、LDAPS を使用するように構成されたドメインの SRV レコードが DNS に含まれている必要があります。ドメインに LDAPS を使用することを選択すると、SRV レコードの使用が暗黙的に指定されます。
- チャネルのバインドを強制するように Active Directory 環境を構成することが強く推奨されます。チャネル バインドの強制は、LDAPS を正しく保護するために（特に中間者攻撃 (MITM) を回避するために）不可欠です。
- サービスのドメイン登録ワークフローで、使用するサービスの優先ドメイン コントローラを指定する場合は、完全修飾 DNS ホスト名を使用して指定する必要があります。これらの優先ドメイン コントローラを Horizon Universal Console に入力すると、コンソールは IP アドレスの入力を防止します。ベスト プラクティスは、少なくとも 2 つの優先 DC を指定することです。
- コンソールのドメイン バインド ウィザードで優先 DC を指定しない場合、サービスが DNS を使用して検出する DC は、すべてのポッドからアクセス可能である必要があります。
- ファイアウォール構成では、次のポートとプロトコルを使用して、すべてのポッドからドメイン コントローラへの送信接続を許可する必要があります。
  - ポート 88/TCP：Kerberos 認証
  - ポート 636/TCP、3269/TCP：LDAPS 通信
- ルート証明書を除く、信頼チェーン内のすべての証明書に対して HTTP の失効エンドポイントが定義されている必要があり、そのエンドポイントは `HTTP` を介してポッドからアクセスできる必要があります。この要件には次のポイントが含まれています。
  - 失効エンドポイントには LDAP を使用できません。
  - サービスは、証明書に定義されている OCSP または CRL `HTTP` URL を使用して失効チェックを実行します。
  - 証明書で HTTP プロトコルの OCSP または CRL エンドポイントが定義されていない場合、サービスは失効チェックを実行できません。その場合、LDAPS 接続は失敗します。
  - すべてのポッドは、失効エンドポイントを認識できる必要があります。ファイアウォールは、デプロイされたポッドから `HTTP` を介して失効エンドポイントに向かう送信トラフィックをブロックすることはできません。

自動検出 - Microsoft CA

Microsoft CA を使用してドメイン コントローラ証明書を発行する場合、Horizon Universal Console は自動検出メカニズムを提供します。このメカニズムにより、Active Directory 環境からのすべてのルート証明書と中間証明書が自動的に検出され、システムでの使用の確認と承認のためにコンソールに表示されます。自動検出された証明書をすべて受け入れるか、まったく受け入れないかのいずれかを選択します。部分的な承認はサポートされていません。

コンソールで承認されると、システムは、同じフォレストのすべてのドメインで使用できるように、承認された証明書を保存します。1 つのドメインを使用して自動検出プロセスを実行し、そのドメインをサービスに登録して、後で同じフォレストから別のドメインを登録するときに、同じフォレストの以前のドメインがすでに登録されていても、コンソールに表示される自動検出された証明書を受け入れる必要があります。このフローは、新しいドメイン登録時に、フォレスト内に新しい証明書が作成されたかどうか、または以前のドメインを登録してから同じフォレストから次のドメインを登録するまでの間に証明書が削除されたかどうかを検出する方法を提供します。

コンソールは、この自動検出パスを次の場所で提供します。

- Active Directory ドメイン登録フローのドメイン バインド部分の [プロトコル] 手順。プロトコルに LDAPS が選択されている場合、[自動検出] 選択とボタンを使用して証明書を自動検出し、証明書の使用を承認することができます。
- [Active Directory 証明書] ページの、[設定] - [Active Directory 証明書] - [自動検出済み]。テナントに 1 つ以上の既存の登録済み Active Directory ドメインがある場合、コンソールはこのページを使用可能にします。このページには自動検出された証明書が表示されるため、どの証明書が承認されているかを確認したり、使用されていない証明書を削除してセットをクリーンアップしたりできます。

手動アップロード：Microsoft 以外の CA または Microsoft の CA

Microsoft 以外の CA を使用してドメイン コントローラ証明書を発行している場合、またはエンタープライズ CA をサポートしていない AADDS を使用している場合、Horizon Universal Console は、システムに CA 証明書を提供するための手動アップロード パスを提供します。この場合、コンソールを使用して、PEM でエンコードされたルート証明書と中間 CA 証明書を手動でアップロードする必要があります。

ご利用の環境で Microsoft CA を使用している場合でも、必要に応じて手動アップロードを選択できます。

`certutil` などのユーティリティを使用して、サードパーティ、Microsoft 以外の CA 証明書を Active Directory ドメインに公開している場合は、自動検出方法でこれらの CA 証明書を検出できます。

コンソールは、この手動アップロード パスを次の場所で提供します。

- Active Directory ドメイン登録フローのドメイン バインド部分の [プロトコル] 手順。プロトコルに LDAPS が選択されている場合、[アップロード] の選択とボタンを使用して証明書をアップロードできます。
- [Active Directory 証明書] ページの、[設定] - [Active Directory 証明書] - [アップロード済み]。テナントに 1 つ以上の既存の登録済み Active Directory ドメインがある場合、コンソールはこのページを使用可能にします。このページで、[アップロード] ボタンをクリックして各証明書をアップロードします。

失効チェック

サービスは、証明書で定義されている内容（OCSP または CRL の `http://` URL）を使用して、証明書の失効のチェックを実行します。サービスは OCSP によるチェックを優先します。エンドポイントにアクセスできない場合、サービスは CRL を使用して正常にチェックを試みます。

固定された OCSP 応答がサポートされます。

注意: 前述の「重要なポイントと要件」セクションで説明したように、CA は、`HTTP` を使用した OCSP または CRL のいずれか、またはその両方を使用するように構成する必要があります。この要件を満たしていない場合、サービス チェックは機能しません。

新規発行された CA 証明書 - ドメイン登録の更新が必要

新しい CA 証明書を発行する場合は、できるだけ早くシステムを更新して、新しく発行された CA 証明書を認識させる必要があります。次のいずれかの方法を使用して、CA 証明書をシステムに取り込みます。

ドメイン登録で手動アップロードを使用する場合

CA 証明書が新しく発行されたらすぐに、システムにアップロードする必要があります。[設定] - [Active Directory 証明書] - [アップロード済み] の順に移動し、[アップロード] を使用します。

ドメイン登録で自動検出が使用されている場合

この方法を使用すると、新しく発行された CA 証明書の存在が自動的に検出されます。システムは新しい CA 証明書を検出すると、通知を生成し、コンソールの標準通知表示とともに表示します。この通知は、新しい CA 証明書をシステムに保存する必要があることを通知するためのものです。ドメイン フォレストの場合、この通知はフォレスト内のすべてのドメインではなく、フォレストごとに 1 つのドメインに対して生成されます。1 つのドメインの登録を更新すると、すべてのフォレストのドメインに対するアクションが満たされるためです。

ドメイン登録を更新するには、コンソールのドメイン バインド ウィザードを起動し、ウィザードの [プロトコル] の手順で [自動検出] ボタンを使用して自動検出プロセスを繰り返します。

DC 証明書の有効期限が近い場合 - できるだけ早く修正

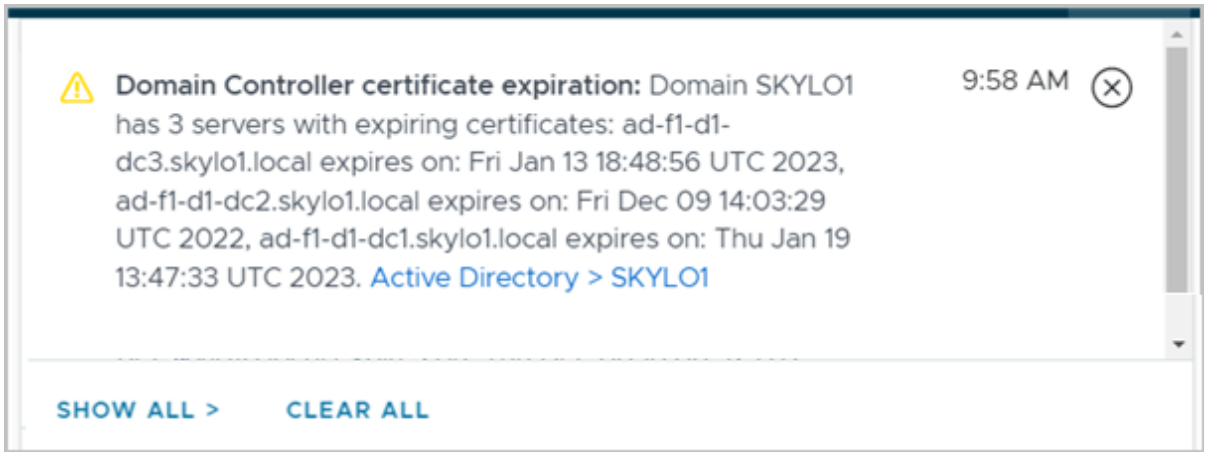
サービスがドメイン コントローラ (DC) 証明書の有効期限が近づいていることを検出すると、通知が作成され、コンソールの標準通知が表示されます。最初の通知は、有効期限の 21 日前に表示されます。

重要： VMware では、管理者がこれらの通知に対してできるだけ早くアクションを実行することを推奨しています。

- 有効期限が近づいている DC 証明書を再発行するための修正アクションを実行します。
- 修正アクションで新しい CA 証明書を発行する場合は、その CA を使用して新しい DC 証明書を発行する前に、新しい CA 証明書をシステムに保存する必要があります。新しい CA 証明書をシステムに保存する手順については、前のセクションを参照してください。

期限切れ間近の証明書通知の例

次のスクリーンショットは、これらの通知の 1 つを示しています。ドメイン フォレストの場合、この通知はフォレスト内のすべてのドメインではなく、フォレストごとに 1 つのドメインに対して生成されます。1 つのドメインを更新すると、すべてのフォレストのドメインに対するアクションが満たされるためです。ハイパーリンクをクリックすると、そのドメインの構成に移動し、そこからドメイン バインド ウィザードを開始できます。



LDAP と LDAPS の切り替えのサポート

テナントがこのページの上部に記載されているこの機能の基準を満たしている場合、1 つのプロトコルを使用して Active Directory ドメインを登録した後、コンソールを使用して既存のドメイン バインド構成を更新し、他のプロトコルに切り替えることができます。たとえば、LDAPS プロトコルを使用するようにドメイン バインドを構成していて、LDAP に切り替える必要がある場合、またはその逆の場合は、[Active Directory] - [ドメイン バインド] の順に移動し、ドメイン バインド情報を編集して他のプロトコルを選択できます。[ドメイン バインド] の編集を開始すると、コンソールにドメイン バインド ウィザードが表示されます。次に、ウィザードを完了し、必要な情報を入力し、手順に従って、現在のプロトコルの選択から別のプロトコルの選択に変更します。

サービスの保存済みコレクションからの証明書の削除

コンソールには、現在サービスに保存されているすべての証明書が表示されます。不要になった証明書をコンソールの表示から消去する機能を提供するため、コンソールの [設定] - [Active Directory 証明書] ページには、[自動検出済み] および [アップロード済み] 証明書の両方の表示に [削除] アクションがあります。

テナントが LDAPS サポートに対して有効になっている場合のドメイン バインド ウィザード

この機能を有効にすると、画面上のドメイン バインド フローは、有効でない場合とは異なって表示されます。この機能を有効にする場合、手順は次のとおりです。

1 `https://cloud.horizon.vmware.com` で コンソールにログインします。

2 テナントに登録されている Active Directory ドメインが 0 の場合（テナントと最初のポッドがまったく新しい場合など）は、その状況でアクセスできる唯一の場所（コンソールの [はじめに] - [全般的なセットアップ] - [Active Directory] - [構成]）からドメイン バインド フローを開始します。

   テナントにすでに Active Directory ドメインが登録されている場合（コンソールでページの左側のメニューにアクセスできるようにするなど）、コンソールの [設定] - [Active Directory] ページに移動して、ドメイン バインド情報の入力を開始できます。

3 手順 2 を実行すると、ドメイン バインド ウィザードが表示されます。このウィザードには、ドメイン バインド、プロトコル、サマリの 3 つの部分があります。

   次のスクリーンショットは、その表示と、ドメイン バインド部分から始まる 3 つの部分を示しています。

4 この最初のウィザードの手順で、必要な情報を入力し、[次へ] をクリックして保存し、次の手順に進みます。各バインド アカウント名を入力する場合は、ドメイン名を含まないアカウント名（`ouraccountname` のようなユーザー ログイン名など）を入力します。これらのドメイン バインド アカウントにサービスが必要とするものについては、ドメイン バインド アカウント - 必須の特性を参照してください。

フィールド	説明
[NETBIOS 名]	テキスト ボックスが表示されます。ポッドが認識できる Active Directory ドメインの NetBIOS 名を入力します。通常、この名前にはピリオドは含まれません。Active Directory ドメイン環境から使用する値を見つける方法の例については、Horizon Cloud の Active Directory の登録ワークフローの NETBIOS 名と DNS ドメイン名のフィールドに必要な情報の検索を参照してください。
[DNS ドメイン名]	[NETBIOS 名] に指定した Active Directory ドメインの完全修飾 DNS ドメイン名を入力します。
[バインド ユーザー名] と [バインド パスワード]	選択したドメインで使用するサービスのドメイン バインド サービス アカウントの認証情報を指定します。
[補助アカウント #1]	[バインド ユーザー名] と [バインド パスワード] フィールドに、補助 LDAP バインド アカウントとして使用するドメイン内のユーザー アカウントとそれに関連するパスワードを入力します。

5 [プロトコル] の手順では、プロトコルを選択し、オプションでサービスが最初のウィザード手順で入力した Active Directory ドメインとの通信に使用する優先ドメイン コントローラと追加情報を指定します。LDAPS 用に構成された Active Directory 環境のコンテキストでは、ウィザードのこの手順で信頼できる CA 証明書を指定します。

ユーザー インターフェイスには、[プロトコル] の選択内容が反映されます。次のスクリーンショットは、[LDAPS] の選択と [自動検出] ラジオ ボタンの選択を示しています。

これらのフィールドはすべて、前のウィザード手順で指定した Active Directory ドメインのコンテキストにあります。ユーザー インターフェイスは、選択内容に基づいて動的に変わります。

フィールド	説明
[プロトコル]	LDAPS または LDAP のいずれかを選択します。
[ドメイン コントローラ]	任意。このテキスト ボックスを使用して、サービスで最初の手順で指定した Active Directory ドメインへのアクセスに使用する DC のカンマ区切りリストを指定できます。テキスト ボックスを空のままにしておくと、サービスではその Active Directory ドメインに使用可能なドメイン コントローラが使用されます。 ■ プロトコルとして LDAPS を選択する場合は、完全修飾 DNS ホスト名を使用して DC を指定する必要があります。 ■ プロトコルとして LDAP を選択した場合、IP アドレスまたは完全修飾 DNS ホスト名を使用できます。
[コンテキスト]	Active Directory ドメインの命名コンテキスト。このテキスト ボックスは、前のウィザード手順の [DNS ドメイン名] で指定した情報に基づいて自動入力されます。
[証明書]	プロトコルに LDAPS が選択されている場合に使用できます。CA 証明書をシステムに提供する方法を選択します。このページで前述したように、システムは次の 2 つの方法をサポートします。 ■ CA 証明書の自動検出。Active Directory ドメイン環境がこの方法の使用をサポートしているかどうかを確認するには、このドキュメント ページの上記の「自動検出 - Microsoft CA」のセクションを参照してください。 ■ CA 証明書を手動でアップロードします。Active Directory ドメイン環境で自動検出方法の使用がサポートされていない場合は、この方法を選択します。

プロトコルに LDAPS を選択し、[証明書] でラジオ ボタンの 1 つを選択したら、証明書を提供するために選択した方法に応じて、次のいずれかの手順を実行します。どちらの場合も、ユーザー インターフェイスに表示される画面のプロンプトに従います。

自動検出

[自動検出] をクリックします。このページの前のセクションで説明したように、システムは、関連するウィザード フィールドに入力された Active Directory ドメインおよびドメイン コントローラ情報によって指定された環境内の CA 証明書を検出します。これらの CA 証明書はユーザー インターフェイスに表示されます。画面に表示されるフローに従います。ユーザー インターフェイスでは、検出されたすべての証明書を受け入れるように求められます。ウィザードが最後の手順に進む前に、検出された証明書のセットを受け入れる必要があります。

アップロード

この方法では、PEM でエンコードされたルート証明書と中間 CA 証明書を手動でアップロードする必要があります。ローカル システムから CA 証明書ファイルをアップロードするには、[アップロード] をクリックします。ユーザー インターフェイスは、PEM ファイル拡張子を持つファイルのみを受け入れます。

ウィザードの [次へ] ボタンが表示されたら、クリックして最後の手順に進みます。

6 [サマリ] の手順で情報を確認し、問題がなければ [終了] をクリックします。

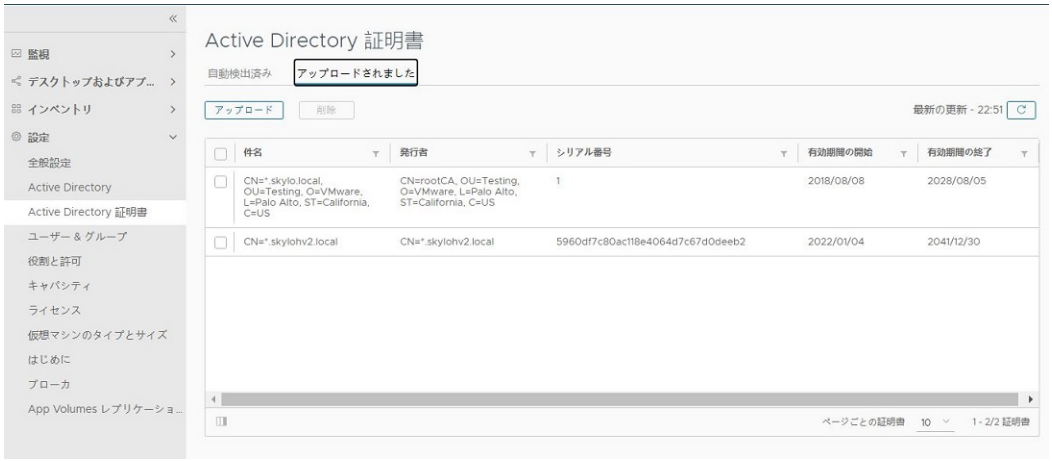
次のスクリーンショットは、前の手順でアップロード方法を使用して証明書を提供した場合のサマリを示しています。この例では、8 つの証明書がアップロードされています。

このフローの最後で、Active Directory ドメインのドメイン バインド構成がシステムに保存されます。

新しい Horizon Cloud テナントの最初の Active Directory ドメインの登録の一環として上記のフローを実行した場合、ユーザー インターフェイスは、ドメイン参加フローと管理者の追加フローを完了するように要求します。これら 2 つのフローの詳細については、最初の Active Directory ドメイン登録の実行の「ドメイン参加とスーパー管理者ロールの追加」というタイトルのセクションを参照してください。

[Active Directory 証明書] ページ

証明書がシステムに保存されると、コンソールの [Active Directory 証明書] ページに表示されます。このページでは、現在システムに保存されている CA 証明書を確認したり、使用されなくなった証明書を削除することができます。次のスクリーンショットは、説明の目的だけのために、管理者が証明書をシステムにアップロードした場合を示しています。



Horizon Cloud LDAP サーバの署名要件がある Active Directory ドメイン コントローラのサポート

Horizon Cloud では、[ドメイン コントローラー: LDAP サーバー署名必須] のセキュリティ ポリシーが [署名を必要とする] に設定されている Active Directory のドメイン コントローラを使用することがサポートされています。

Horizon Cloud では、署名とシーリングの両方を有効する際に、安全な Generic Security Services Application Program Interface (GSSAPI) の LDAP バインドを使用します。この機能により、LDAP データに整合性とプライバシーの両方がもたらされます。Horizon Cloud ポッドはこの機能により、[ドメイン コントローラー: LDAP サーバ署名必須] のセキュリティ ポリシーが [署名を必要とする] に設定されている ドメイン コントローラに接続可能になります。

Horizon Cloud のクラウド接続されたポッドに対する外部およびフォレストの信頼のサポートについて

複雑な Active Directory 環境における組織のシナリオでは、ポッドでプロビジョニングされたリソースが 1 つのフォレストのドメインに参加する一方で、ユーザー アカウントが別のフォレストのドメインに存在し、ドメイン内のユーザーが他のドメインのリソースにアクセスすることを可能にする外部またはフォレストの信頼がある場合があります。このトピックでは、複数のフォレストにおけるドメイン間の外部の信頼またはフォレストの信頼をスキャンするための Horizon Cloud サポートについて説明します。

管理コンソールで、ポッドでプロビジョニングされたリソースの使用資格をユーザーとグループに付与する、いわゆる割り当てを作成します。コンソールを使用して VDI デスクトップ割り当てまたはファームを作成する場合、作成されたデスクトップ仮想マシンまたはファームのセッション ホスト仮想マシンをどのクラウド登録済みドメインに配置するかを指定します。また、コンソールを使用して、Active Directory ドメイン内のユーザーおよびグループにこれらのリソースの使用を提供するように割り当てを構成します。これらの割り当てに対する複雑なドメイン環境の使用に対応するため、Horizon Cloud は次の機能をサポートします。

- あるフォレストのドメインに参加しているポッドでプロビジョニングされたリソースの使用資格を、別のフォレストのドメインに参加しているユーザーおよびグループに付与する。

- 一方向の信頼。

重要： Horizon Cloud の割り当てにドメイン ローカル グループを使用することはサポートされていません。さまざまなフォレストのグループに同じ割り当ての使用資格を付与するには、各フォレストの 1 つのユニバーサル グループを登録する必要があります。

外部およびフォレストの信頼を Horizon Cloud がサポートするには、以下を実行する必要があります。

- クラウド接続されたポッドからプロビジョニングされたリソースで使用するアカウントを含むすべてのフォレストのすべてのドメインを Horizon Cloud に登録します。グループのドメインが Horizon Cloud に登録されていない限り、システムはフォレストのグループを検証できません。第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行および追加の Active Directory ドメインをクラウド構成の Active Directory ドメインとして Horizon Cloud テナント環境に登録するを参照してください。これらのトピックで説明するように、クラウド接続されたすべてのポッドは、クラウド登録されたすべての Active Directory ドメインを認識できる必要があります。
- フォレストの信頼の両側にあるフォレスト ルート ドメインを登録します。フォレストのルート ドメインにユーザーまたはデスクトップがない場合でも、この要件を満たす必要があります。この要件により、Horizon Cloud がフォレストのルートに接続し、関連する TDO（信頼されたドメイン オブジェクト）をデコードできるようになります。
- 各フォレストの 1 つ以上の登録済みドメインでグローバル カタログを有効にします。パフォーマンスを最適化するためには、すべての登録済みドメインでグローバル カタログを有効にする必要があります。
- さまざまなフォレストのグループに Horizon Cloud の同じ割り当ての使用資格を付与するには、各フォレストの少なくとも 1 つのユニバーサル グループを登録します。
- フォレスト ドメインの DNS 名およびルート命名コンテキストの階層構造に従います。たとえば、親ドメインが `example.edu` の場合、子ドメインは `vpc.example.edu` となり、`vpc.com` とはなりません。
- 外部の信頼されたフォレストのドメインが、別の登録済みドメインと競合する NETBIOS 名を使用しないようにします。このようなドメインはシステムの列挙から除外されるためです。登録済みの NETBIOS 名は、信頼されたフォレストのドメインに関するシステムの列挙時に検出された衝突する NETBIOS 名よりも優先されます。

Horizon Universal Console にログインして Horizon Cloud 環境で管理タスクを実行する

クラウドベースの Horizon Universal Console を使用して、クラウド接続されたポッドで管理タスクを実行します。コンソールは、クラウド サービスによって提供されるブラウザベースのインターフェイスです。業界標準のブラウザを使用してコンソールにログインします。ログイン手順の詳細は、特定の環境の構成によって異なることがあります。

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。

コンソールへのアクセスに使用する認証フローの概要については、Horizon Cloud テナント環境への認証についてを参照してください。

前提条件

Horizon Cloud テナント環境に関連付けられている VMware Cloud Services アカウントまたは VMware Customer Connect アカウント（以前の My VMware アカウント）の認証情報があることを確認します。

Active Directory ドメインがすでに Horizon Cloud テナントに登録されている場合、アクセス権限を持つそのドメインの Active Directory アカウントの認証情報があることを確認します。

手順

1 Horizon Universal Console の https://cloud.horizon.vmware.com/ ポータル URL に移動します。

この URL は、以下のスクリーンショットに示すように、VMware Cloud Services ログイン画面にリダイレクトされます。Horizon Cloud テナントに関連付けられている認証情報を使用してログインします。

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。

2 Horizon Cloud テナントの状態に適用可能な認証フローに従って、画面上のフローを実行します。テナントの状態とフローの詳細については、Horizon Cloud テナント環境への認証についてを参照してください。

結果

コンソールが表示されます。

重要：

- Active Directory ログイン画面で正しい Active Directory 認証情報を送信し、「`Active Directory` 権限が一致しません。メイン管理者に連絡して、割り当てられたロールを確認してください。」というエラー メッセージが表示される場合、これは、Active Directory ユーザー アカウントが、Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てる Active Directory グループに属していて、提供される権限が Horizon Cloud テナント環境のカスタマイズ可能な全般設定の [My VMware] セクションで割り当てられたロールよりも少ないことを意味しています。この違いにより、ユーザーはログインできなくなります。この問題を修正するために、Horizon Cloud テナントの管理者権限を持つ組織のユーザーは、[全般設定] ページの [My VMware] セクションにログインし、割り当てられたロールを変更することができます。これにより、権限は [役割と許可] ページで選択したロールの権限と一致します。2 つのタイプのロールがどのように連携するかについては、Horizon Universal Console 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。

  VMware Cloud Services のログイン画面で入力された認証情報が、環境のクラウド プレーンのテナント レコードで所有者としてマークされているアカウントの認証情報である場合、このメッセージは表示されません。システムは、Active Directory グループのロールとロールの権限が一致しない場合でも、その所有アカウントがログインできるようにします。
- ご使用の環境でメンテナンスが実行されている場合、メンテナンス期間中にログインできないことを示すメッセージがログイン画面に表示されます。
- Active Directory ユーザー名またはパスワードの入力に誤りがある場合、システムは VMware Cloud Services を使用して認証をログアウトします。この状況では、VMware Cloud Services ログインに戻り、ログイン フローを実行して Active Directory ログイン画面に戻り、もう一度やり直すことができます。

次のステップ

該当する場合、Active Directory ドメイン登録プロセスを実行して Active Directory ドメインを Horizon Cloud 顧客アカウントに登録します。第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行を参照してください。Active Directory 登録プロセス全体を完了しないと、他のサービスを操作することはできません。

注： 管理者がコンソールにログインできるデフォルトの期間は 30 分です。この時間が経過すると認証済みセッションが終了し、管理者は再度ログインする必要があります。Microsoft Azure に少なくとも 1 つのポッドがある場合、[全般設定] ページの [セッション タイムアウト] セクションで、[管理ポータルのタイムアウト] 値を編集することでこの時間を調整できます。環境に Horizon ポッドしかない場合、デフォルト値である 30 分を変更することはできません。Horizon Cloud テナント環境のカスタマイズ可能な全般設定を参照してください。

Horizon Cloud テナント環境への認証について

Horizon Cloud テナント環境は、管理コンソールを使用して管理します。このコンソールにアクセスできるかどうかは、その Horizon Cloud テナントにアクセスする権限を持つ VMware Customer Connect アカウントの認

証、および同じテナントに登録されている Active Directory ドメインを使用した認証を提供する認証フローに依存します。

ログイン手順と、ログイン画面のスクリーンショットについては、Horizon Universal Console にログインして Horizon Cloud 環境で管理タスクを実行するを参照してください。

Horizon Cloud 環境を Workspace ONE 環境に統合している場合、Workspace ONE または Horizon Cloud のログイン フローを使用して Horizon Cloud テナントにログインできます。

注： ジャストインタイム ユーザー プロビジョニングを使用して作成されたユーザーは、Horizon Cloud ログイン フローを使用してログインできません。これらのユーザーは、Workspace ONE を使用してログインする必要があります。

次のすべてのテナント状態では、ログイン フローは認証要求を VMware Cloud Services にリダイレクトします。

- 組織で VMware Cloud Services に特定の構成がある場合は、その組織の構成に従って認証されます。
- それ以外の場合は、VMware Cloud Services ログイン フローで VMware Customer Connect アカウントの認証情報を使用します（VMware Customer Connect アカウントは、以前は My VMware アカウントという名前でした）。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。

上記のいずれかの方法を使用した後に表示される特定の認証フローは、ログイン時の Horizon Cloud テナントの状態によって異なります。たとえば、ログイン時にテナントがクラウド接続されたポッドを持っているか、単一のクラウド接続されたポッドを持っていて、まだ Active Directory ドメインを登録していないか、1 つの登録された Active Directory ドメインを持っているか、などによって異なります。

初期テナントの状態 - クラウド接続されたポッドを持っていない

テナントへの認証が完了すると、コンソールに [はじめに] ウィザードが表示され、デフォルトで [キャパシティ] セクションが展開されています。ポッドをクラウド接続するまでは、[はじめに] ウィザードが唯一のアクセス可能なユーザー インターフェイス ページになります。この時点で、ポッドを Horizon Cloud にオンボーディングして、テナントをこの初期状態から移行する必要があります。ポッドのオンボーディングの詳細については、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およびそのサブトピックを参照してください。

ヒント: ライセンスとロールの要件を満たしている場合は、[無期限キーの表示] リンクを使用できます。[無期限キーの表示] リンクをクリックして [無期限キー] ページにアクセスし、基盤となる VMware 製品の無期限キーを表示および生成できます。最初のポッドがオンボーディングされ、ドメイン登録が完了すると、ライセンスとロールの要件を満たしている場合は、[ライセンス] ページと [はじめに] ページの両方でリンクが使用可能になります。第 1 世代のテナント - Horizon Universal Console を使用したライセンス情報の取得を参照してください。

次のスクリーンショットは、テナントがこの初期状態にあるときのコンソールを示しています。

1 つのクラウド接続ポッドを持っているが Active Directory ドメインが登録されていないテナント

テナントに対して認証を行った後、コンソールの表示は初期状態とは少し異なって見える場合があります。[はじめに] ウィザードは、デフォルトで [キャパシティ] セクションが展開された状態で表示され、アクセス可能な唯一のユーザー インターフェイス ページです。ただし、この Horizon Cloud テナントを使用して組織の Active Directory ドメインを構成するためにアクセスできるようになりました。テナントをこの状態から移行するには、第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行の手順を実行します。

単一の登録済み Active Directory ドメインを持つテナント

VMware Cloud Services による認証に成功すると、次のいずれかの処理が行われます。

- Horizon Cloud テナントに登録されている登録済みの Active Directory ドメインが、VMware Cloud services でエンタープライズ フェデレーション用にも構成されている場合、認証はその構成に従ってフローが実行されます。認証フローでは Horizon Cloud Active Directory ログイン ウィンドウが省略されます。組織がフェデレーション ID 管理用に VMware Cloud Services で構成した内容に従って認証を行うと、コンソールが表示されます。
- 登録済みの Active Directory ドメインが VMware Cloud Services にフェデレーションされていない場合、ブラウザは Horizon Cloud Active Directory ログイン ウィンドウにリダイレクトされます。この Active Directory ログイン ウィンドウで、Active Directory アカウントの認証情報を入力します。このログイン画面で認証が正常に完了すると、コンソールが表示されます。次のスクリーンショットは、`EXAMPLEDOMAIN` という名前のドメインがテナントに登録されている場合のこのログイン ウィンドウを示しています。

複数の登録済み Active Directory ドメインを持つテナント

この状態では、認証フローは、上記の単一の登録済み Active Directory ドメインの状態と比較して次のような違いがあります。

- Horizon Cloud Active Directory ログイン ウィンドウが表示されている認証フローで、ドロップダウン リストを使用して、指定された認証情報が有効なドメインを選択します。次のスクリーンショットは、Horizon Cloud テナントに 2 つの登録済み Active Directory ドメイン（`DOMAIN-A`、`DOMAIN-B`）が含まれている例を示しています。

- テナントに登録され、また VMware Cloud services でエンタープライズ フェデレーションが設定されている Active Directory ドメインにアカウントが属している場合、認証フローでは前のセクションで説明した Horizon Cloud Active Directory ログイン ウィンドウが省略されます。ただし、アカウントが属している Active Directory ドメインがテナントに登録されていても、組織が VMware Cloud services でそのドメインをエンタープライズ フェデレーション用に構成していない場合、ブラウザは Horizon Cloud Active Directory ログイン ウィンドウにリダイレクトされます。この場合は、ドロップダウンでドメインを選択し、ログインするための Active Directory 認証情報を入力します。

  注： 2020 年 5 月の時点で、このフェデレーション ID 管理機能は制限されており、Horizon Cloud テナントのクラウド接続ポッドがすべて Microsoft Azure のポッドである場合にのみ使用できます。

第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアー

このクラウドベースおよび Web ベースのコンソールは、第 1 世代 Horizon Cloud 環境とクラウド接続されたポッドを管理および監視するための統合管理を提供するユーザー インターフェイスです。

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。

注意: Horizon Universal Console は動的であり、テナント環境の最新の構成に適した機能を反映しています。このドキュメントで説明されている機能へのアクセスは、以下の要因（ただしこれらに限定されない）に依存する場合があります。

- その機能が最新の Horizon Cloud ポッド マニフェスト、Horizon ポッドのバージョン、または Horizon Cloud Connector のバージョンでのみ使用可能なシステム コードに依存するかどうか。
- 機能が初登場したときに、リリース ノートに記載されているように制限付きで機能へのアクセスが提供されるかどうか。
- 機能に特定のライセンスまたは SKU が必要かどうか。

このドキュメントに機能の記載があり、コンソールにその機能が表示されない場合は、まずリリース ノートを読み、その機能のアクセスが制限されているかどうか、およびテナントで有効化をリクエストする方法について確認します。または、このドキュメントに記載されている機能を使用する資格があり、コンソールにその機能が表示されない場合は、Customer Connect でサポート リクエストを提出する方法 (VMware KB 2006985)に記載されている情報（技術以外）サービス リクエスト (SR) を開くことができます。

対応ブラウザ

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。

ナビゲーションおよび機能領域

インターフェイスの左側にはナビゲーション バーがあり、ユーザー インターフェイスのメイン領域に移動するための階層が用意されています。次の表は、バーの先頭から開始する各領域について説明します。

カテゴリ	機能領域
[監視]	[監視] カテゴリでは、統一されたダッシュボード、アクティビティ監視、レポート、および通知にアクセスできます。このカテゴリのページの概要については、Horizon Universal Console の [監視] メニューについておよび第 1 世代のテナント - 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、[アクティビティ] ページ、第 1 世代テナント - 第 1 世代 Horizon Universal Console の [レポート] ページ、通知ページのトピックを参照してください。
[割り当て]	[割り当て] カテゴリでは、割り当て、割り当て関連のアクション、およびワークフローにアクセスできます。このカテゴリのページの概要と、割り当てに対して実行できるさまざまな割り当て関連ワークフローへのリンクについては、Horizon Universal Console の [割り当て] メニューについてを参照してください。
[インベントリ]	[インベントリ] カテゴリは、インポートしたベース仮想マシン、シールド イメージ、ファーム、アプリケーションなど、ポッドからのサービスとしてのデスクトップ アーティファクトへのアクセスを提供します。このカテゴリのページの概要および実行可能なタスクについては、Horizon Cloud テナントのインベントリ内の資産の表示を参照してください。 **注：** このカテゴリのページの多くは、Microsoft Azure のポッドにのみ適用できます。
[設定]	[設定] カテゴリは、環境内の設定と構成を含むページへのアクセスを提供します。このカテゴリのページの概要および実行可能なタスクについては、Horizon Universal Console の [設定] メニューについてを参照してください。

たとえば、このリリースでは、コンソールの一部の領域は Microsoft Azure にデプロイされた Horizon Cloud ポッドにのみ適用されます。Horizon Cloud ポッドは、コンソールの自動化されたポッド デプロイ ウィザードによって Microsoft Azure にデプロイされ、ポッド マネージャ ソフトウェア テクノロジーを実行するポッドです。クラウド接続されたポッドのフリートが Horizon ポッド (Horizon Connection Server ソフトウェアを実行しているポッド) のみで構成されている場合、ポッド マネージャベースのポッドにのみ適用可能な領域にグラフィックとメッセージが表示されます。次のスクリーン ショットは、表示される内容の一部です。

クラウド接続されたポッドのフリートに Horizon Cloud ポッドと Horizon ポッドの両方が含まれている場合、各種ページには説明バナーが表示されることがあります。

上部のツールバー

コンソールの上部には、ログイン ユーザー名の下に [ログアウト] アクションのアイコンが表示されるほか、以下のアイコンが表示されます。

- ユーザーまたは仮想マシンを検索するコンソールの検索機能（ 

）。詳細については、コンソールの検索機能の使用を参照してください。
- 通知（  ）。詳細については、通知ページを参照してください。
- サポート関連情報（  ）。現在のサービス レベルの新機能、Web ベースのドキュメント、ビルド情報、サポートのリクエスト方法などを確認できます。
- サポートされている言語でコンソールを表示するための言語セレクタ。

第 1 世代 Horizon Universal Console のナビゲーション メニューとフィルタ フィールドの使用について

このドキュメント ページでは、第 1 世代コンソールのナビゲーション メニューとフィルタ フィールドの使用方法について説明します。

左側のナビゲーション メニュー

第 1 世代コンソールのメニューを使用すれば、Horizon Cloud 環境ですぐに移動してアクティビティを監視したり、さまざまな機能を実行したりできます。これらのメニューは、コンソールの左側に沿って配置されています。

表 1-5. コンソールのナビゲーション メニュー

メニュー	説明
	[はじめに] ページをデフォルトのランディング ページとして設定した場合、このアイコンをクリックすると、[はじめに] ページが表示されます。Horizon Cloud の [はじめに] ウィザード - 概要を参照してください。設定していない場合、このアイコンをクリックすると 第 1 世代のテナント - 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が表示されます。
[監視]	以下に対するアクセスを提供します。 ■ 環境全体に関する情報（問題のステータス、キャパシティと使用率レベル、エンドユーザーのアクティビティなど）を示すダッシュボード。 ■ アクティビティ レポートと監査ログ。 ■ エンド ユーザーのデスクトップおよびアプリケーション セッションに関するさまざまな詳細レポート。 ■ 通知。
[割り当て]	コンソールの割り当て関連領域へのアクセスを提供します。この領域では、環境のインベントリ内にある割り当て可能なアイテムへのエンドユーザーアクセスを付与する割り当てを操作できます。 **ヒント:** コンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。コンソールの割り当て関連ページに表示されるラベルは、テナントの設定済みのブローカ設定、フリート内のクラウド接続されたポッドのタイプ、テナントの地域別クラウド プレーン、および特定のライセンスに基づく機能などの要因によって異なります。

表 1-5. コンソールのナビゲーション メニュー （続き）

メニュー	説明
[インベントリ]	Microsoft Azure にデプロイされたポッドが環境にある場合、このコンソール領域には、次のような資産を処理するためのアクセス権限があります。 ■ システムがインクラウド ポッドからインポートした基本イメージ仮想マシンおよびその他の仮想マシン（ある場合）。 ■ 公開済みの（シールドされた）イメージ ■ RDSH ファーム ■ RDSH ファームからのリモート アプリケーション ■ App Volumes アプリケーション（テナント環境で App Volumes の使用が有効になっている場合）。 環境にクラウド接続された Horizon ポッドがある場合、このコンソール領域では、クラウド プレーンで管理されているイメージを操作するためのアクセスを提供します。
[設定]	次のような各種のシステム領域でシステム全体の設定と構成を操作できる画面へのアクセスを提供します。 ■ Active Directory ドメイン ■ 役割と許可 ■ 環境内のキャパシティに関連する項目 ■ Workspace ONE Access を使用する ID 管理 ■ Microsoft Azure のポッドで使用される仮想マシンのタイプとサイズ ■ 環境およびポッド全体に適用される構成 ■ [はじめに] ページ

Horizon Universal Console の [監視] メニューについて

[監視] を使用して、さまざまなダッシュボード、表示、およびレポートに移動します。環境の使用状況および環境内の管理者とユーザーのアクティビティの調査、システム通知の参照、およびさまざまなレポートの表示を実行できます。

[監視] をクリックして、次のページに移動します。

オプション	説明
[ダッシュボード]	全体的な環境に関する情報を表示します。これにはポッドの健全性ステータス、キャパシティと使用率レベル、エンドユーザーのアクティビティなどが含まれます。
[アクティビティ]	管理者およびエンド ユーザーのアクティビティの詳細、および監査ログを提供します。
[レポート]	ユーザーをデスクトップにマッピングする方法など、事前定義されたさまざまなレポートにアクセスできます。
[通知]	重要なイベントなど、システムについての情報を提供する通知をリストします。

[アクティビティ] ページ

システムの現在および過去のイベントに関するデータにアクセスするには、[アクティビティ] ページを使用します。

[アクティビティ] ページは、[監視] アイコンからアクセスできます。このページには、管理者イベント、ユーザー イベント、およびポッドで開始されたイベントの監査ログのタブが含まれています。

使用可能なアクション

[アクティビティ] ページの各タブには、次のアクションが用意されています。

- 各タブで使用可能なフィルタ ツールを使用して、表示されるイベントをフィルタリングする。
- リストを更新する。
- [レポートのエクスポート] 機能で、表示されている情報をレポート ファイルとしてエクスポートします。他のタブとは異なり、[監査ログ] タブでは、データのエクスポートに [エクスポート] ボタンが使用されます。

[管理者] タブでは、管理者関連のイベントをキャンセルすることもできます。詳細は次の 管理者イベント セクションを参照してください。

[アクティビティ] ページのタブからのレポートのエクスポート

各タブには、タブに関連付けられたデータを含むレポートをエクスポートするためのアクションがあります。

ほとんどのタブでは、レポートをエクスポートすると、[レポート] ページの [エクスポートされたレポート] タブに表示されます。ここから、レポートをダウンロードできます。詳細については、第 1 世代テナント - 第 1 世代 Horizon Universal Console の [レポート] ページを参照してください。

[監査ログ] タブは、他のタブとは若干異なるエクスポート メカニズムを使用します。[監査ログ] タブで、そのタブの [エクスポート] をクリックすると、エクスポートされたレポート機能を使用する代わりに CSV ファイルがダウンロードされます。

重要： [レポートのエクスポート] ボタンを使用するタブで、ポッド フィルタで [すべてのポッド] を選択すると、[レポートのエクスポート] ボタンは無効になります。各ポッドのエクスポートを実行することで、すべてのポッドのデータをエクスポートできます。

エクスポートを開始するときに、すべてのデータをエクスポートするか、現在フィルタされているデータのみをエクスポートするかを選択できます。

次に、レポートが生成中であることを示すメッセージがページの最上部に表示されます。

この準備はレコードの数に応じて数分間かかります。たとえば、50,000 レコードのレポートには、約 10 分かかります。

[レポート] ページの [エクスポートされたレポート] タブで、レポートの進行状況を確認したり、エクスポートが完了したレポートをダウンロードできます。その [エクスポートされたレポート] タブで、リストから [Horizon Cloud Service] を選択してレポートを表示します。

管理者またはユーザー イベントの場合、エクスポートされたレポート ファイルは ZIP ファイルに含まれる CSV ファイルです。生成された CSV ファイル内のデータは日付で並べ替えられません。この点は、次のいずれかの方法で変更できます。

- Excel で CSV ファイルを開き、*yy/mm/dd hh:mm AM/PM* 形式のを日付を含むセルの日付書式を設定します。
- Excel で新規の空のワークブックを作成し、Excel のデータ インポート ウィザードを使用して、ダウンロードした CSV ファイルをインポートします。

管理者イベント

[管理者] タブには、管理者イベントに関する情報が表示されます。イベントを展開して、そのイベントの詳細とサブタスクを表示します。イベントをクリックして、そのイベントの詳細と進捗状況を表示します。イベントの説明をクリックすると、詳細情報が表示されます。

列	説明
説明	イベントに関する詳細。
ステータス	[成功] は、イベントが完全に実行されたことを示します。[失敗] は、イベントが部分的に実行されたか、まったく実行されなかったことを示します。
% 完了	イベントの現在の進捗状況。
時刻	イベントが記録された時刻。

これらのフィルタ オプションは、[管理者] タブで使用できます。

- タブの上部にあるフィルタを使用して、特定の期間、特定のポッド、または特定のステータスのイベントのみを表示します。
- 各列のフィルタ ツールを使用してテーブルに表示されるイベントをフィルタします。

[管理者] タブから、割り当てに関連するタスクを完了する前に、リストでタスクを選択して [タスクをキャンセル] ボタンをクリックすることによってそのタスクをキャンセルできます。

- キャンセルするタスクの選択を行う前に、ビューを更新して表示されているタスクのステータスを最新の状態にします。
- タスクが現在、システムによってキャンセルできる状態になっている場合、そのキャンセル可能なタスクに対応しているチェック ボックスを選択できます。リスト内のすべてのタスクがキャンセル可能の場合は、リストの上部にある [すべて選択] チェックボックスを選択して、すべてのタスクをキャンセルすることもできます。そうでなければ、タスクを個別に選択する必要があります。

次の表はキャンセルできるタスクを示しています。

タスク	タスクがキュー状態にあるときにキャンセル	タスクが実行状態にあるときにキャンセル
ファームの拡張	サポートされています **注：** システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。	サポートされています 次の点に注意してください。 ■ システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。 ■ 仮想マシンや OS/データ ディスクなど、すでに作成されているリソースは、タスクがキャンセルされると破棄されます。仮想マシンが破棄された場合または作成されていない場合、割り当てのサイズは変わります。 ■ このオプションは、マルチクラウドの割り当てでは使用できません。
割り当ての拡張	サポートされています **注：** システムによって VDI デスクトップ割り当てに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、割り当てがオフラインになる必要があります。	サポートされています 次の点に注意してください。 ■ システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。 ■ 仮想マシンや OS/データ ディスクなど、すでに作成されているリソースは、タスクがキャンセルされると破棄されます。仮想マシンが破棄された場合または作成されていない場合、割り当てのサイズは変わります。 ■ このオプションは、マルチクラウドの割り当てでは使用できません。
仮想マシンのイメージへの変換	サポートされています **注：** このタスクをキャンセルして再試行する場合は、まず仮想マシンが変換可能な状態であることを確認します。不明な場合は、仮想マシンをパワーオフしてからパワーオンします。	サポートされています **注：** このタスクをキャンセルして再試行する場合は、まず仮想マシンが変換可能な状態であることを確認します。不明な場合は、仮想マシンをパワーオフしてからパワーオンします。

ユーザー イベント

テナントのフリート内のポッド タイプに応じて、コンソールには [ユーザー (Azure)] タブ、[ユーザー (VMware SDDC)] タブ、またはその両方が表示されます。

これらのタブを使用して、イベントに関連付けられているポッド タイプ別に分類されたエンドユーザー イベントの説明と時間にアクセスします。

たとえば、[ユーザー (VMware SDDC)] タブを使用して、テナントの Horizon 環境に関連するエンドユーザー イベントのログ データにアクセスします。

これらのタブでは、次のフィルタ オプションを使用できます。

- タブの上部にあるフィルタを使用して、特定の期間または特定のポッドのイベントのみを表示します。
- 各列のフィルタ ツールを使用してテーブルに表示されるイベントをフィルタします。

監査ログ

[監査ログ] タブには、ポッド上で管理者により開始されたアクションから発生したイベントについて記録された時刻、ステータス、説明、ユーザー情報が表示されます。詳細については、監査ログの操作を参照してください。

タブの上部にある [フィルタ] ツールを使用して表示されるイベントをフィルタリングできます。

第 1 世代テナント - 第 1 世代 Horizon Universal Console の [レポート] ページ

コンソールの [レポート] ページを使用して、第 1 世代の Horizon Cloud テナントによって提供されるエンド ユーザーのデスクトップおよびアプリケーション セッションに関連するさまざまなレポートにアクセスします。

注目: この [レポート] ドキュメント ページは、「VMware ナレッジベースの記事 KB91183」で説明されているように、第 1 世代コンソールへの変更に合わせて更新されています。

ナレッジベースの記事で説明されているように、VMware Workspace ONE Intelligence for Horizon は、VMware Horizon Universal、Horizon Apps Universal、および Horizon Apps Standard のサブスクリプション ライセンスを持つ第 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。
- コンソールの [レポート] ページに以前に表示されていた Azure 同時実行、セッション、ユーザー使用量、VDI アプリケーション使用量、使用率のレポートは、Workspace ONE Intelligence コンソールでのみ使用できるようになりました。
- これらの変更により、[レポート] ページの [スケジュール] タブと関連する機能は、[セッション]、[ユーザー使用量]、および [VDI アプリケーション使用量] レポートにのみ適用されます。
- 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す。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す。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、Workspace ONE Intelligence ドキュメントの「Horizon and DEEM for Horizon」、「Horizon Cloud First-Gen Integration」、「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。

[レポート] ページのナビゲート

[監視] - [レポート] の順に選択して [レポート] ページを開き、さまざまなタイプのレポートの詳細情報を表示できます。レポートを作成すると、結果をフィルタリングしたり、ページを手動で更新したり、レポートをエクスポートしたりするオプションとともにレポートがコンソールに表示されます。

[レポート] ページには、次のタブがあります。

- [レポートの作成] タブには、作成可能なレポートのタイプが表示されます。レポート タイプをクリックして、コンソールでレポートを作成できます。レポート タイプの詳細については、以下のレポート タイプを参照してください。
- [エクスポートされたレポート] タブには、ダウンロード可能なエクスポートされたレポートが表示されます。これには、[レポート] ページの [レポートの作成] タブで作成されたレポートと、コンソール内の他の場所（[アクティビティ] ページなど）からエクスポートしたデータから作成されたレポートが含まれます。
  - タブの上部にあるドロップダウン メニューを使用して、表示するレポートのタイプを選択します。選択肢の数は、テナントのポッド フリート内のポッド タイプによって異なります。
  - レポートを選択し、[ダウンロード] ボタンをクリックして、XLSX 形式のレポート ファイルを含む ZIP ファイルをダウンロードします。

レポート データのエクスポート

コンソールにレポートを表示すると、エクスポート用のラベル付きボタンまたはエクスポート用のアイコン ボタンのいずれかが表示されます。アイコンは、右向きの矢印が付いたページの形をしています。

ボタンをクリックしてエクスポートを開始した後のシステムの動作は、レポートのタイプによって異なります。

ほとんどのレポートの場合

関連するボタンをクリックしてエクスポートを開始すると、レポート作成の進行状況が表示されます。画面のプロンプトに従います。

注目: Microsoft Azure にポッドがあり、それらのポッドのいずれかが 2552 より前のマニフェストにある場合、より大きいレポートはシステムによって次のように処理されます。

- エクスポートを開始すると、レポートがコンパイル中で、しばらく時間がかかることを知らせるメッセージが表示されます。この準備はレコードの数に応じて数分間かかります。たとえば、50,000 レコードのレポートには、約 10 分かかります。
- 準備が完了すると、「**レポートが正常に生成されました**」というメッセージおよび [ダウンロード] ボタンが表示された別のダイアログボックスが表示されます。[ダウンロード] ボタンをクリックした後、このダイアログボックスを閉じる前にダウンロードが完了するまで待機する必要があります。ダウンロードが完了する前に閉じると、ダウンロードがキャンセルされます。

このプロセスが完了するまでコンソールでその他のアクションを実行することはできないため、大量のアクティビティ レコードがある場合は、情報のエクスポートを、コンソールで他のタスクを実行するまでに最大 10 分ほど待つことができるときに計画する必要があります。

レポート タイプ

Horizon Agent がインストールされると、デフォルトで Horizon Monitoring Service Agent オプションがインストールされます。このオプションをインストールしない場合、このイメージに基づくデスクトップ インスタンスまたはファーム マルチセッション インスタンスのユーザー セッションからのアクティビティ関連データは報告されません。その結果、エンドユーザー アクティビティや他の種類のデスクトップ アクティビティのデータは、レポートには表示されません。また、RDP プロトコルの場合、そのエージェント オプションは、他のプロトコルに提供するメトリックのサブセットのみを提供します。

注意: デスクトップ データを vRealize Operations Manager に送信しているクラウド接続された Horizon ポッドがある場合、第 1 世代のクラウド監視トグルを有効にすると、データは代わりに Cloud Monitoring Service (CMS) に送信されます。vRealize Operations Manager を引き続き使用してデスクトップ セッション データを収集するには、[設定] - [全般設定] - [監視] のコンソール設定で CMS を無効にします。

レポート タイプ	詳細
ユーザー マッピング	詳細を表示したり、ユーザー名、ドメイン、デスクトップ名、デスクトップ モデル、ファーム、およびマッピング タイプ（ユーザーまたはグループ）などのさまざまなカテゴリでソートしたりします。 **注：** このレポートは、デスクトップへの直接割り当てを少なくとも 1 つ持つユーザーにのみ表示されます。コンソールで、デスクトップ割り当てを行うときに個々のユーザーまたはユーザー グループを選択できます。ユーザーに個別のユーザーとして少なくとも 1 つの割り当てがあり、割り当て済みグループの一部として 0 以上の割り当てがある場合、このレポートはそのユーザーのすべてのデスクトップ割り当てをレポートします。 ただし、ユーザーのすべてのデスクトップ割り当てがグループを使用して行われた場合、そのユーザーの割り当てはこのレポートにはレポートされません。 ユーザーがデスクトップに個々のユーザーとしてマッピングされる場合、[グループ名] の列は空白です。ユーザーが、デスクトップ割り当てに対する資格が付与されているグループのメンバーである状態から、デスクトップにマッピングされている場合、[グループ名] 列には、資格が付与されているグループの名前が表示されます。
デスクトップ マッピング	詳細を表示したり、デスクトップ名、モデル、割り当て名、タイプ、ファーム、アクティブ ユーザー、マッピングされたユーザーおよびマッピングされたユーザー グループなどのさまざまなカテゴリでソートしたりします。 **注：** このレポートでは、[マップされたユーザー] 列は専用の VDI デスクトップ割り当てのみについて入力されます。これらの割り当てでは、各ユーザーは特定の VDI デスクトップにマッピングされて、ログインするたびに同じデスクトップに戻るためです。そのマッピングされたユーザーは、そのデスクトップに割り当てられたユーザーです。ただし、ファームによって提供されるフローティング VDI デスクトップ割り当ておよびセッション デスクトップ割り当てでは、ユーザーは特定のデスクトップ仮想マシンにマッピングされません。その結果、これらのデスクトップ割り当てのタイプについては、[マップされたユーザー] 列にデータがありません。
URL の構成	現在構成されている URL リダイレクトの情報を表示します。詳細については、シングルポッド ブローカ - Horizon Cloud ポッド - URL リダイレクトのカスタマイズを作成し、ユーザーに割り当てるを参照してください。
エージェントのバージョン	各仮想マシンのエージェントの現在のバージョンを表示します。Microsoft Azure のポッドの場合、このタブには、エージェントのバージョンを更新する必要があるかを判断するのに役立つポッドのマニフェスト バージョンも表示されます。 ポッドの情報を表示するページの左上にある [ポッド] ドロップダウンからポッドを選択します。割り当て名を含むすべての列で、データを並べ替えることもできます。

通知ページ

Horizon Cloud は、イベントやサービス登録など、特定のタイプのシステム アクティビティを伝えるために通知を使用します。

任意のページの右上隅にあるベル アイコン（  ）をクリックすると、管理コンソールに最近の通知を表示できます。通知ページを開くと、すべての通知が表示されます。[監視] - [通知] の順にクリックすると、アクティブな通知と破棄された通知の両方が表示されます。

また、過去 30 日までの任意の期間の通知を表示したり、ページを更新したり、検索対象をフィルタしたりすることもできます。

表 1-6. 通知タイプ

通知タイプ	説明
サービス登録	サービス登録通知は環境の構成中に発行されます。パッケージ サービスの 1 つが正常に登録されると、システムはこのタイプの通知を発行します。
ポッド関連	ポッド関連の通知は、システムが Microsoft Azure にデプロイされたポッドのステータスの変更を検出すると発行されます。これらの通知には、ポッドが Horizon Cloud クラウド プレーンとの接続を失った場合の通知や、サブネットがいっぱいになっているときの通知が含まれます。サブネットがいっぱいになると、仮想マシンのクローン作成に関係するシステム操作により通知が発生します。
ポッド API 関連	この通知は、クラウドプレーンから Microsoft Azure のポッド リソースに送信される API 要求で、API の速度低下やタイムアウトなどの状態が検出されると発生します。
ロックされたプライマリ バインド アカウント	プライマリ ドメイン バインド アカウントが失敗した状態または非アクティブの状態であることをシステムが検出すると、この通知が発行されます。詳細については、プライマリ ドメイン バインド アカウントがロックアウトされているときの通知を参照してください。
緊急アクセス時のドメイン バインド アカウントの使用	この通知は、プライマリ ドメイン バインド アカウントまたは補助ドメイン バインド アカウントを使用してコンソールにログインすると発行されます。Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるの説明のとおり、プライマリ ドメイン バインド アカウントおよび補助ドメイン バインド アカウントには、常にスーパー管理者ロールが割り当てられます。これにより、コンソールで管理アクションを実行するためのすべての権限が付与されます。
新しい Horizon Agents Installer (HAI) の利用可能な更新	この通知は、ポッドのソフトウェア バージョンに関連付けられているエージェントの新しいバージョンが利用可能な場合に発行されます。デフォルトでは、システムは 7 日ごとに更新を確認します。

監査ログの操作

[監査ログ] タブには、ポッド上で管理者により開始されたアクションから発生したイベントについて記録された時刻、ステータス、説明、ユーザー情報が表示されます。[監査ログ] タブに報告されるイベント データの量とタイプは、ポッドのタイプによって異なる場合があります。Horizon Cloud 制御プレーンは、1 年間のイベント データを保持します。

監査ログ

- 監査ログを表示するには、次のいずれかを実行します。
  - [監視] - [アクティビティ] を選択します。[アクティビティ] ページで、[監査ログ] タブをクリックします。
  - [設定] - [キャパシティ] の順に選択します。[キャパシティ] ページで、ログを表示するポッドの名前をクリックしてから、[監査ログ] タブをクリックします。

  デフォルトでは、[監査ログ] タブには、過去 24 時間に生じたすべてのポッド関連イベントのログが、発生時刻の降順で最新のイベントから順に表示されます。
- ログを時刻の昇順でソートするには、[時刻] 列のヘッダーをクリックします。降順に戻すには、ヘッダーを再度クリックします。

- 最新の報告されたイベントで監査ログの表示を更新するには、[更新]（  ）ボタンをクリックします。

監査ログのフィルタリング

監査ログの表示をカスタマイズするために、[期間] フィルタの設定を調整できます。追加のフィルタを適用して、表示されるログの選択をさらに絞り込むこともできます。各フィルタにはドロップダウン メニューがあり、それによってログの選択を絞り込むために使用する操作と値を定義できます。

- [期間] フィルタをカスタマイズするには、ドロップダウン メニューから操作と時間の値を選択し、[適用] をクリックします。
- 追加のフィルタを指定するには、プラス記号 (+) ボタンをクリックします。ドロップダウン メニューを使用して、フィルタのタイプ、操作、およびフィルタの値を選択します。次に、[適用] をクリックします。

  操作メニューと値メニューで使用できるオプションは、フィルタのタイプによって異なります。たとえば、フィルタのタイプに [重要度] を選択して、操作について [次の値以上] を選択し、値に [成功] を選択すると、そのフィルタによりステータスが「成功」または「情報」のすべてのログが表示されます。

  同じタイプのフィルタを複数適用することもできます。たとえば、ステータスが [次の値と等しい] で、値が [成功] のログを表示する [重要度] フィルタを適用できます。さらに、ステータスが [次の値と等しい] で、値が [失敗] のログを表示する [重要度] フィルタを適用できます。

監査ログのダウンロード

注： ダウンロード機能は、Horizon Cloud スーパー管理者の権限を持つユーザーのみが使用できます。

現在のフィルタリングされた監査ログのリストをダウンロードするには、[ダウンロード]（  ）ボタンをクリックします。

ダウンロードされたログは CSV ファイルに格納され、次のプロパティを含んでいます。

- ダウンロード ファイルには、[監査ログ] タブに表示されているかどうかにかかわらず、現在のフィルタ基準を満たすログがすべて含まれています。

  たとえば、現在のフィルタでは、[監査ログ] タブの複数のページにわたる合計 1000 個のログが返される場合があります。ただし、各ページに表示できるログは 10 個のみです。ダウンロード ファイルには、現在表示されているページだけでなく、すべての [監査ログ] ページでの 1000 個のログがすべて含まれます。

- ダウンロード ファイルは、[監査ログ] タブで指定されたソート順に関係なく、常にログを降順で一覧表示します。ソート順は、[監査ログ] タブの表示にのみ適用されます。
- デフォルトでは、ダウンロード ファイルの名前形式は *AuditReport-<YYYY-MM-DDTHH_MIN_SEC.millisZ>*になります（たとえば、「AuditEventReport-2019-08-14T11_16_32.096Z」）。

Horizon Universal Console の [割り当て] メニューについて

コンソールのナビゲーション バーの [割り当て] は、Horizon Cloud 環境で実行できる割り当て関連のワークフローへのアクセスを提供します。

ヒント: コンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。コンソールの割り当て関連ページに表示されるラベルは、テナントの設定済みのブローカ設定、フリート内のクラウド接続されたポッドのタイプ、テナントの地域別クラウド プレーン、および特定のライセンスに基づく機能などの要因によって異なります。

異なるポッド タイプが混在する場合

Horizon ポッドと Microsoft Azure のポッドの両方がある場合、[割り当て] をクリックすると、テナントの構成済みの仲介設定、およびテナントが App Volumes の使用に対して有効になっているかどうかに応じてさまざまな選択肢が表示されます。

すべてのポッドが Horizon ポッドの場合

すべてのポッドが Horizon ポッドの場合、[割り当て] をクリックすると、新しいデスクトップ割り当てを作成して既存の割り当てを操作するアクションを開始できるページが表示されます。リストされた割り当てごとに、割り当ての名前をクリックすると、割り当てられているユーザーやその他の詳細など、その割り当てに関する詳細情報を確認できます。クラウド接続された Horizon ポッドのデスクトップ割り当ての詳細については、Universal Broker 環境での割り当ての作成および管理とそのサブトピック、および Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成を参照してください。

すべてのポッドが Microsoft Azure にある場合

Horizon ポッドがない場合、[割り当て] をクリックすると、新しい割り当てを作成するアクションと既存の割り当てを操作するアクションを実行するための選択肢にアクセスできます。割り当て関連のページでは、リストされた割り当てごとに、割り当ての名前をクリックすると、割り当てられているユーザーやその他の詳細など、その割り当てに関する詳細情報を確認できます。VDI デスクトップ割り当てをクリックすると、その割り当てに関する詳細情報を確認できるだけでなく、VDI デスクトップ割り当ての [デスクトップ] タブに移動して、VDI デスクトップ割り当てにある仮想デスクトップの一覧を表示したり、オプションでこれらのデスクトップにアクションを実行することもできます。

Microsoft Azure のポッドの割り当てを管理するための概要情報と、その他のドキュメント トピックへのリンクについては、Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた割り当ての管理を参照してください。

Horizon Cloud テナントのインベントリ内の資産の表示

Horizon Cloud テナントのインベントリには、RDSH ファーム、公開されたイメージ、アプリケーション、インポートされた仮想マシン (VM) などの資産が含まれています。資産は、エンド ユーザーに割り当てられたデスクトッ

プとリモート アプリケーションの派生元となる構成要素です。Horizon Universal Console の [インベントリ] を使用して、このインベントリおよびさまざまな資産にアクセスします。

注意: クラウドベースの Horizon Universal Console のツアーで説明されているように、第 1 世代のコンソールは動的であり、第 1 世代のテナント環境の最新の構成に適した機能を反映しています。このドキュメントで説明されている機能へのアクセスは、以下の要因（ただしこれらに限定されない）に依存する場合があります。

- その機能が最新の第 1 世代の Horizon Cloud ポッド マニフェスト、Horizon ポッドのバージョン、または Horizon Cloud Connector のバージョンでのみ使用可能なシステム コードに依存するかどうか。
- 機能が初登場したときに、リリース ノートに記載されているように制限付きで機能へのアクセスが提供されるかどうか。
- 機能に特定のライセンスまたは SKU が必要かどうか。

このドキュメントに機能の記載があり、第 1 世代のコンソールにその機能が表示されない場合は、まずリリース ノートを読み、その機能のアクセスが制限されているかどうか、およびテナントで有効化をリクエストする方法について確認します。または、このドキュメントに記載されている機能を使用する資格があり、コンソールにその機能が表示されない場合は、VMware Horizon Cloud Service の担当者に問い合わせるか、担当者がいない場合は Customer Connect でサポート リクエストを発行する方法 (VMware KB 2006985)の記載内容に従って、サービス リクエストを Horizon Cloud Service チームに発行することができます。

コンソールの動的な性質により、実際の環境では、ここでの説明とは異なるエントリとラベルが表示されることがあります。

注意: クラウド接続されたポッド フリートは、2 つの異なるポッド タイプで構成できます。Horizon ポッドは、Horizon Connection Server に基づいており、VMware SDDC ベースのプラットフォームにデプロイされているポッド タイプです。Horizon Cloud ポッドは、ポッド マネージャ テクノロジーに基づくポッド タイプであり、第 1 世代テナント - Microsoft Azure 上の Horizon Cloud ポッド - 第 1 世代 Horizon Universal Console の [キャパシティ] ページを使用した、ポッド フリートへのポッドの追加で説明されているように、Horizon Cloud ポッド デプロイヤによって Microsoft Azure にデプロイされます。

アプリケーション資産

[インベントリ] から、アプリケーション関連の資産をインベントリに追加し、それらの資産を管理するワークフローにアクセスします。このようなアプリケーション関連の資産には、App Volumes アプリケーションやファームベースのリモート アプリケーションが含まれます。Horizon Cloud インベントリ内のアプリケーションを参照してください。

ファーム資産

[インベントリ] から、RDSH ファームとその RDSH 仮想マシンを作成および管理するためのファーム関連のワークフローにアクセスします。Horizon Cloud のファーム とそのサブトピックを参照してください。

イメージ資産

[インベントリ] から、イメージ関連のワークフローにアクセスします。コンソールに表示される実際のラベルとページ、およびそれらのページがサポートする利用可能なワークフローは、現在ポッド フリートにあるポッドのタイプによって異なる場合があります。

ポッド フリートがクラウド接続された Horizon ポッドのみで構成されている場合

クラウド接続された Horizon ポッドは、Horizon Image Management Service の機能と、マルチポッド イメージ管理の使用をサポートします。マルチポッド イメージは、Horizon Image Management Service によって提供されます。マルチポッド イメージ管理のワークフローについては、クラウドからの Horizon イメージの管理ガイドを参照してください。

ポッド フリートに Microsoft Azure の 1 つ以上の Horizon Cloud ポッドが含まれる場合

Horizon Cloud ポッドは、Horizon Cloud インベントリでのポッドごとのイメージの使用をサポートします。ポッドごとのイメージのワークフローについては、次のトピックを参照してください。

- Microsoft Azure でのデスクトップ イメージと Horizon Cloud ポッドの作成およびそのサブトピック。
- Microsoft Azure での Horizon Cloud ポッドの公開イメージの管理およびそのサブトピック。

2021 年 7 月のサービス リリースでは、すべての Horizon Cloud ポッドがマニフェスト 2632 以降で、テナントが Universal Broker を使用するように構成されている場合に、それらのポッドで Horizon Image Management Service およびマルチポッド イメージ管理の機能を使用することができます。マルチポッド イメージ管理のワークフローについては、クラウドからの Horizon イメージの管理ガイドを参照してください。

インポートされた仮想マシン資産

[インベントリ] から、Microsoft Azure の単一の Horizon Cloud ポッドで基本イメージ仮想マシンの自動作成とインポートを開始したり、リストされた仮想マシンでのパワーオフやパワーオンなどの操作を実行したりするページにアクセスします。このページにリストされた仮想マシン (VM) は、次の方法で Horizon Cloud 環境に配置された仮想マシンです。

- ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリングの手順に従い、[インポートされた仮想マシン] ページの [インポート] アクション ボタンを使用してポッドごとに作成してインポートした仮想マシン。
- Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートするの手順に従って手動で作成されたときに、システムがポッドの *podID*-base-vms リソース グループからインポートした仮想マシン。

仮想マシンをファームまたは VDI デスクトップ割り当てで使用できるようにするには、その仮想マシンを公開済みの状態に変換する必要があります。これは、イメージのシーリングとも呼ばれます。[インポートされた仮想マシン] ページには、リストされたベース仮想マシンを公開済みの状態に変換するアクションが含まれていますが、このページのアクションを使用するのではなく、通常は前述のセクション イメージ資産 に記載されているイメージ関連のページを使用してシールドされた公開イメージを作成します。シーリングする前に、必要なすべてのアプリケーションとドライバが仮想マシンにインストールされていることを確認してください。

Microsoft Azure の Horizon Cloud ポッドの場合、ページの [エージェント ペアリングのリセット] アクションは、ポッド マネージャとインポートされた仮想マシン内のエージェント間のキー交換を管理するエージェントの状態を更新して、二者間の接続を保護します。これらの安全な接続を確立するためにキーのペアが使用されるため、ペアリングという用語は、このキーの交換を説明するために使用されます。通常、このワークフローは次のシナリオで使用します。

- ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリングを使用して最近インポートされた仮想マシンの場合：このシナリオでは、このアクションにより、ワークフローが仮想マシンにインストールしたエージェント ソフトウェアが再起動され、ペアリングが完了します。

  Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートするを使用して手動で作成し、エージェント ソフトウェアをインストールした仮想マシンの場合：このシナリオでは、このアクションにより、ワークフローが仮想マシンにインストールしたエージェント ソフトウェアが再起動され、ペアリングが完了します。

  [エージェントのステータス] 列にエラー メッセージが表示されているリストされた仮想マシンの場合：このシナリオでは、このアクションはエージェント ソフトウェアを再起動してペアリングの障害を修復し、ペアリングを完了します。

[インポートされた仮想マシン] ページに関するその他の注意事項：

- Microsoft Azure Marketplace からイメージをインポートするプロセスが失敗すると、失敗に関するシステム通知が生成され、[エージェントのステータス] 列に [失敗] リンクが表示されます。そのリンクをクリックすると、[通知] ページが開いて、失敗の原因を確認することができます。
- [インポートされた仮想マシン] ページは自動的には更新されません。アクションを実行した後、現在のステータスを確認するには、更新アクションをクリックする必要があります。たとえば、仮想マシンがパワーオフの状態で [パワーオン] アクションを選択すると、パワーオンのプロセスが開始したときにページには [進行中] と表示され、ページを更新するまでそのステータスが表示され続けます。
- テナント環境でマルチポッド イメージ管理機能を使用できる場合は、単一セッション VDI イメージである仮想マシンで [マルチポッド イメージに移動] アクションを使用できます。このアクションは主に、手動でインポートされた仮想マシンに対して、それらの仮想マシンをマルチポッド イメージ ワークフロー内で使用できるようにするために使用されます。

Horizon Universal Console の [設定] メニューについて

Horizon Cloud コンソールのナビゲーション バーの [設定] では、環境全体の設定、ID 管理、コンソールのロールベースのアクセス (RBAC) 設定、デプロイされたポッド、およびさまざまな関連設定や構成など、Horizon Cloud 環境のさまざまな側面を操作するためのページにアクセスできます。

[設定] をクリックして、コンソールの次のページにアクセスします。

注意: 第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアーで説明されているように、コンソールはテナント環境の現在の状態を動的に反映します。結果として、設定をクリックすると、以下で説明するようなエントリとラベルが表示される場合があります。通常は、このページがテナント環境の最新の状況に該当しない場合、コンソールはビューからページを非表示にします。

ユーザー インターフェイス ページ	説明
[全般設定]	この特定の Horizon Cloud テナント環境全体に適用される設定、たとえば、環境にログインできる My VMware ユーザー、そのロール、およびその他の同等の設定（ユーザー セッション情報の監視を有効または無効にするトグルなど）が表示されます。このページから設定を編集することができます。詳細については、Horizon Cloud テナント環境のカスタマイズ可能な全般設定を参照してください。
[Active Directory]	Active Directory (AD) の詳細を表示および編集し、環境に True SSO 機能を構成します。True SSO は、エンド ユーザーが Active Directory 認証情報を入力する必要なく自分のデスクトップおよび RDS ベースのリモート アプリケーションに接続する機能を提供します。Horizon Cloud - True SSO - Horizon Cloud 環境の True SSO の構成を完了するを参照してください。
[ユーザーとグループ]	エンド ユーザーのホーム サイト割り当てを管理します。Universal Broker のホーム サイトの構成を参照してください。
[役割と許可]	役割と許可を編集します。Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるを参照してください。
[キャパシティ]	各ポッドによる使用率やキャパシティの使用状況など、展開されたポッドの詳細を表示します。また、指定の NTP サーバ、関連する Microsoft Azure サブスクリプションのアプリケーション キーなど、ポッドに関連付けられた編集可能ないくつかのプロパティをドリルダウンして表示し、オプションで更新します。詳細については、3 章 第 1 世代テナント - 第 1 世代 Horizon Cloud がサポートするすべてのポッド タイプのクラウド接続ポッドの管理を参照してください。
[ID 管理]	コンソールでは、テナントがすでに Microsoft Azure のポッド フリートの Horizon Cloud ポッドにシングル ポッド仲介を使用するように構成されている場合にのみ、このページが表示されます。このテナント シナリオでは、このページを使用して、テナントとの VMware Workspace ONE® Access™ 環境の統合を構成します。
[ライセンス]	お使いの環境の現在のライセンスの詳細を表示します。これには、シート数や請求サイクル数が含まれます。また、ライセンスの SID をクリックして MyVMware のサブスクリプション リスト ページを開くことができます（MyVMware 認証情報を使用してログインする必要があります）。
[仮想マシンのタイプとサイズ]	Microsoft Azure のポッドのファームおよび割り当てで使用する仮想マシンのタイプとサイズを管理します。詳細については、Horizon Universal Console でのファームと割り当ての仮想マシン タイプとサイズの管理を参照してください。
[はじめに]	[はじめに] ウィザードを表示します。詳細については、Horizon Cloud の [はじめに] ウィザード - 概要を参照してください。
[ブローカ]	エンドユーザー セッションのタイムアウトを制御する設定など、システムがエンドユーザーにポッドをプロビジョニングしたリソースを仲介することに適用される設定を構成します。テナントが Universal Broker で構成されている場合、このページには、テナントと Workspace ONE Access および Workspace ONE Intelligent Hub との統合に適用される設定を構成するためのタブがあります。詳細については、Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合するを参照してください。

Horizon Cloud テナント環境のカスタマイズ可能な全般設定

Horizon Cloud テナント環境全体に適用される設定を変更するには、Horizon Universal Console の [全般設定] ページを使用します。

第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアーで説明されているように、コンソールはテナント環境の現在の状態を動的に反映します。その結果、[全般設定] ページに表示されるセクションと変更できる設定は、テナント環境の現在の状態に関連するものに限定されます。たとえば、クラウド接続されたポッドがすべて Horizon ポッドで、Microsoft Azure のポッドがない場合、このページでは Horizon ポッドに関連する設定のみが提供されます。Microsoft Azure に少なくとも 1 つのポッドがデプロイされている場合、[全般設定] ページではそのポッド タイプに関連する設定が使用可能です。

設定を変更するには、変更する設定を含むセクションの横にある鉛筆アイコンを使用します。編集ウィンドウが開き、そのセクションの設定が表示されます。そのウィンドウで設定を変更し、変更をシステムに保存します。

注： 次の設定を変更する場合は、更新内容を有効にするまでに最大 5 分程度かかります。

- [デスクトップ割り当てのオプション] セクションの [専用デスクトップ割り当て名を有効にする] 設定。
- [ドメイン セキュリティ設定] セクションの設定については、Horizon Cloud - [全般設定] ページでのドメイン セキュリティ設定に記載されています。

デフォルトのドメイン

環境内で登録されている Active Directory ドメインが 1 つしかない場合、そのドメインの名前がここに表示されます。複数の Active Directory ドメインを登録している場合、デフォルトの Active Directory ドメインとして指定されていて、管理者が管理コンソールにログインした際に使用する Active Directory ログイン ページのドメイン選択リストに最初に表示されるものがこのテキスト ボックスに表示されます。

この設定は、Active Directory ログイン ページのドメイン選択リストに最初に表示される Active Directory ドメインだけを制御するものです。Horizon Universal Console にログインして Horizon Cloud 環境で管理タスクを実行するに記載されているように、環境内に複数の Active Directory ドメインが登録されている場合は、Active Directory ログイン ページにドメイン選択リストが表示されます。この [デフォルトのドメイン] テキスト ボックスを使用して、Active Directory ドメインのいずれかをデフォルトとして指定することができます。そのデフォルト Active Directory ドメインは、Active Directory ログイン ページのドメイン選択リストに最初に表示されます。現在の設定を変更するには、[編集] をクリックします。

My VMware アカウント

ユーザーが Horizon Cloud にログインできるようにするために、ユーザーの My VMware アカウントを追加します。ここに My VMware 情報を追加したら、Active Directory ユーザー アカウントに自分のジョブまたはビジネス タスクに適したロールを割り当てます。Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるを参照してください。

通知の受信者

管理者以外の特定のユーザーまたはグループが Horizon Cloud 環境に関する E メール通知を受信できるようにするには、そのユーザーのメール アドレスを [通知の受信者] リストに追加します。

前述の My VMware アカウント リストには、さまざまなタイプの管理者が含まれる場合があります。ただし、管理者以外のユーザーまたはグループが、管理およびスケジュール設定されたメンテナンスの E メール通知などの E メール通知を受信するようにする場合は、[通知の受信者] セクションを使用してメール アドレスを追加します。

Horizon Cloud から生成されたすべての E メール通知は、リストされているすべてのメール アドレスに送信されます。

セッション タイムアウト

これらの設定は Horizon Cloud 環境への接続のタイムアウトを制御します。

- [管理ポータルのタイムアウト] 設定は、管理者がコンソールへのログインを継続できる時間を制御します。この時間が経過すると管理者の認証済みセッションが終了し、管理者は再度ログインする必要があります。

削除保護

[削除保護] 設定は、それぞれの専用デスクトップ割り当てにおいて 1 時間あたりの削除可能なデスクトップ仮想マシンの数を制御します。[専用デスクトップの一括削除 (1 時間あたり)] に対して次のオプションのいずれかを選択します。

- [無制限] - 無制限のデスクトップ仮想マシンを専用デスクトップ割り当てから削除できます。
- [なし] - [最大デスクトップ削除数] を使用して特定の割り当てを許可しない限り、デスクトップ仮想マシンを専用デスクトップ割り当てから削除することはできません（以下の注を参照）。
- [カスタム] - 1 時間あたりの専用デスクトップ割り当てから削除できるデスクトップ仮想マシンの数。[カスタム] を選択した場合は、このドロップダウン メニューの右側に数値も入力する必要があります。[最大デスクトップ削除数] を使用して、特定の割り当てから追加のデスクトップ仮想マシンを削除できるようにすることができます（以下の注を参照）。

注： [なし] または [カスタム] を選択した場合は、割り当てを作成または編集するときに、[デスクトップ削除の最大数] 設定を編集して、この制限が呼び出される前に特定の割り当ての追加の削除を行うことができます。[最大デスクトップ削除数] に 0 より大きい値を入力した場合、システムは、その数の仮想マシンの削除を許可した上で、[削除保護] に設定したレートに対してカウントします。

たとえば、[最大デスクトップ削除数] を値 10 で [カスタム] に設定し、[削除保護] を値 1 で [カスタム] に設定することができます。この場合、最初の 10 台の仮想マシンが削除された後（数が 10 になるまでの時間に関係なく）、システムはそれ以降、1 時間あたり 1 台の追加の仮想マシンのみを削除できます。

[削除保護] で [無制限] を選択した場合、[最大デスクトップ削除数] 設定を使用する必要はありません。

[最大デスクトップ削除数] 設定の詳細については、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 を参照してください。

専用デスクトップ割り当て内のすべての仮想マシンの削除を防止するには、[割り当て] ページの [削除の防止] 設定を使用します。専用デスクトップ割り当ての削除の防止または削除の許可を参照してください。

RDSH ファーム

セッション デスクトップまたはリモート アプリケーションを使用してログインしている Windows セッションがファームに設定された最大セッション時間に達したときに、Horizon Cloud でエンド ユーザーに対して表示するメッセージを指定できます。猶予期間が経過すると、システムはログインした Windows セッションからユーザーを強制的にログアウトします。

[猶予期間] テキスト ボックスには、システムの待機時間（リマインダ メッセージが送信されてからユーザーを強制的にログアウトするまで）を指定できます。

デスクトップ割り当てのオプション

この設定を使用して、エンド ユーザーがエンドユーザー クライアントを使用して割り当てられた仮想デスクトップにアクセスするときにエンド ユーザーに表示される仮想デスクトップの名前を構成します。この設定は、Microsoft Azure のポッドからプロビジョニングされた専用 VDI デスクトップ割り当てによってプロビジョニングされた仮想デスクトップにのみ適用されます。Horizon Cloud のデスクトップ割り当ての詳細については、Microsoft Azure の Horizon Cloud ポッドに基づくテナントのデスクトップ割り当ての概要を参照してください。

最初に、エンド ユーザーがエンドユーザー クライアントにログインし、専用 VDI デスクトップ割り当てから新しくプロビジョニングされたデスクトップを確認すると、クライアントには専用 VDI デスクトップ割り当ての名前が表示されます。この時点では、特定のデスクトップ仮想マシン (VM) はまだ専用のデスクトップ仮想マシンとしてエンド ユーザーに割り当てられていません。そのエンド ユーザーが仮想デスクトップを初めて起動する手順を実行すると、その時点で、システムはその初回の起動の結果として特定のデスクトップ仮想マシンをそのユーザー専用に使用します。その後のデスクトップ起動では、エンド ユーザーのクライアントに表示されるデスクトップの名前はここで選択した設定によって異なります。

重要：

- [専用デスクトップ割り当て名を有効にする] 設定の有効化は、ポッド マニフェスト バージョン 1900 以降のポッドに適用されます。ポッドのマニフェスト バージョンが 1900 よりも低い場合、このトグルの設定に関係なく、そのポッドからプロビジョニングされた仮想デスクトップに対してレガシーの動作が有効のままになります。
- この設定を変更する場合、更新内容が有効になるまでに最大 5 分かかる場合があります。
- このオプションは、Workspace ONE Access を使用するエンドユーザー接続には適用されません。エンドユーザーが Workspace ONE Access を使用して専用 VDI デスクトップ割り当てから使用資格のあるデスクトップにアクセスすると、Workspace ONE Access は割り当て名とユーザーの Horizon Client を表示し、HTML Access ポータルにはその後のデスクトップ起動用の仮想マシン名が表示されます。

- [専用デスクトップ割り当て名を有効にする] トグルが無効になっている場合、エンドユーザー クライアントには仮想デスクトップの基盤となる仮想マシンの名前が表示されます。仮想マシン名の表示はレガシーの動作です。
- [専用デスクトップ割り当て名を有効にする] トグルを有効にすると、エンドユーザー クライアントは、以降のデスクトップ起動の場合でも仮想デスクトップをプロビジョニングする専用 VDI デスクトップ割り当ての名前を引き続き表示します。

エージェント アップデート

[障害のしきい値] の設定は、更新プロセスが停止するまでに、Microsoft Azure のポッドでの専用デスクトップ割り当ての自動エージェント更新の失敗が許容されている仮想マシンの数を示しています。このしきい値により、大量の障害が発生するのを防ぎます。デフォルト値は 30 です。詳細については、Horizon Cloud ポッド - VDI デスクトップ割り当て、ファーム、公開イメージ、ベース仮想マシンにインストールされたエージェント関連ソフトウェアの更新を参照してください。

イメージ管理設定

これらの設定は、テナントのポッドのフリートに少なくとも 1 つの Horizon ポッドが含まれている場合に表示されます。これらの設定は、Horizon ポッドのイメージ管理サービス (IMS) 機能に適用されます。これらの設定を使用して、イメージ レプリケーションのプロセスを最適化します。イメージ管理サービスに関するすべての情報については、クラウドからの Horizon イメージの管理ドキュメントとそのサブトピックを参照してください。

ドメイン セキュリティ設定

これらの設定を使用して、Microsoft Azure のポッドに接続するために、さまざまな Horizon Client を使用する非認証ユーザーへの Active Directory ドメイン名の通信を防止します。これらの設定は、Active Directory ドメイン情報をクライアントに送信するかどうか、および、送信する場合、エンドユーザー クライアントのログイン ページにどのように表示するかを制御します。詳細については、Horizon Cloud - [全般設定] ページでのドメイン セキュリティ設定を参照してください。

重要：

- これらの設定は、同じ Horizon Cloud ユーザー アカウント（テナント）の下にある、Microsoft Azure にデプロイされているすべての環境のポッドに適用されます。
- ここで選択したオプションの組み合わせによって、クライアントのユーザー エクスペリエンスが変わります。特定の組み合わせでは、特に、より古いクライアント、コマンドライン クライアントを使用する場合、および環境に複数の Active Directory ドメインがある場合に、エンドユーザーがクライアント ログイン ページでドメイン情報を入力する方法の要件を設定できます。これらの設定がクライアントのユーザー エクスペリエンスに与える影響は、クライアントによって異なります。組織のセキュリティ ポリシーに応じて、エンドユーザー エクスペリエンスのバランスを取る必要がある場合があります。詳細については、Horizon Cloud - [全般設定] ページでのドメイン セキュリティ設定を参照してください。
- ポッド マニフェスト バージョン 1273 以降にまだ更新されていない Microsoft Azure のポッドが Horizon Cloud 環境にある場合、[全般設定] ページにこの [ドメイン セキュリティの設定] セクションが表示されません。これらのコントロールにアクセスするには、Microsoft Azure のすべてのポッドをこのリリースに更新してください。
- すべてのポッドがポッド マニフェスト バージョン 1273 以降に更新されるまで、以前の Horizon Cloud リリースと同じ動作を提供するようにデフォルトで環境が構成されます。すべてのポッドがこのリリース レベルになるまで、システムは Active Directory ドメイン名をエンドユーザー クライアントに送信し、クライアントは Active Directory ドメイン ドロップダウン メニューを表示するレガシー動作となります。

  その後、すべてのポッドのマニフェストがバージョン 1273 以降になると、これらの設定は [全般設定] ページに表示されます。その時点で、表示される設定にはレガシー動作 (両方のコントロールが[いいえ]に設定されています) が反映され、クライアントに対するドメイン情報の通信を制御するように変更できます。

ポッドの現在のマニフェスト バージョンを表示するには、3 章 第 1 世代テナント - 第 1 世代 Horizon Cloud がサポートするすべてのポッド タイプのクラウド接続ポッドの管理 を使用します。このリリースのポッド マニフェスト バージョンについては、Horizon Cloud のドキュメント ページからリンクされているリリース ノート ページを参照してください。

監視

Cloud Monitoring Service (CMS) は、監視とレポートの目的で、接続されたポッドからセッション、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。CMS は、Horizon Cloud で提供される中心的なサービスの 1 つです。CMS の概要については、2 章 第 1 世代のテナント - 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 デスク機能の紹介を参照してください。

- Cloud Monitoring Service を有効または無効にするには、[Cloud Monitoring Service] トグルを使用します。これはデフォルトでは有効になっています。

この設定を無効にすると、以下の [セッション データ] 設定が表示されなくなります。

- Cloud Monitoring Service が有効になっている場合は、[セッション データ] トグルを使用して、エンド ユーザーのセッションに関連するユーザー情報の追跡をオプトインまたはオプトアウトすることができます。収集された情報には、ユーザーごとのログイン時刻、セッションの接続時間、および平均のセッションの長さが含まれます。

  ユーザー データの収集をオプトインすると、サービスはこの情報を収集し、第 1 世代の Horizon Cloud 環境を使用している間維持します。「VMware ナレッジベースの記事 KB91183」で説明されているように、このデータは Workspace ONE Intelligence で入手できます。[セッション データ] トグルをオフにすると、収集したデータを削除できます。

  ユーザー データの収集をオプトアウトし、監視サービスを有効にすると、サービスは一定期間セッション データを収集し、ユーザー名をハッシュしてリアルタイム管理を可能にします。その結果、Horizon ユーザー使用量レポートなどの一部のレポートは使用できません。この場合、システムは、接続されたポッド内のアプリケーションおよびデスクトップに関連する他のデータの収集も継続します。

Cloud サービス プロバイダ

このセクションでは、テナント環境が VMware Cloud Service Engagement Platform にオンボーディングされているかを示します。VMware Cloud Service Engagement Platform へのオンボーディングについては、第 1 世代テナント - Horizon Universal Console を使用して Horizon Cloud テナントを VMware Cloud Services Engagement Platform および VMware Cloud Services にオンボーディングするを参照してください。

Pendo 分析とガイド

コンソールには、VMware Cloud Services ログイン方法を使用して Horizon Cloud テナントにログインしている場合にのみ、このセクションが表示されます。Horizon Cloud ログイン画面で My VMware 認証情報を使用してログインした場合、コンソールにはこのセクションは表示されません。

このセクションには、Pendo 分析とガイドに基づいて、Workspace ONE サービス機能の現在の有効化状態が示されます。VMware Cloud Services ログイン方法を使用してテナントにログインすると、Pendo 関連の機能がデフォルトで有効になります。

Pendo 関連の機能について確認し、必要に応じて現在の設定を変更するには、[編集]（鉛筆アイコン）をクリックします。このアイコンをクリックすると、コンソールは、Workspace ONE コンソールの Cookie 使用状況ページにリダイレクトされます。このページには、Pendo 関連の機能に関する情報が表示され、設定を変更するためのトグルが表示されます。

Workspace ONE コンソールの Cookie 使用状況ページで行った変更を Horizon Universal Console の [全般設定] ページに反映させるには、[全般設定] ページを更新します。

Horizon Cloud - [全般設定] ページでのドメイン セキュリティ設定

これらの設定を使用して、さまざまな Horizon Client を使用する非認証ユーザーへの Active Directory ドメイン名の通信を防止します。これらの設定は、Horizon Cloud 環境に登録されている Active Directory ドメインに関する情報を、Horizon エンドユーザー クライアントに送信するかどうか、および送信する場合はエンドユーザー クライアントのログイン画面にどのように表示するかを制御します。

環境の構成には、Active Directory ドメインへの環境の登録が含まれます。エンドユーザーが、使用資格のある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 Horizon Client を使用すると、それらのドメインは使用資格が付与されたアクセスに関連付けられます。2019 年 3 月の四半期ごとのサービスリリース以前は、システムとクライアントにはデフォルトの動作があり、そのデフォルトの動作を調整するオプションはありませんでした。2019 年 3 月のリリース以降では、デフォルトが変更されると共に、オプションで新しいドメイン セキュリティ設定コントロールを使用してデフォルトから変更できます。

重要： これら設定を変更する場合、更新内容が有効になるまでに最大 5 分かかる場合があります。

このトピックには次のセクションが含まれています。

- ドメイン セキュリティ設定
- 過去のリリースと比較したこのリリースのデフォルト動作
- ポッドのマニフェスト レベルとの関係
- 単一の Active Directory ドメインのシナリオとユーザーのログイン要件
- 複数の Active Directory ドメインのシナリオとユーザーのログイン要件
- 2 要素認証で構成された Unified Access Gateway インスタンスを使用する Microsoft Azure 内のポッドについて

ドメイン セキュリティ設定

これらの設定の組み合わせは、ドメイン情報をクライアントに送信するかどうか、およびクライアントのエンドユーザーがドメイン選択メニューを使用できるかどうかを決定します。

重要： これらの設定は、同じ Horizon Cloud 環境内にある Microsoft Azure 内のすべての Horizon Cloud ポッドに適用されます。同じ Horizon Cloud ユーザー アカウント（テナント）を使用して Microsoft Azure にデプロイされているポッドはすべて、同じ組み合わせになります。ポッドに接続しているすべてのエンドユーザーは、どのポッドが仮想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しているかにかかわらず、これらの設定に従って動作を受け取ります。

注意： これらの設定により、クライアントのユーザー エクスペリエンスが変更されます。バージョン 5.0 より前の Horizon Client のバージョンを使用するエンドユーザーの動作は、Horizon Client 5.0 以降とは異なります。特定の組み合わせでは、特に、より古いクライアント、コマンドライン クライアントを使用する場合、および環境が複数の Active Directory を使用して構成されている場合に、エンドユーザーがクライアント ログイン画面でドメイン情報を指定する方法の要件を設定できます。これらの設定がクライアントのユーザー エクスペリエンスに与える影響は、クライアントによって異なります。組織のセキュリティ ポリシーに応じて、エンドユーザー エクスペリエンスのバランスを取る必要がある場合があります。単一の Active Directory ドメインのシナリオとユーザーのログイン要件および複数の Active Directory ドメインのシナリオとユーザーのログイン要件のセクションを参照してください。

表 1-7. [全般設定] ページのドメイン セキュリティ設定

オプション	説明
[デフォルトのドメインのみを表示]	このオプションは、ユーザー認証の前に、システムが接続先クライアントに送信するドメイン情報を制御します。 ■ [はい] - システムは文字列値 `*DefaultDomain*` のみを送信します。 ■ [いいえ] - システムは、登録されている Active Directory ドメイン名のリストをクライアントに送信します。
[ドメイン フィールドを非表示にする]	このオプションは、[[デフォルトのドメインのみを表示]] 設定に基づいて、クライアントに送られるドメイン関連情報のクライアントのログイン画面における表示を制御します。 ■ [はい] - [デフォルトのドメインのみを表示] の設定に関わらず、クライアントのログイン画面にはドメインに関する情報は表示されません。文字列値 `*DefaultDomain*` もドメイン名もクライアントのログイン画面に表示されません。 ■ [いいえ] - クライアントのログイン画面には、[デフォルトのドメインのみを表示] 設定に応じて次のいずれかの項目が表示されます。 ■ [デフォルトのドメインのみを表示] が [はい] の場合は、文字テキスト`*DefaultDomain*`。この組み合わせは、バージョン 5.0 よりも古い Horizon Client におけるユーザー エクスペリエンスを最適化する一方で、セキュリティも向上させます。 ■ [デフォルトのドメインのみを表示] が [いいえ] の場合は、ドロップダウン メニューのドメイン名のリスト。

過去のリリースと比較したこのリリースのデフォルト動作

次の表では、以前のデフォルト動作、新しいデフォルト動作、および組織のニーズに合わせて動作を調整するための設定について説明します。

以前のリリースのデフォルト動作	このリリースのデフォルト動作	このリリースのデフォルト動作に対応するドメイン セキュリティ設定の組み合わせ
システムは登録された Active Directory ドメイン名をクライアントに送信します。	システムは、文字列値 (`*DefaultDomain*`) だけをクライアントに送信し、登録された Active Directory ドメイン名は送信しません。 **注：** 文字列を送信することで、ドメイン名の文字列リストを想定するために実装された古い Horizon Client がサポートされます。	[デフォルトのドメインのみを表示] デフォルト設定：[はい]
クライアントにはログイン画面にドロップダウン メニューが表示され、ログインする前にエンドユーザーがドメインを選択するための登録済み Active Directory ドメイン名のリストが示されます。	クライアントには文字列 `*DefaultDomain*` が表示されます。	[ドメイン フィールドを非表示にする] デフォルト設定：[いいえ]

ポッドのマニフェスト レベルとの関係

以前のサービス リリースで作成されたポッドを持つ既存のユーザーである場合は、Microsoft Azure 内のすべてのポッドがこの Horizon Cloud リリースのマニフェスト レベルに更新されるまで、以前の Horizon Cloud リリースと同じ動作を提供するために、環境はデフォルトで設定されます。その以前の動作とは次のとおりです。

- システムによって Active Directory ドメイン名がクライアントに送信されます（[デフォルトのドメインのみを表示] が [いいえ] に設定）。
- クライアントには、ログインする前にエンドユーザーにドメイン名のリストを表示するドロップダウン メニューがあります（[ドメイン フィールドを非表示にする] が [いいえ] に設定）。

また、すべてのポッドがこのサービス リリース レベルになるまで、[全般設定] ページにはドメイン セキュリティ設定のコントロールが表示されません。更新されていない既存のポッドと、このリリース レベルで新たにデプロイされたポッドが混在する環境では、新しいコントロールは使用できません。その結果、すべてのポッドがこのサービス リリース レベルになるまで、以前の動作を変更することはできません。

環境のすべてのポッドがアップグレードされると、Horizon Cloud 管理コンソールで設定を使用できるようになります。更新後のデフォルト設定は、更新前の動作に設定されます（[デフォルトのドメインのみを表示] が [いいえ]、かつ [ドメイン フィールドを非表示にする] が [いいえ]）。更新後のデフォルト設定は、新しいユーザーのデフォルト値とは異なります。これらの設定は、組織のセキュリティ ニーズに合わせて設定を変更することを選択するまで、更新後のエンドユーザーに対して更新前のレガシー動作が継続するように適用されます。

単一の Active Directory ドメインのシナリオとユーザーのログイン要件

次の表では、環境内に単一の Active Directory ドメインがあり、2 要素認証を使用しておらず、エンドユーザーが Horizon Client 5.0 以降のバージョンを使用する場合の、さまざまな設定の組み合わせの動作について説明します。

表 1-8. Horizon Client 5.0 以降のバージョンで、1 つの Active Directory ドメインがある場合の動作

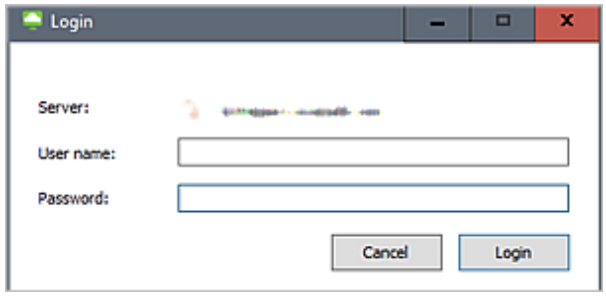
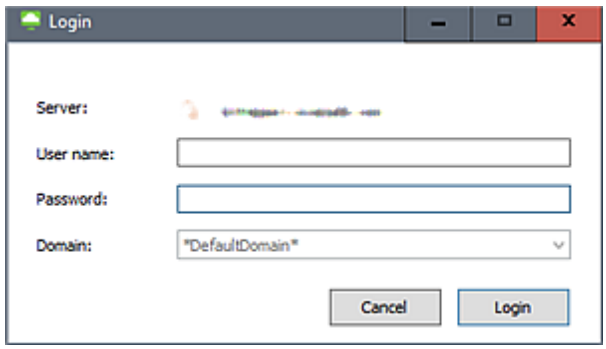
デフォルトのドメインのみを表示（有効な送信 `*DefaultDomain*`）	ドメインフィールドを非表示にする	Horizon Client 5.0 ログイン画面の詳細	ユーザーのログイン方法
はい	はい	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。ドメインフィールドが表示されません。ドメイン名は送信されません。 次のスクリーンショットは、Windows クライアントのログイン画面の表示についての例です。 	ログインするドメインが 1 つだけの場合、[ユーザー名] テキスト ボックスに次のいずれかの値を入力できます。ドメイン名は不要です。 ■ `username` ■ `domain\username` コマンドライン クライアントの起動を使用し、コマンドでドメインを指定すると機能します。
はい	いいえ	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。[ドメイン] フィールドには、`*DefaultDomain*` と表示されます。ドメイン名は送信されません。 次のスクリーンショットは、Windows クライアントのログイン画面の表示についての例です。 	ログインするドメインが 1 つだけの場合、[ユーザー名] テキスト ボックスに次のいずれかの値を入力できます。ドメイン名は不要です。 ■ `username` ■ `domain\username` コマンドライン クライアントの起動を使用し、コマンドでドメインを指定すると機能します。

表 1-8. Horizon Client 5.0 以降のバージョンで、1 つの Active Directory ドメインがある場合の動作 （続き）

デフォルトのドメインのみを表示（有効な送信 *DefaultDomain*）	ドメイン フィールドを非表示にする	Horizon Client 5.0 ログイン画面の詳細	ユーザーのログイン方法
いいえ	はい	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。ドメインフィールドが表示されません。システムによって、ドメイン名がクライアントに送信されます。 **注：** この組み合わせは、典型的なものです。通常、システムがドメイン名を送信している場合でも、ドメインフィールドを非表示にするため、この組み合わせは通常は使用されません。 ログイン画面は、この表の最初の行と同じように見えますが、ドメインフィールドは表示されません。	エンドユーザーは、[ユーザー名]テキストボックスにドメイン名を含める必要があります。 ■ `domain\username`
いいえ	いいえ	クライアントのログイン画面には、標準のユーザー名とパスワードのフィールドがあり、標準のドロップダウン ドメイン セレクタには使用可能なドメイン名が 1 つ表示されます。ドメイン名が送信されます。	エンドユーザーは、[ユーザー名]テキストボックスにユーザー名を指定して、クライアントに表示されるリストにある単一のドメインを使用することができます。 コマンドライン クライアントの起動を使用し、コマンドでドメインを指定すると機能します。

この表は、環境に単一の Active Directory ドメインがあり、エンドユーザーが以前のバージョンの Horizon Client（5.0 より前）を使用している場合の動作について説明します。

重要： 以前の（5.0 より前の）クライアントのコマンドライン クライアント起動を使用し、コマンドでドメインを指定すると、以下のすべての組み合わせに対して失敗します。この動作を回避するには、コマンドのドメイン オプションに `*DefaultDomain*` を使用するか、クライアントを 5.0 バージョンに更新します。ただし、複数の Active Directory ドメインがある場合は、`*DefaultDomain*` の受け渡しが機能しません。

表 1-9. 古い Horizon Client（5.0 より前）と 1 つの Active Directory ドメインがある場合の動作

デフォルトのドメインのみを表示（有効な送信 *DefaultDomain*）	ドメイン フィールドを非表示にする	5.0 より前 Horizon Client ログイン画面の詳細	ユーザーのログイン方法
はい	はい	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。ドメインフィールドが表示されません。ドメイン名は送信されません。	エンドユーザーは、[ユーザー名]テキストボックスにドメイン名を含める必要があります。 ■ `domain\username`
はい	いいえ	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。[ドメイン] フィールドには、`*DefaultDomain*` と表示されます。ドメイン名は送信されません。	エンドユーザーは、[ユーザー名] テキストボックスに `username` を入力する必要があります。ドメイン名が含まれていると、指定したドメイン名がドメイン リストに存在しないというエラー メッセージが表示されます。

表 1-9. 古い Horizon Client（5.0 より前）と 1 つの Active Directory ドメインがある場合の動作 （続き）

デフォルトのドメインのみを表示（有効な送信 *DefaultDomain*）	ドメイン フィールドを非表示にする	5.0 より前 Horizon Client ログイン画面の詳細	ユーザーのログイン方法
いいえ	はい	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。ドメインフィールドが表示されません。システムによって、ドメイン名がクライアントに送信されます。 **注：** この組み合わせは、典型的なものです。通常、システムがドメイン名を送信している場合でも、ドメインフィールドを非表示にするため、この組み合わせは通常は使用されません。 ログイン画面は、この表の最初の行と同じように見えますが、ドメインフィールドは表示されません。	エンドユーザーは、[ユーザー名]テキストボックスにドメイン名を含める必要があります。 ■ `domain\username`
いいえ	いいえ	クライアントのログイン画面には、標準のユーザー名とパスワードのフィールドがあり、標準のドロップダウン ドメイン セレクタには使用可能なドメイン名が 1 つ表示されます。ドメイン名が送信されます。	エンドユーザーは、[ユーザー名]テキストボックスにユーザー名を指定して、クライアントに表示されるリストにある単一のドメインを使用することができます。

複数の Active Directory ドメインのシナリオとユーザーのログイン要件

次の表では、環境内に複数の Active Directory ドメインがあり、2 要素認証を使用しておらず、エンドユーザーが Horizon Client 5.0 以降のバージョンを使用する場合の、さまざまな設定の組み合わせの動作について説明します。

基本的に、エンドユーザーはユーザー名を `domain\username` のようにドメイン名を含めて入力する必要があります。ただし、ドメイン名が送信されていてクライアントで表示されるレガシーの組み合わせの場合を除きます。

表 1-10. Horizon Client 5.0 以降のバージョンで、複数の Active Directory ドメインがある場合の動作

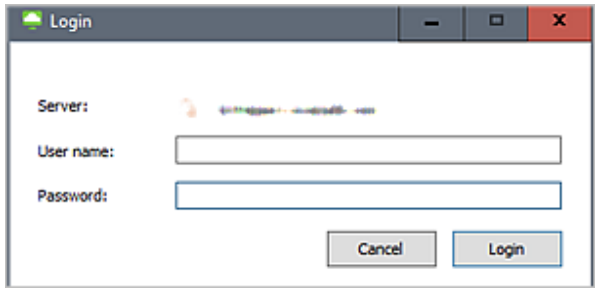
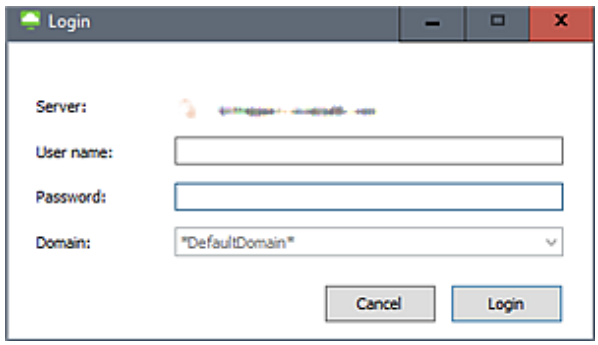
デフォルトのドメインのみを表示（有効な送信 `*DefaultDomain*`）	ドメイン フィールドを非表示にする	Horizon Client 5.0 ログイン画面の詳細	ユーザーのログイン方法
はい	はい	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。ドメインフィールドが表示されません。ドメイン名は送信されません。 次のスクリーンショットは、Windows クライアントのログイン画面の表示についての例です。 	エンドユーザーは、[ユーザー名]テキストボックスにドメイン名を含める必要があります。 ■ `domain\username` コマンドライン クライアントの起動を使用し、コマンドでドメインを指定すると機能します。
はい	いいえ	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。[ドメイン] フィールドには、`*DefaultDomain*` と表示されます。ドメイン名は送信されません。 次のスクリーンショットは、Windows クライアントのログイン画面の表示についての例です。 	エンドユーザーは、[ユーザー名]テキストボックスにドメイン名を含める必要があります。 ■ `domain\username` コマンドライン クライアントの起動を使用し、コマンドでドメインを指定すると機能します。

表 1-10. Horizon Client 5.0 以降のバージョンで、複数の Active Directory ドメインがある場合の動作 （続き）

デフォルトのドメインのみを表示（有効な送信 *DefaultDomain*）	ドメイン フィールドを非表示にする	Horizon Client 5.0 ログイン画面の詳細	ユーザーのログイン方法
いいえ	はい	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。ドメインフィールドが表示されません。システムによって、ドメイン名がクライアントに送信されます。 **注：** この組み合わせは、典型的なものです。システムがドメイン名を送信している場合でも、ドメイン フィールドを非表示にするため、この組み合わせは通常使用されません。 ログイン画面は、この表の最初の行と同じように見えますが、ドメイン フィールドは表示されません。	エンドユーザーは、[ユーザー名]テキスト ボックスにドメイン名を含める必要があります。 ■ `domain\username`
いいえ	いいえ	クライアントのログイン画面には、標準のユーザー名とパスワードのフィールドがあり、標準のドロップダウン ドメイン セレクタには使用可能なドメイン名のリストが表示されます。ドメイン名が送信されます。	エンドユーザーは、[ユーザー名] テキスト ボックスにユーザー名を指定して、クライアントに表示されるリストからドメインを選択することができます。 コマンドライン クライアントの起動を使用し、コマンドでドメインを指定すると機能します。

この表は、環境に複数の Active Directory ドメインがあり、エンドユーザーが以前のバージョンの Horizon Client（5.0 以前）を使用している場合の動作について説明します。

重要：

- [ドメイン フィールドを非表示にする] 設定を [はい] に設定すると、エンドユーザーはこれらの 5.0 以前の Horizon Client において [ユーザー名] テキスト ボックスにドメインを入力することができるようになります。複数のドメインがあり、5.0 より前の Horizon Client の使用をサポートする場合は、[ドメイン フィールドを非表示にする] を [はい] に設定して、エンドユーザーがユーザー名を入力するときにドメイン名を含めることができるようにする必要があります。
- 以前の（5.0 より前の）クライアントのコマンドライン クライアント起動を使用し、コマンドでドメインを指定すると、以下のすべての組み合わせに対して失敗します。複数の Active Directory ドメインがあり、コマンドライン クライアントの起動を使用する場合の唯一の回避方法は、クライアントを 5.0 バージョンに更新することです。

表 1-11. 古い Horizon Client（5.0 より前）と複数の Active Directory ドメインがある場合の動作

デフォルトのドメインのみを表示（有効な送信 *DefaultDomain*）	ドメイン フィールドを非表示にする	5.0 より前 Horizon Client ログイン画面の詳細	ユーザーのログイン方法
はい	はい	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。ドメインフィールドが表示されません。ドメイン名は送信されません。	エンドユーザーは、[ユーザー名]テキストボックスにドメイン名を含める必要があります。 ■ `domain\username`
はい	いいえ	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。[ドメイン] フィールドには、`*DefaultDomain*` と表示されます。ドメイン名は送信されません。	この組み合わせは、複数の Active Directory ドメインがある環境ではサポートされません。
いいえ	はい	クライアントのログイン画面には、標準のユーザー名フィールドとパスワードフィールドがあります。ドメインフィールドが表示されません。システムによって、ドメイン名がクライアントに送信されます。 **注：** この組み合わせは、典型的なものです。システムがドメイン名を送信している場合でも、ドメイン フィールドを非表示にするため、この組み合わせは通常使用されません。	エンドユーザーは、[ユーザー名]テキストボックスにドメイン名を含める必要があります。 ■ `domain\username`
いいえ	いいえ	クライアントのログイン画面には、標準のユーザー名とパスワードのフィールドがあり、標準のドロップダウン ドメイン セレクタには使用可能なドメイン名が 1 つ表示されます。ドメイン名が送信されます。	エンドユーザーは、[ユーザー名] テキスト ボックスにユーザー名を指定して、クライアントに表示されるリストからドメインを選択することができます。

2 要素認証で構成された Unified Access Gateway インスタンスを使用する Microsoft Azure 内のポッドについて

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で説明されているように、ポッドを Microsoft Azure にデプロイするときには、その Unified Access Gateway インスタンスに構成された 2 要素認証を使用したデプロイを選択することができます。

Microsoft Azure 内のポッドが 2 要素認証を使用した Unified Access Gateway 構成を持っている場合、Horizon Client で認証するエンドユーザーには、最初に 2 要素認証情報を求める画面が表示され、次に Active Directory ドメインの認証情報を求めるログイン画面が表示されます。この場合、システムは、エンドユーザーの認証情報が正常に初期認証画面に適合した場合に限って、ドメイン リストをクライアントに送信します。

一般的に、すべてのポッドで Unified Access Gateway インスタンスに 2 要素認証が構成されている場合、システムによってドメイン リストがクライアントに送信され、クライアントにドメイン ドロップダウン メニューが表示されるようにする必要があります。この構成では、使用している Horizon Client のバージョンや、Active Directory ドメインの数に関係なく、すべてのエンドユーザーに同じレガシー エンドユーザー エクスペリエンスが提供されます。エンドユーザーが 2 要素認証パスコードの手順を問題なく完了すると、2 回目のログイン画面のドロップダウン メニューからドメインを選択できます。最初の認証画面に認証情報を入力するときに、ドメイン名を含める必要がなくなります。

ただし、ドメインのセキュリティ設定は Horizon Cloud ユーザーアカウント（テナント）レベルで適用されるため、一部のポッドで 2 要素認証が構成されていない場合、エンドユーザーがログインする前に、それらのポッドが接続するクライアントにドメイン名を送信してしまうので、ドメイン リストを送信しないようにした方がいい場合があります。

重要： ポッドの 2 要素認証構成で [ユーザー名を維持] が [はい] に設定されている場合、[ドメイン フィールドを非表示にする] が [いいえ] に設定されていることを確認してください。そうしないと、システムがログイン認証情報を関連付けるために必要なドメイン情報を、エンドユーザーが提供することができません。

Horizon Client のエンドユーザーのログイン要件は、単一の Active Directory ドメインのシナリオとユーザーのログイン要件および複数の Active Directory ドメインのシナリオとユーザーのログイン要件に記載されているものと同じパターンに従います。2 要素認証が構成されているポッドに接続するときに複数の Active Directory ドメインがある場合、[ドメイン フィールドを非表示にする] が [はい] に設定されているのであれば、エンドユーザーはドメイン名を `domain\username` として指定する必要があります。

Horizon Cloud - 廃止 - [ファイル共有] ページ

Horizon Universal Console での [ファイル共有] ページの使用は廃止されました。その結果、このページが表示されても、ページには情報が表示されません。通常、環境内に Microsoft Azure にデプロイされたポッドしかない場合は、このページはコンソールに表示されません。

第 1 世代のテナント - Horizon Universal Console を使用したライセンス情報の取得

このドキュメント ページでは、第 1 世代の Horizon Universal Console が第 1 世代の Horizon Cloud 環境からライセンス関連情報を取得するために提供する方法について説明します。

Horizon Cloud テナントには、さまざまなタイプのライセンス関連情報を関連付けることができます。これらのタイプには通常、VMware Horizon サブスクリプション ライセンス、VMware 基本製品のキー（Horizon ライセンスに含まれている場合）、テナントで使用できるアドオン ライセンスなどがあります。

注： すべての VMware SKU が、VMware の基本製品、またはすべての基本製品（vSphere、vSAN、vCenter などの製品）のライセンスの対象となるわけではありません。Horizon Cloud Service アカウントに関連付けられている VMware SKU が VMware 基本製品ライセンスの対象外の場合、コンソールの [生成] アクションでその基本製品のキーは生成されません。

VMware 基本製品のキーを取得するためにのみログインする

Horizon Cloud テナントに関連付けられているライセンスに vSphere、vSAN、vCenter などの VMware 基本製品が含まれ、Horizon Cloud 顧客管理者ロールで Horizon Universal Console にログインすると、コンソールの [はじめに] ページに [無期限キーの表示] リンクが表示されます。

前述の要件を満たしていない場合、コンソールには [無期限キーの表示] リンクは表示されません。

次のスクリーンショットは、前述の要件を満たしている場合にのみ [はじめに] ページにこの [無期限キーの表示] リンクが表示される場所を示しています。

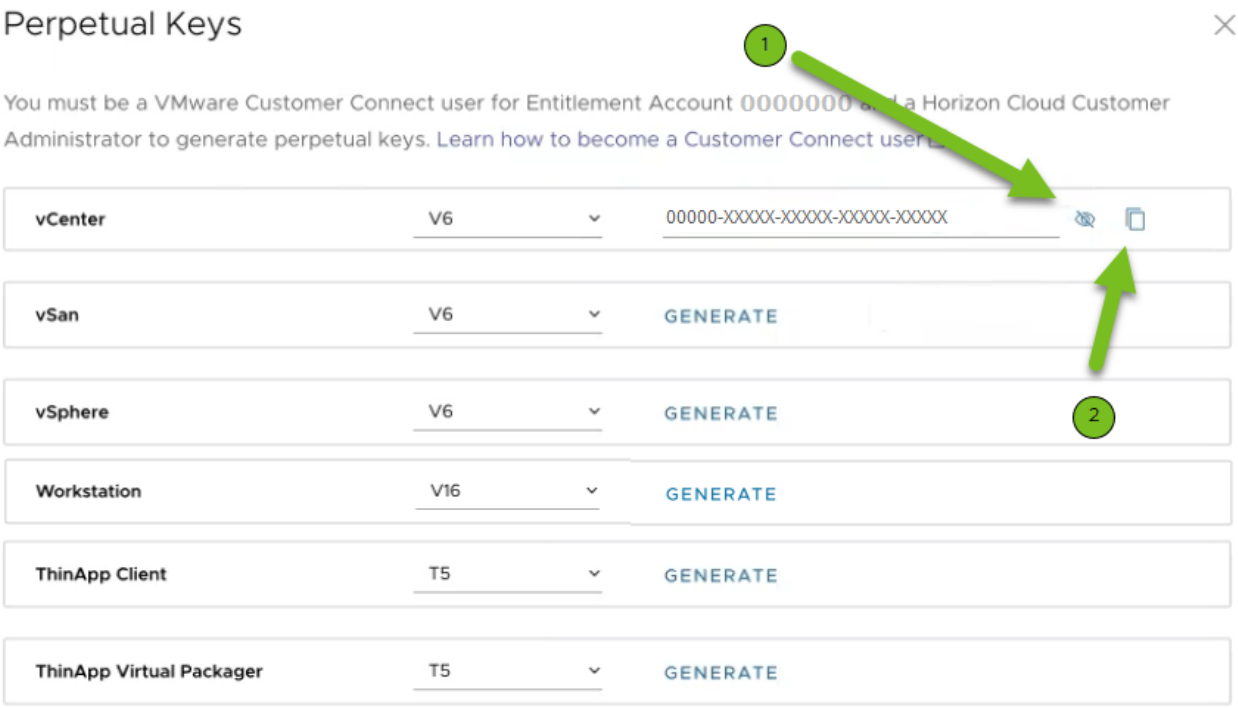
このリンクが表示された場合は、そのリンクをクリックすると、次の機能を提供するユーザー インターフェイス画面が表示されます。

- Horizon Cloud 顧客管理者ロールを持つテナントの管理者の 1 人によって以前に生成されたプロダクト キーの表示とコピー。
- ログイン時に VMware Customer Connect ユーザーという要件を満たしている場合は、プロダクト キーを生成します。VMware Customer Connect に関連付けられたログインでのみ、[生成] 機能を使用できます。

キーの表示またはコピー

[無期限キーの表示] をクリックすると、次のスクリーンショットに示すユーザー インターフェイス画面が表示されます。この画面には、このテナントに関連付けられている可能性のあるさまざまな VMware 基本製品が一覧表示されています。このユーザー インターフェイスには、キーがすでに生成されている製品と生成されていない製品が示されます。

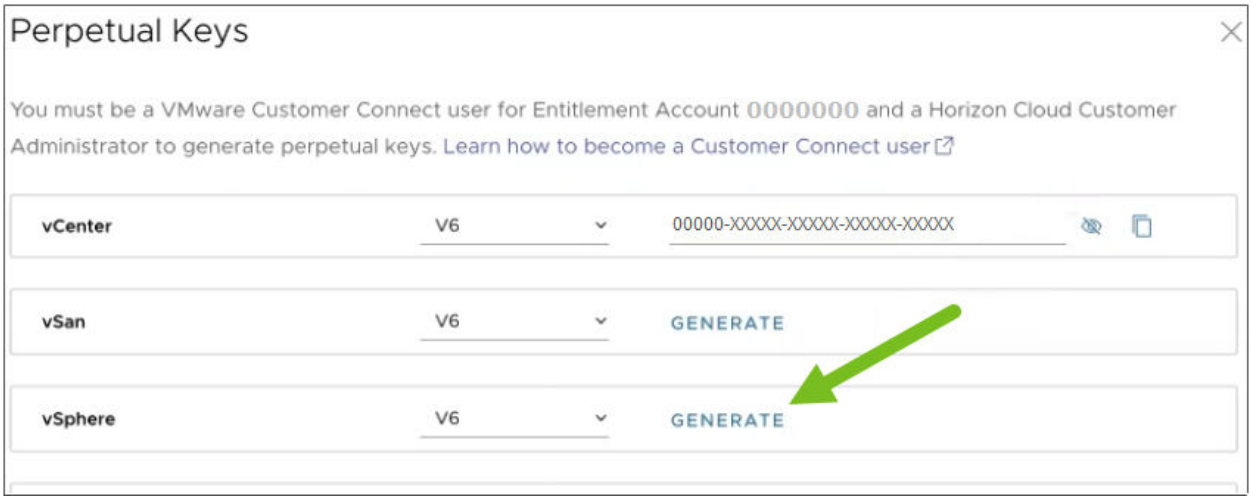
以前に生成されたキーの場合は、キーの行のアイコンを使用してキーを表示するか、キーをコピーします。次のスクリーンショットでは、コールアウト [1] はキーの表示を切り替えるアイコンを指し、コールアウト [2] はキーをクリップボードにコピーするアイコンを指します。



キーの生成

表示される無期限キーのリストを見るときに、VMware Customer Connect ユーザーのログインである場合は、特定の VMware 製品の新しいキーを生成できます。製品のドロップダウン リストからバージョンを選択し、[生成] をクリックします。

注： ライセンスは、VMware Customer Connect ポータルに表示されます。コンソールの [生成] アクションを使用して生成した無期限キーは、VMware Customer Connect ポータルに表示されません。新しいキーを生成するには、第 1 世代の Horizon Universal Console にログインしてこのドキュメント ページに記載されている手順を使用するか、第 1 世代コンソールへのログイン アクセス権がない場合は、VMware のサポート リクエストを開き、キーの送信を依頼してください。



システムがすべての要件が満たされていることを確認すると、その行のアイコンを使用して表示およびコピーできるキーが生成されます。

キーを生成したいが、現在 VMware Customer Connect ユーザーではない場合は、ユーザー インターフェイス画面に VMware Customer Connect ユーザーになる方法を学ぶための [Customer Connect ユーザーになる方法について] リンクが表示されます。

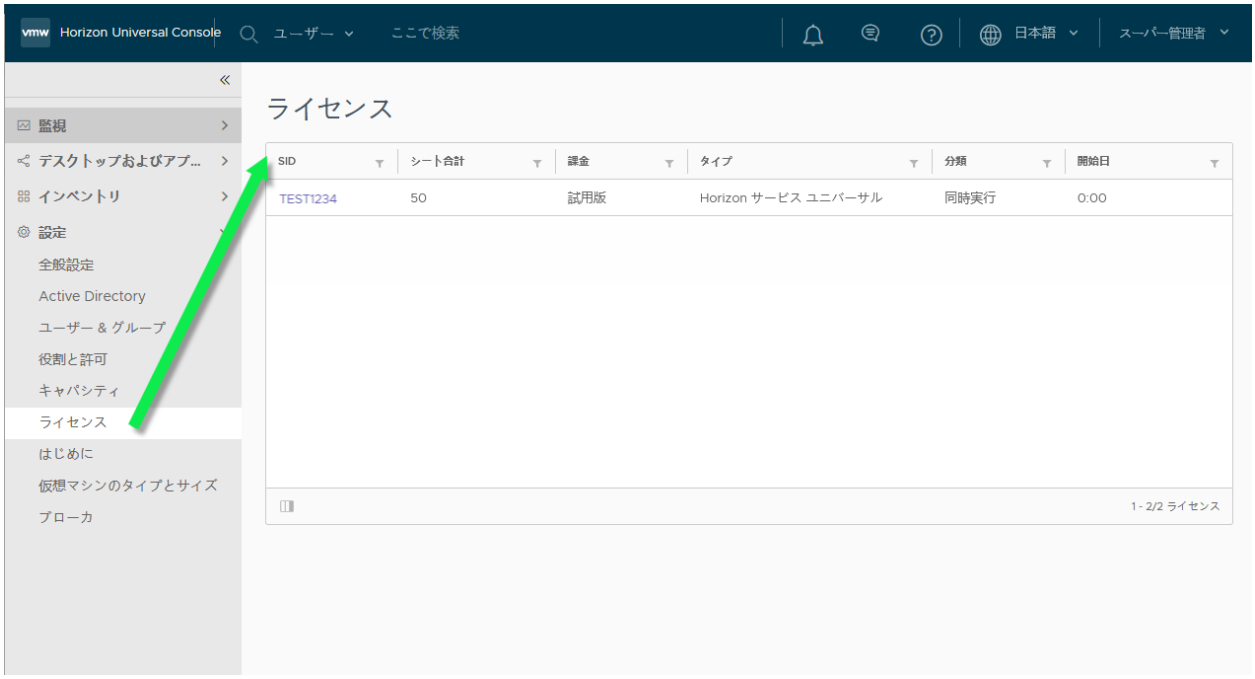
テナントに Active Directory ドメインが最低 1 つ登録されている場合

Horizon Cloud テナントに少なくとも 1 つの Active Directory ドメインが登録されている場合にのみ、[ライセンス] ページという名前のユーザー インターフェイス ページを表示できます。

設計上、左側のナビゲーションにあるコンソールのすべてのページへのアクセスは、[はじめに] ユーザー インターフェイス ページを除いて、最初の登録が完了するまでブロックされます。

[ライセンス] ページは、最初のドメイン登録が完了するまでアクセスがブロックされているユーザー インターフェイス ページの 1 つです。

ただし、テナントに少なくとも 1 つのドメインが登録されている場合は、コンソールの左側のナビゲーション [設定] - [ライセンス] から [ライセンス] ページにアクセスできます。



[ライセンス] ページには、次の条件が満たされている場合にのみ [無期限キーの表示] リンクが表示されます。それ以外の場合、このリンクは存在しません。

- テナントに、vSphere、vSAN、vCenter などの VMware 基本製品を含む、関連付けられた Horizon サブスクリプション ライセンスがあります。
- Horizon Cloud 顧客管理者ロールを使用して コンソールにログインしています。

このリンクが表示された場合は、そのリンクをクリックすると、次の機能を提供するユーザー インターフェイス画面が表示されます。

- このページのキーの表示またはコピーセクションの説明に従った、以前に生成されたプロダクト キーの表示とコピー。
- このページのキーの生成セクションの説明に従った、プロダクト キーの生成。VMware Customer Connect に関連付けられたログインでのみ、[生成] 機能を使用できます。

[ライセンス] ページ

次の表に、[ライセンス] ページに表示される情報の種類を示します。

フィールド	説明
SID	サービス インスタンス ID。この値は、サブスクリプションごとに生成される一意の識別子です。この値は、VMware Customer Connect のログイン ページにある SID の関連付けられたサブスクリプション リスト ページを開くために使用できるハイパーリンクでもあります。このハイパーリンクをクリックすると、ログイン ページが表示されます。
シート合計	ライセンスに含まれているシート数。
課金	課金のタイプとライセンスの合計期間。課金のタイプは以下のとおりです。 ■ 支払い済み - ライセンスの開始時に課金が 1 回発生しました。 ■ 毎月 - ライセンス期間中の各月に課金が 1 回発生します。 ■ 試用版 - 試用版ライセンスであるため、課金は発生しません。
タイプ	特定のライセンスのタイプ。表の行ごとに、この列に表示される名前は、このテナントでの使用にも関連付けられている、Customer Connect アカウントの VMware サブスクリプション ライセンスおよびアドオン ライセンスの 1 つになります。たとえば、Horizon Service Universal、VMware Workspace ONE Assist for VMware Horizon などです。
分類	ライセンスの分類は次のとおりです。 ■ 名前付き - この分類は、このライセンスの合計シート数がエンドユーザー名に基づいて使用量をカバーすることを示します。指定ユーザーの場合、システムは、このテナントを使用して仮想デスクトップとアプリケーションにアクセスした固有エンド ユーザーの数をカウントします。指定ユーザーが複数の単一ユーザー デスクトップ、公開デスクトップ、または公開アプリケーションを実行する場合でも、そのユーザーは単一ユーザーとしてカウントされます。 ■ 同時実行 - この分類は、このライセンスの合計シート数が同時実行に基づいて使用量をカバーすることを示します。同時ユーザーの場合、システムは、セッションあたりの単一ユーザー デスクトップ接続数をカウントします。同時ユーザーが複数の単一ユーザー デスクトップを実行している場合、接続された各デスクトップ セッションは個別にカウントされます。
開始日	ライセンスがアクティブになった日付。

Horizon Universal Console の [ID 管理] ページ

このページは、Microsoft Azure の Horizon Cloud ポッドでシングルポッド仲介を使用するように Horizon Cloud 環境が構成されている場合に表示されます。この構成では、[ID 管理] ページを使用して、この Horizon Cloud テナントと統合されている Workspace ONE Access クラウド テナントに必要な ID 管理プロバイダ情報を追加、編集、および構成します。

第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアーで説明したように、コンソールはテナント環境の現在の構成と状態を動的に反映します。Microsoft Azure のポッドに対してシングルポッドの仲介を使用するようにテナント環境が構成されている場合に、コンソールでは [ID 管理] ページを使用できるようになります。Universal Broker を使用するように環境が構成されている場合、このページは使用できず、代わりに [ブローカ] ページを使用します。環境に対して構成されている仲介タイプを表示するには、コンソールのブローカ ページ（[設定] - [ブローカ]）に移動します。

注： シングルポッド ブローカ Horizon Cloud テナントが v2207 サービス リリースより前に Workspace ONE Access クラウド テナントと統合されていた場合、コンソールの [ID 管理] ページの上部に、関連付けられた Workspace ONE Access クラウド テナントの名前が表示されることがあります。

Workspace ONE Access 構成

このセクションでは、コンソールに、この Horizon Cloud テナント用に現在構成されている ID 管理プロバイダが表示されます。各テナントの次の情報も含まれます。

- ステータス - リストされた構成の現在のステータス。アイコンにカーソルを置くと現在のステータスが表示されます。
- Workspace ONE Access の URL - ID 管理プロバイダのメタデータ URL。
- Workspace ONE のリダイレクト - リストされた構成に対して Workspace ONE Access への自動リダイレクトが構成されているかどうかを示します。リダイレクトはテナントごとに 1 つの ID プロバイダに対してのみ有効にできます。この機能は主に、エンドユーザーが Workspace ONE Access を経由して自分のデスクトップとアプリケーションにアクセスするように強制する機能と一緒に使用されます。Workspace ONE Access を使用するようにエンドユーザーのアクセスを強制するオプションの設定を参照してください。
- SSO トークンのタイムアウト：タイムアウト値（分）。
- データセンター - Microsoft Azure にデプロイされたポッドの場合、表示される値は、この特定のプロバイダで構成されている特定のポッドに対するポッドのソフトウェア バージョンに対応します。この数は、ポッドの詳細ページに一覧表示されているポッドのバージョン番号と同じです。3 章 第 1 世代テナント - 第 1 世代 Horizon Cloud がサポートするすべてのポッド タイプのクラウド接続ポッドの管理で、ポッドの詳細ページについての説明を参照してください。
- クライアント アクセスの FQDN - Horizon Cloud に接続するためにエンドユーザーが接続先に指定する FQDN。
- 場所 - ポッドの場所。
- ポッド - この構成が適用されるポッド。

新しい構成の追加

シングルポッド ブローカを使用している Horizon Cloud ポッドで使用するように Workspace ONE Access クラウド テナントを構成する場合は、複数の手順を実行します。

- シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure の環境の Horizon Cloud ポッドと Workspace ONE Access の統合をお読みください。
- シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure で関連する Workspace ONE Access テナント情報を使用して Horizon Cloud ポッドを構成する手順の手順に従います。

構成の設定の編集

このページで構成の情報を編集するには、次の手順を実行します。

1 一覧表示されている構成を選択します。

2 [編集] をクリックします。

3 次の情報を編集します。

フィールド	説明
SSO トークンのタイムアウト	タイムアウト値（分）。
クライアント アクセスの FQDN	Microsoft Azure のポッドの場合、Horizon Cloud に接続するためにエンドユーザーが接続先に指定する FQDN を入力します。
Workspace ONE のリダイレクト	構成を編集するときに現在の設定を変更できます。 また、エンドユーザーが Workspace ONE Access を経由してアクセスするように設定している場合、これを [はい] に設定してエンドユーザーのクライアントを自動的にその Workspace ONE Access 環境にリダイレクトすることができます。エンドユーザーが Workspace ONE Access 経由でアクセスするように強制するオプションについては、Workspace ONE Access を使用するようにエンドユーザーのアクセスを強制するオプションの設定を参照してください。自動リダイレクトを [はい] に設定した場合、エンドユーザー クライアントでクライアントが Horizon Cloud に接続しようとしたときに Workspace ONE Access を介してアクセスするように強制されていると、クライアントは、この ID 管理プロバイダ構成で指定された Workspace ONE Access 環境に自動的にリダイレクトされます。[いいえ] に設定すると、自動リダイレクトは有効にならず、クライアントは代わりに情報メッセージをユーザーに表示します。 **注：** このリダイレクトは、ポッドごとに 1 つの ID 管理 URL に対してのみ有効にできます。同じポッドの複数の URL に対してこの機能を有効にしようとすると、エラー メッセージが表示されます。

4 [保存] をクリックします。

Workspace ONE Access を使用するようにエンドユーザーのアクセスを強制するオプションの設定

リストされたプロバイダごとに、以下の手順を使用して、エンドユーザーが割り当てられたデスクトップおよびリモート アプリケーションに直接 Horizon Cloud からアクセスできるようにするか、アクセスする場合には必ず Workspace ONE Access を使用するようにするかを設定できます。

注： この設定を変更する場合、更新内容が有効になるまでに最大 5 分かかる場合があります。

1 [構成] をクリックします。

2 以下のように設定を編集します。

フィールド	説明
[リモート ユーザーを Workspace ONE Access に強制的に登録]	ID 管理プロバイダ以外によるリモート ユーザー アクセスをブロックするには、[はい] を選択します。そのプロバイダのステータスが緑色の場合にのみ表示されるオプションです。
[内部ユーザーを Workspace ONE Access に強制的に登録]	ID 管理プロバイダ以外による内部ユーザー アクセスをブロックするには、[はい] を選択します。そのプロバイダのステータスが緑色の場合にのみ表示されるオプションです。

3 [保存] をクリックします。

Workspace ONE Access を介したエンドユーザー アクセスを強制する場合、通常は、対応する ID プロバイダ構成を編集して、エンドユーザー クライアントが自動的に Workspace ONE Access にリダイレクトするように指定することもできます。構成の設定の編集を参照してください。

Workspace ONE Access へのエンドユーザー アクセスを強制する機能は、次のように Workspace ONE Access リダイレクト機能と連携して動作します。

Workspace ONE Access 設定を介したエンドユーザー アクセスの強制	Workspace ONE Access リダイレクトの設定	エンドユーザーのクライアントが Horizon Cloud に接続して自分のデスクトップとアプリケーションにアクセスした場合の動作
有効（はい）	有効（はい）	クライアントは Workspace ONE Access に自動的にリダイレクトされる。
有効（はい）	無効（いいえ）	クライアントは Workspace ONE Access を介して Horizon Cloud にアクセスしなければならないことをユーザーに通知するメッセージを表示する。自動リダイレクトは発生しない。
無効（いいえ）	有効（はい）	クライアントはエンドユーザーがログインするための Horizon Cloud ログイン画面を表示する。Workspace ONE Access への強制アクセスが有効になっていないため、自動リダイレクトは発生しない。
無効（いいえ）	無効（いいえ）	クライアントはエンドユーザーがログインするための Horizon Cloud ログイン画面を表示する。このシナリオでは、強制アクセスと自動リダイレクト機能の両方が無効になっている。

構成の削除

構成の 1 つを削除するには：

1 リストで構成を選択します。

2 [削除] をクリックします。

3 [削除] をクリックして確認します。

Horizon Cloud テナント環境のブローカ関連の設定

Horizon Universal Console の [ブローカ] ページを使用して、Horizon Cloud テナント環境全体に適用されるブローカ関連の設定を変更します。

第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアーで説明されているように、コンソールはテナント環境の現在の状態を動的に反映します。その結果、コンソールには、このページのセクションと、テナント環境の現在の最新の状態に関連した適切なものに基づいて、さまざまな設定が表示されます。

注： 以下のセクションで説明する次の設定のいずれかを変更すると、更新が有効になるまで最大 5 分かかる場合があります。

- [セッション タイムアウト] セクションの設定。
- [タブを閉じるときに HTML Access 認証情報をクリーンアップ]する設定。

Universal Broker

クラウドに接続されたポッドが Universal Broker を使用してエンド ユーザーのクライアントをそのポッド プロビジョニング リソースに仲介するようにテナントが構成されている場合、コンソールにこのセクションが表示されます。Universal Broker の設定がすでにシステムに保存されている場合は、このセクションに現在の設定が表示されます。これらの設定を変更するには、[Universal Broker] ラベルの横にある鉛筆アイコンをクリックし、画面の指示に従います。画面上の設定の詳細については、Universal Broker の設定 に記載されている情報を参照してください。

テナントの最新の構成によっては、[ブローカ] ページに次のような追加のタブが表示される場合があります。

- クライアントの受信トラフィックが内部ネットワークから送信されるタイミングを区別するための、Universal Broker への IP アドレス範囲を識別する設定。内部ネットワーク範囲の定義を参照してください。
- エンドユーザー セッションのクライアント制限設定。グローバル クライアントの制限の構成を参照してください。
- Workspace ONE Access および Intelligent Hub サービスとの統合。テナントを Workspace ONE Access および Intelligent Hub サービスと統合するを参照してください。

シングルポッド ブローカ

このセクションは、テナントが Microsoft Azure の Horizon Cloud ポッドでサービスの従来のポッドベースの仲介方法を使用して、エンド ユーザーのクライアントをそのポッド プロビジョニングされたリソースに仲介するように構成されている場合に表示されます。これらのポッドは、Horizon Cloud ポッド マネージャ テクノロジーを実行しているポッドです。

v2111 サービス リリースの時点では、グリーンフィールドのお客様テナント環境ではシングルポッド仲介を使用できません。このコンテキストでは、グリーンフィールドとは、テナントの Horizon Cloud ポッドに対してコンソールの [ブローカ] ページ内でコンソールの有効化手順が一度も開始されたことのないテナント環境を意味します。

セッション タイムアウト

これらの設定は、エンド ユーザーが Horizon Client、Horizon HTML Access、および Workspace ONE を使用してエンドポイント デバイスから行った接続を制御します。これらのタイムアウト設定を調整することで、ユーザーが Horizon Cloud に対する再認証が必要となる予期しない状況を回避するための十分な時間を割り当てることができます。これらの設定は、資格のあるエンド ユーザーのエンドポイント デバイスで実行されているクライアントと、その資格のあるエンド ユーザーに VDI デスクトップ、RDS セッション デスクトップ、およびリモート アプリケーションをプロビジョニングするポッドとの間の接続に関連付けられています。これらの設定は、それらのデスクトップおよびアプリケーションの基盤となる Windows オペレーティング システムへのユーザーのログインセッションとは異なります。ポッドがこれらの設定によって判定される条件が発生したことを検出すると、ユーザーの認証済み Horizon Client、Horizon HTML Access、または Workspace ONE 接続が期限切れになります。

タイムアウト	説明
Client ハートビートの間隔	Horizon Client ハートビートの間隔と、ポッド内のポッド マネージャへのエンドポイントの接続状態を制御します。これらのハートビートは、ポッド マネージャに対して、エンドポイントへの接続で経過したアイドル時間の合計をレポートします。アイドル時間は、ユーザーのデスクトップまたはリモート アプリケーションの使用の基盤となる Windows オペレーティング システム セッションのアイドル時間とは反対に、エンドポイント デバイスとの対話式処理がないときに発生します。大規模なデスクトップのデプロイ環境では、アクティビティ ハートビートの間隔を長く設定すると、ネットワーク トラフィックを低減し、パフォーマンスを向上できる場合があります。
Client アイドル ユーザー	エンド ユーザーのエンドポイント デバイスとポッドのポッド マネージャ間の接続に関連して、クライアント デバイスでキーボードまたはマウスのアクティビティが検出されない場合のような、エンド ユーザーがその接続でアイドル状態を維持できる最大時間。この最大時間に達すると、ポッド マネージャに対する接続の認証が期限切れになり、アクティブな Horizon Client、Horizon HTML Access、および Workspace ONE リモート（RDS ベース）アプリケーションの接続がすべて閉じられます。 ■ ポッド マネージャのシングル サインオン (SSO) 認証情報は破棄されます。ユーザーは、クライアントの再認証を行って、エンドポイント デバイスから接続を再度開き、そのポッド内のポッド マネージャに接続する必要があります。 ■ RDS ベースのアプリケーション セッションは切断されています。 **注：** エンド ユーザーが予期せずに切断されないように、少なくとも [Client ハートビートの間隔] 設定の 2 倍の値になるように [Client アイドル ユーザー] のタイムアウトを設定します。
Client ブローカ セッション	エンド ユーザーのエンドポイント デバイスとポッドのポッド マネージャ間の接続に関連して、接続の認証が期限切れになる前に、Horizon Client、Horizon HTML Access、または Workspace ONE 接続をポッド マネージャに接続できる最大時間。タイムアウトのカウントは、ユーザーがエンドポイント デバイスのクライアント内のポッドに対して認証を行うごとに開始されます。このタイムアウトが発生すると、ユーザーは現在ポッド マネージャから割り当てられている既存のセッションで作業を続行できます。ユーザーがエンドポイント デバイス上のクライアントで、クライアント設定の変更など、ポッド マネージャとの通信を必要とするアクションを実行する場合、ポッド マネージャは再認証された接続を必要とします。エンド ユーザーは、エンドポイント デバイス（Horizon Client、Horizon HTML Access、または Workspace ONE）でクライアントに再度ログインする必要があります。 **注：** [Client ブローカ セッション] のタイムアウトは、少なくとも [Client ハートビートの間隔] 設定と [Client アイドル ユーザー] のタイムアウトの合計値以上にする必要があります。

HTML Access

[タブを閉じたときに HTML Access 認証情報をクリーンアップ] 設定は、エンド ユーザーが HTML Access を使用してデスクトップまたはアプリケーションにアクセスするときにシステムのセキュリティと使いやすさに影響します。この設定は、エンド ユーザーが認証情報を再入力する必要があるかどうかを決定します。

- [はい] の値はセキュリティを優先するオプションであり、再接続時に認証情報を再入力するようにエンド ユーザーに要求します。
- [いいえ] の値は使いやすさを優先するオプションであり、再接続時に認証情報を再入力するようにエンド ユーザーに要求しません。

プール/ファーム オプション

[クライアントが電源オフの仮想マシンを待機することを許可する] オプションは、クラウド内で基盤となる VDI または RDSH 仮想マシンがパワーオフされた状態で、エンド ユーザーが Horizon Client を使用してデスクトップまたはリモート アプリケーションに接続しようとした場合の結果を制御します。割り当てまたは RDSH ファームの電源管理設定の結果、クライアントの要求を処理するためのパワーオンされた仮想マシンのキャパシティが不足している可能性があります。接続が開始すると、Horizon Cloud は要求を処理するのに必要な基盤となる仮想マシンのパワーオンを開始します。ただし、基盤となる仮想マシンがパワーオンしていても、仮想マ

シンの Horizon Cloud エージェントはまだ起動しておらず、Horizon Client の接続要求に応答できません。クライアントが接続してからエージェントが起動するまでには時間がかかることがあるため、このオプションを使用して、クライアントが接続を再試行するようにし、エンド ユーザーに予想される時間を通知することができます。このシナリオでは、[クライアントによる再試行を有効にする] トグルが [はい] に設定されていると、クライアントは予想される待ち時間についてのメッセージをエンド ユーザーに通知します。

1 Horizon Cloud は、エンド ユーザーのクライアント要求に対応するため、クラウド内の基盤となる仮想マシンのパワーオンを開始します。

2 Horizon Cloud は、仮想マシンのエージェントが起動して実行状態になると Horizon Client に接続を再試行するよう通知します。

3 クライアントは、クライアントが接続を再試行するまでの予想される待機時間についてのメッセージをユーザーに表示します。

Horizon Cloud の [はじめに] ウィザード - 概要

[はじめに] ウィザードを使用して、環境を完全に管理および使用するために、Active Directory ドメインの登録などの必要な構成手順を実行します。[はじめに] ウィザードは、デフォルトでは Horizon Universal Console に初めてログインするときに表示されます。1 つの Active Directory ドメインを登録し、そのドメイン内の Active Directory グループに Horizon Cloud のスーパー管理者ロールを付与した後は、コンソールの左側のナビゲーション バーにアクセスして、環境で管理タスクを実行できます。また、その時点では、[はじめに] ページの下部にあるトグルを切り替えて、[はじめに] をデフォルトのコンソール ホーム ページとして使用するのをやめ、代わりに [ダッシュボード] ページをデフォルトのホーム ページとして使用できます。

注： ここで使用される用語：

- Horizon Cloud ポッドは、VMware Horizon Cloud on Microsoft Azure のポッド マネージャ テクノロジーに基づいて構築されました。
- Horizon ポッドは、VMware Horizon の Connection Server テクノロジーに基づいて構築されました。

[はじめに] ウィザードには、これまでユーザーが完了した作業の概要と、今後実行する必要がある作業が表示されます。ウィザードには、[設定] - [はじめに] からアクセスできます。

注： 環境の実行と管理に必要なすべてのタスクが完了したことを確認するには、最初に環境にデプロイしたポッドのタイプに応じて、下記のトピックの手順を確認します。証明書のアップロードなど、[はじめに] ウィザードではいくつかのタスクを実行できません。

- Horizon Cloud on Microsoft Azure デプロイの場合：最初のクラウドに接続されたポッドがポッド デプロイヤを使用してポッドを Microsoft Azure にデプロイする場合のワークフローの概要
- Horizon ポッドおよび Horizon Cloud Connector のデプロイの場合：Horizon Cloud テナント環境への最初のポッドとして、VMware SDDC に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

表 1-12. [はじめに] ウィザードの選択項目

セクション	説明
キャパシティ	**ヒント:** ライセンスとロールの要件を満たしている場合は、[無期限キーの表示] リンクを使用できます。[無期限キーの表示] リンクをクリックして [無期限キー] ページにアクセスし、基盤となる VMware 製品の無期限キーを表示および生成できます。最初のポッドがオンボーディングされ、ドメイン登録が完了すると、ライセンスとロールの要件を満たしている場合は、[ライセンス] ページと [はじめに] ページの両方でリンクが使用可能になります。第 1 世代のテナント - Horizon Universal Console を使用したライセンス情報の取得を参照してください。 テナントのポッド フリートにポッドがない（ゼロ）場合は、このセクションから開始してください。次のことが可能です。 ■ [管理] - [ポッドの追加] を使用して、Horizon Cloud on Microsoft Azure デプロイで使用される自動ポッド デプロイ ウィザードを起動します。 ■ Horizon Cloud Connector、および Horizon Cloud Connector アプライアンスをダウンロードするためのリンクを使用して Horizon ポッドのデプロイを接続する方法については、[追加] ボタンを使用します。 **注：** ■ [管理] メニューからのウィザードは、Microsoft Azure VMware Solution を含むデプロイに使用できません。そのようなポッドは VMware SDDC カテゴリの下にあります。このカテゴリでは、[追加] ボタンおよび Horizon Cloud Connector のダウンロードのルートを使用します。 ■ [追加] をクリックすると、VMware Cloud on AWS で Horizon ポッドを追加する 2 つの方法を示すウィンドウが表示されます。ただし、現在のリリースで完全にサポートされているのは、[ダウンロード] の方法のみです。 テナントのポッド フリートに少なくとも 1 つのポッドがある状態になると、このセクションでは次が提示されます。 ■ 環境内のポッドのフリートの概要。 ■ サブスクリプション情報を編集、追加、および削除したり、Microsoft Azure 上のポッド マネージャ ベースの Horizon ポッドを削除したりするために使用される [管理] メニュー。
[全般的なセットアップ]	Active Directory ドメインの登録など、さまざまなテナント全体の設定の最初の構成についての詳細とリンクを提供します。Horizon Universal Console の [はじめに] ウィザードの [全般的なセットアップ] セクションを参照してください。
[デスクトップ割り当て]	■ ポッド フリートに少なくとも 1 つの Horizon Cloud ポッドがある場合、このセクションでは Horizon Cloud 環境にインポートされた仮想マシン (VM) の操作、およびゴールド イメージの公開に関するタスク ページへのリンクを提供します。これらのイメージは、ファームおよび VDI デスクトップ割り当てで使用されます。Microsoft Azure でのデスクトップ イメージと Horizon Cloud ポッドの作成 とそのサブトピックを参照してください。 ■ ポッド フリートに少なくとも 1 つの Horizon ポッドのデプロイがある場合、このセクションでは、デスクトップ割り当ての構成に関連するタスク ページへのリンクを提供します。デスクトップ割り当てを使用すると、クラウド接続された複数のポッドのデスクトップ プールをエンド ユーザーが利用できます。Universal Broker 環境での割り当ての作成および管理とそのサブトピック、および Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成を参照してください。
アプリケーション割り当て	**注：** このリリースでは、ポッド フリートが Horizon ポッドのみで構成されている場合、このセクションは表示されません。 ポッド フリートに少なくとも 1 つの Horizon Cloud ポッドがある場合、このセクションでは、アプリケーションおよびアプリケーション割り当てに関連するタスク ページへのリンクを提供します。Horizon Cloud インベントリ内のアプリケーション とそのサブトピックを参照してください。

1 つ以上の Active Directory ドメインの登録および 1 つ以上の Active Directory ユーザー グループへのスーパー管理者ロールの付与の必要な手順を完了した場合、ウィザードの表示はオプションです。コンソールにログインするたびにウィザードが表示されるように切り替えるには、ウィザードのメイン ページの下部にあるスライダを [はい] に移動します。

注： ウィザードが主に使用されるのは初めてポッドを設定するときであり、通常、ほとんどのユーザーはその後でウィザードをオフに切り替えます。しかし、いくつかの標準タスクを実行するときにはウィザードを開始ポイントとして使用すると便利な場合があります。

Horizon Universal Console の [はじめに] ウィザードの [全般的なセットアップ] セクション

Horizon Cloud 環境に接続されたポッドの最初の設定では、Active Directory ドメインの登録など、各種のポッド全体に関する初期設定を [全般的なセットアップ] セクションの選択項目を使用して行います。最初の設定が終了したら、[全般的なセットアップ] セクションの選択項目を使用してコンソール ページを開き、設定を編集することができます。

選択	説明
[My VMware アカウント]	他のユーザーが自分の My VMware アカウントを使用してコンソールと Horizon Cloud 環境にログインするための権限を付与します。Horizon Cloud テナント環境にログインし、Horizon Universal Console を使用してアクションを実行するための管理者ロールを組織内の個人に付与するを参照してください。
[Active Directory]	初期の Active Directory ドメインを登録し、ドメイン バインドやドメイン参加情報を追加します。役割と許可をコンソール ユーザーに付与する、またはサービスをユーザーに割り当てるため、少なくとも 1 つの Active Directory ドメインのドメイン登録が必要です。追加の Active Directory ドメインの登録を含め、最初のクラウド接続されたポッドでその他の操作を実行するには、Active Directory ドメインを登録し、ドメイン参加を完了する必要があります。Active Directory およびポッドに関連するタスクについては、以下を参照してください。 ■ 第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行 ■ 追加の Active Directory ドメインをクラウド構成の Active Directory ドメインとして Horizon Cloud テナント環境に登録する ■ Horizon Cloud のクラウド構成の Active Directory ドメイン用に補助バインド アカウントを追加する
[役割と許可]	環境を管理するユーザーに役割を割り当てます。役割は、関連付けられている許可をその役割が付与されたユーザーに付与します。Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるを参照してください。

選択	説明
[ブローカ]	エンドユーザーのクライアントが、使用資格が付与されているポッド プロビジョニングされたリソースに接続するときに使用する仲介テクノロジーを有効にします。セッション タイム アウト設定など、仲介されたエンドユーザー セッションに関連する設定を構成します。
[Cloud Monitoring Service]	Horizon Cloud Cloud Monitoring Service は、監視とレポートの目的で、接続されたポッドからセッション、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。 ■ Horizon Cloud Cloud Monitoring Service を有効または無効にするには、[Cloud Monitoring Service] トグルを使用します。これはデフォルトでは有効になっています。 この設定がオフに切り替わると、以下の [セッション データ] 設定が表示されなくなります。 ■ Cloud Monitoring Service が有効になっている場合は、[セッション データ] トグルを使用して、エンド ユーザーのセッションに関連するユーザー情報の追跡をオプトインまたはオプトアウトすることができます。収集された情報には、ユーザーごとのログイン時刻、セッションの接続時間、および平均のセッションの長さが含まれます。 ユーザー データの収集をオプトインすると、Horizon Cloud はこの情報を収集し、Horizon Cloud を使用している間維持します。「VMware ナレッジベースの記事 KB91183」で説明されているように、このデータは Workspace ONE Intelligence で入手できます。[セッション データ] トグルをオフにすると、収集したデータを削除できます。[セッション データ] トグルをオフにすると、収集したデータを削除できます。 ユーザー データの収集をオプトアウトし、監視サービスを有効にすると、サービスは一定期間セッション データを収集し、ユーザー名をハッシュしてリアルタイム管理を可能にします。その結果、Horizon ユーザー使用量レポートなどの一部のレポートは使用できません。この場合、システムは、接続されたポッド内のアプリケーションおよびデスクトップに関連する他のデータの収集も継続します。 Horizon Cloud Cloud Monitoring Service によって収集される情報は、Horizon Universal Console および Workspace ONE Intelligence コンソールのさまざまな場所で使用されます。詳細については、「第 1 世代のテナント - 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」および「第 1 世代テナント - 第 1 世代 Horizon Universal Console の [レポート] ページ」を参照してください。

Horizon Universal Console でのフィルタ フィールドの使用

Horizon Cloud 管理コンソールの各ページには、各種レポートや [アクティビティ] ページなどのページに表示される大量の情報をフィルタリングする方法が用意されています。一部のページでは、フィルタ フィールドはページの上部に表示されます。その他のページでは、各列の列見出しにフィルタ アイコンがあります。このアイコンをクリックすると、フィルタ テキスト ボックスにアクセスできます。フィルタ機能を提供するページでは、フィルタ テキスト ボックスに文字を入力すると、そのパターンに一致する文字を含む表示されたレコードのサブセットのみが表示されます。

次のスクリーンショットは、一部のページにあるフィルタ ボックスの例と、一部のページの列に対するフィルタ アイコンの例を示しています。この最初の例は [イメージ] ページにあります。

この 2 番目の例は、[アクティビティ] ページにあります。

注： ページの上部にあるフィルタ テキスト ボックスでは、フィルタ テキスト ボックスに 3 文字を入力すると、システムがパターンとの照合を開始し、ページに表示されるレコードをフィルタリングします。列見出しの上部にあるフィルタ アイコンでは、1 文字を入力すると、システムがフィルタリングを開始します。

[レポート] ページでの画面上のフィルタ機能

[レポート] ページのタブでは、フィルタ テキスト ボックスはユーザー インターフェイス自身に表示される項目の数に対して機能し、その項目のシステム レコードの合計セットに対しては機能しません。これらのページでは、最大 500 の項目の表示をサポートします。したがって、項目に対して 500 を超えるレコードがシステムに含まれている場合、ユーザー インターフェイスのページには 500 の項目までしか表示されません。フィルタ テキスト ボックスを使用すると、表示されている 500 のレコードのみがフィルタされます。フィルタは、セット全体には適用されません。以下に例を示します。

- VDI フローティング デスクトップ割り当てに 2000 人のユーザーが割り当てられているとします。
- ユーザー名は vdiuser-1 から始まり、vdiuser-500、vdiuser-501、vdiuser-502 のようになり、最後が vdiuser-2000 です。
- 1 日の間に、2000 人のすべてのユーザーがログインし、その割り当てからデスクトップを使用します。
- [監視] - [レポート] - [デスクトップ マッピング] に移動すると、レポートの項目数が 500 を超えているというメッセージが表示されます。
- フィルタに vdiuser-54 と入力してユーザー vdiuser-54、vdiuser-540、さらに vdiuser-541 から vdiuser-549 までのレコードを表示する場合、11 行が表示されると予測されます。

しかし実際には、2000 すべてのセットからフィルタされた 11 行が表示されるのではなく、[デスクトップ マッピング] ページにはフィルタ パターンに一致する最初に表示された 500 行のサブセットのみが表示されます。完全なデータ セットを表示するには、エクスポート機能（ ）を使用します。

追加の Active Directory ドメインをクラウド構成の Active Directory ドメインとして Horizon Cloud テナント環境に登録する

オプションとして、Horizon Cloud 顧客アカウントに追加の Active Directory ドメインを登録することができます。Active Directory ドメインを登録すると、そのドメインが Horizon Cloud 顧客アカウントに関連付けられた一連のクラウド構成のドメインに追加されます。ドメインがクラウド構成のドメインのセットにある場合、そのドメ

インのユーザー アカウントとグループがシステム提供の機能を使用できるようにすることができます。たとえば、ヘルプ デスク管理者のためのヘルプ デスク機能や、エンド ユーザーのためのデスクトップ関連機能などです。

重要： ドメイン バインドやドメイン参加アカウントに関連する [バインド ユーザー名] および [参加ユーザー名] のテキスト ボックスに、アカウント名を指定します。これは、`ouraccountname` など、ドメイン名なしのユーザー ログイン名のようになります。

注： 配布グループは、セキュリティ グループにネストされていてもサポートされません。Active Directory グループを作成するときは、常に [グループ タイプ] に [セキュリティ] を選択します。

テナントで、Horizon Cloud on Microsoft Azure - LDAPS (LDAP Over SSL) 用に構成された Active Directory 環境の使用で説明されている機能を使用できるようになっている場合、手順 3 のコンソールの画面は、ここで説明する画面とは異なります。テナントでその機能を使用できる場合は、代わりにそのページに従ってください。

前提条件

ドメイン参加アカウントの手順が失敗しないようにするには、Active Directory インフラストラクチャが正確な時間のソースと同期していることを確認します。このような障害が発生した場合は、Horizon Cloud サポートにお問い合わせください。[ドメイン バインド] 手順は成功したが、ドメイン参加の手順に失敗した場合、ドメインをリセットし、時間のソースを調整する必要があるかどうかを確認してみてください。ドメインをリセットするには、Active Directory ドメイン登録の削除の手順を参照してください。

必要なプライマリおよび補助ドメイン バインド アカウントの場合、Horizon Cloud の運用に必要なサービス アカウントに記載されている要件を満たす 2 つの Active Directory ユーザー アカウントの情報があることを確認します。

注意： 偶発的なロックアウトによって、Horizon Cloud 環境を管理するためにクラウドベースのコンソールにログインできなくなるのを防ぐには、ドメイン バインド アカウントの期限切れ、変更、ロックアウトが発生しないようにする必要があります。このタイプのアカウント設定を使用する必要があります。これは、システムでは Active Directory ドメインを問い合わせてコンソールへのログインに使用する認証情報を検証するために、プライマリ ドメイン バインド アカウントがサービス アカウントとして使用されるためです。何らかの理由でプライマリ ドメイン バインド アカウントにアクセスできない場合、システムは補助ドメイン バインド アカウントを使用します。プライマリ/補助の両方のドメイン バインド アカウントが期限切れかアクセス不能になると、コンソールにログインし、構成を更新してアクセス可能なドメイン バインド アカウントを使用することができません。

プライマリ ドメイン バインド アカウントおよび補助ドメイン バインド アカウントには、常にスーパー管理者ロールが割り当てられます。これにより、コンソールで管理アクションを実行するためのすべての権限が付与されます。スーパー管理者権限を必要としないユーザーは、管理者が指定したドメイン バインド アカウントにアクセスできないようにする必要があります。

ドメイン参加アカウントについては、アカウントが、Horizon Cloud の運用に必要なサービス アカウントに記載されている要件を満たしていることを確認します。

注意：

- スーパー管理者ロールが割り当てられた Active Directory グループが 1 つしかない場合は、そのグループを Active Directory サーバから削除しないでください。これを行うと、以降のログインで問題が発生する可能性があります。
- 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 ポッドがある場合は、ドメイン参加アカウントにスーパー管理者ロールを付与する必要があります。2298 より前のマニフェストはサポート対象外であり、ナレッジベースの記事 KB86476 の記載に従って更新する必要があります。

Active Directory ドメインの NetBIOS 名と DNS ドメイン名があることを確認します。これらの値は、このワークフローの最初のステップでコンソールの [Active Directory の登録] ウィンドウに入力します。これらの値を特定する方法の例については、Horizon Cloud の [Active Directory の登録] ワークフローの NETBIOS 名および DNS ドメイン名のフィールドに必要な情報の特定を参照してください。

注意： 追加の Active Directory ドメインを登録するときは、クラウド接続されたすべてのポッドがそのドメインとの通信路を確立した状態であることを確認します。同じ顧客アカウント レコードのすべてのポッドは、そのアカウントに登録された同じクラウド構成の Active Directory ドメインのセットに到達できる必要があります。すべてのポッドは、同じ Active Directory サーバに到達できる必要があります。また、DNS 構成でこれらのすべてのクラウド構成の Active Directory ドメインを解決する必要があります。

手順

1 コンソールで、[設定] - [Active Directory] の順に選択します。

2 [登録] をクリックします。

3 [Active Directory の登録] ダイアログ ボックスで、必要な登録情報を指定します。

重要： 前提条件で説明されているとおりに、プライマリおよび補助ドメイン バインド アカウントのガイドラインに準拠する Active Directory アカウントを使用します。

オプション	説明
NETBIOS 名	■ クラウド接続された Horizon ポッドがある場合、このステップでは Horizon ポッドが認識できるすべての Active Directory ドメインの名前が入力された選択メニューが表示されます。最初に登録する Active Directory ドメインを選択します。 ■ クラウド接続されたポッドのみが Microsoft Azure にある場合、このステップではテキスト ボックスが表示されます。登録する Active Directory ドメインの NetBIOS 名を入力します。通常、この名前にはピリオドは含まれません。Active Directory ドメイン環境から使用する値を見つける方法の例については、Horizon Cloud の Active Directory の登録ワークフローの NETBIOS 名と DNS ドメイン名のフィールドに必要な情報の検索を参照してください。
DNS ドメイン名	■ クラウド接続された Horizon ポッドがある場合、[NETBIOS 名] に選択した Active Directory ドメインの完全修飾ドメイン名が自動的に表示されます。 ■ クラウド接続されたポッドのみが Microsoft Azure にある場合、テキスト ボックスが表示されます。[NETBIOS 名] に指定した Active Directory ドメインの完全修飾 DNS ドメイン名を入力します。Active Directory ドメイン環境から使用する値を見つける方法の例については、Horizon Cloud の Active Directory の登録ワークフローの NETBIOS 名と DNS ドメイン名のフィールドに必要な情報の検索を参照してください。
プロトコル	サポートされているプロトコルとして、LDAP が自動的に表示されます。
[バインド ユーザー名]	プライマリ LDAP バインド アカウントとして使用するドメインのユーザー アカウント。 **注：** ユーザー名のみを指定します。ここにドメイン名を含めないでください。
バインド パスワード	[バインド ユーザー名] テキスト ボックスの名前と関連付けられているパスワード。
補助アカウント #1	[バインド ユーザー名] と [バインド パスワード] フィールドに、補助 LDAP バインド アカウントとして使用するドメイン内のユーザー アカウントとそれに関連するパスワードを入力します。 **注：** ユーザー名のみを指定します。ここにドメイン名を含めないでください。

4 [ドメイン バインド] をクリックします。

ドメイン バインドの手順が成功すると、[ドメイン参加] ダイアログ ボックスが表示され、次の手順を続行できます。

5 [ドメイン参加] ダイアログ ボックスで、必須の情報を入力します。

注： 前提条件に説明されているドメイン参加アカウントのガイドラインに準拠した Active Directory アカウントを使用します。

オプション	説明
プライマリ DNS サーバ IP アドレス	Horizon Cloud でマシン名の解決に使用するプライマリ DNS サーバの IP アドレス。 Microsoft Azure のポッドの場合、この DNS サーバは、Microsoft Azure クラウド内のマシン名、および外部名を解決できる必要があります。
セカンダリ DNS サーバ IP アドレス	（オプション）セカンダリ DNS サーバの IP アドレス
デフォルト OU	インポートされた仮想マシン、ファーム RDSH 仮想マシン、VDI デスクトップ インスタンスなど、ポッドのデスクトップ関連の仮想マシンで使用する Active Directory 組織単位 (OU)。Active Directory OU の形式は、`OU=NestedOrgName,OU=RootOrgName,DC=DomainComponent` のようになります。システム デフォルトは `CN=Computers` です。`CN=myexample` など、必要に応じてデフォルトを変更できます。 **注：** ネストされた組織の名前の説明については、ネストされた Active Directory ドメイン組織単位の使用についての考慮事項を参照してください。入力した個々の OU は、`OU=` の入力部分を除いて 64 文字以内の長さでなければなりません。Microsoft は、個々の OU を 64 文字以内に制限します。64 文字を超える OU パスは、個々の OU が 64 文字を超えていなければ、有効です。ただし、個々の OU はそれぞれ 64 文字以内である必要があります。
参加ユーザー名	その Active Directory ドメインにコンピュータを参加させる権限を持つ Active Directory のユーザー アカウント。 **注：** ユーザー名のみを指定します。ここにドメイン名を含めないでください。
参加パスワード	[参加ユーザー名] テキスト ボックスの名前と関連付けられているパスワード。

6 （オプション） 補助ドメイン参加アカウントを指定します。

指定したプライマリ ドメイン参加アカウントにアクセスできない場合、システムは、Microsoft Azure のポッドで、イメージ仮想マシンのインポート、ファーム RDSH インスタンスの作成、VDI デスクトップ インスタンスの作成など、ドメインに参加する必要がある操作に対して補助ドメイン参加アカウントを使用します。

注：

- 前提条件に説明されているプライマリ ドメイン参加アカウントの同じガイドラインに準拠した Active Directory アカウントを使用します。両方のアカウントに [Never Expires（有効期限なし）] が設定されている場合を除き、この補助ドメイン参加アカウントの有効期限はプライマリ ドメイン参加アカウントとは異なることを確認します。プライマリおよび補助ドメイン参加アカウントの両方の有効期限が同時に切れる場合、ファーム RDSH 仮想マシンと VDI デスクトップ仮想マシンのプロビジョニングやイメージのシーリングにおけるシステム動作が失敗します。
- Horizon Cloud で登録する各 Active Directory に対して 1 つの補助ドメイン参加アカウントのみを追加できます。
- この時点で補助ドメイン参加アカウントを追加しない場合、後でコンソールを使用して追加することができます。
- このアカウントは、後で更新したり削除したりすることができます。
- システムが仮想マシンで補助ドメイン参加アカウントを使用するには、デスクトップ関連仮想マシン（シールド イメージ、ファーム RDSH インスタンス、または VDI デスクトップ インスタンスなど）のエージェント関連ソフトウェアがバージョン 18.1 以降である必要があります。

オプション	説明
補助参加ユーザー名	その Active Directory ドメインにシステムを参加させる権限を持つ Active Directory のユーザー アカウント。 **重要：** このフィールドには、アカウント名のみを指定します。つまり、`ouraccountname` など、ドメイン名なしのユーザー ログイン名のようになります。スラッシュまたは @ 記号を入力するとエラーが表示されます。
補助参加パスワード	[補助参加ユーザー名] テキスト ボックスの名前と関連付けられているパスワード。

7 [保存] をクリックします。

この時点で、ドメイン参加の手順が完了すると、[管理者の追加] ダイアログ ボックスが表示され、次の手順を続行できます。

8 [スーパー管理者の追加] ダイアログ ボックスで、Active Directory 検索機能を使用し、コンソールを使用して環境で管理アクションを実行する Active Directory 管理者グループを選択します。

この顧客アカウントの Active Directory ドメインが設定されたので、この割り当てにより、少なくとも 1 つの Active Directory ドメインのユーザー アカウントに対して、Horizon Universal Console にログインして Horizon Cloud 環境で管理タスクを実行するを使用してログインするための権限が付与されます。

重要： 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 ポッドがある場合は、前提条件の説明に従って、ドメイン参加アカウントを含む Active Directory グループをスーパー管理者ロールに追加する必要があります。ポッド フリートにそれらの古いマニフェストで実行されているポッドがある場合、ドメイン参加アカウントがスーパー管理者ロールを持つどの Active Directory グループにも属していない場合、これらのポッドで仮想マシンのインポート ワークフローを使用すると失敗する可能性があります。

9 [保存] をクリックします。

結果

これで以下の項目が設定されました。

- Active Directory ドメインは、この Horizon Cloud 顧客アカウントに関連付けられたクラウド構成の Active Directory ドメインの 1 つです。
- Microsoft Azure のポッドの場合、Horizon Cloud には、デスクトップ関連の仮想マシンをドメインに参加させることを含むシステム操作に必要なドメイン参加アカウントがあります。
- VMware アカウントの認証情報を使用して Horizon Cloud にログインした後、Active Directory ログイン ウィンドウで、その Active Directory 内で Horizon Cloud ロールを割り当てられたユーザーは、Active Directory アカウントに対応するドメインを選択できます。
- スーパー管理者ロールが付与されたグループ内のユーザーは、最初のログイン画面で関連付けられた VMware アカウントの認証情報を使用してログインすると、コンソールにアクセスして管理アクティビティを実行できます。これらの管理者が最初のログイン手順で自分の VMware アカウントの認証情報を使用できるようにするには、Horizon Cloud テナント環境にログインし、Horizon Universal Console を使用してアクションを実行するための管理者ロールを組織内の個人に付与するで説明する手順を実行します。
- 登録された Active Directory ドメインからのユーザー アカウントは、Microsoft Azure のポッドからのリソースを含む割り当てに対して選択できます。
- コンソールのヘルプ デスク機能は、その登録された Active Directory ドメインのユーザー アカウントで使用できます。

次のステップ

この時点から、通常は次のタスクを実行します。

- このドメイン内の追加ユーザーに、環境を管理するためにアクセス権限を付与します。まず関連付けられた Horizon Cloud ロールがある VMware アカウントを追加してから、それらの Active Directory アカウントに適切な Horizon Cloud ロールを付与します。Horizon Cloud テナント環境にログインし、Horizon

Universal Console を使用してアクションを実行するための管理者ロールを組織内の個人に付与するおよび Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるを参照してください。

- コンソールへの読み取り専用アクセス権限を付与するこのドメイン内のユーザーにデモ管理者ロールを割り当てます。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 プラクティスおよび Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対してコンソールのどの部分を有効にするかを制御するロールをそのグループに割り当てるを参照してください。

Horizon Cloud のクラウド構成の Active Directory ドメイン用に補助バインド アカウントを追加する

Horizon Cloud 環境に最初の Active Directory ドメインを登録するときは、構成に 1 つの補助ドメイン バインド アカウントが必要です。少なくとも 1 つの補助ドメイン バインド アカウントがあれば、Active Directory ドメインでプライマリ バインド アカウントにアクセスできない場合に管理者ユーザーが管理コンソールからロックアウトされることがなくなります。オプションで、クラウド構成の Active Directory ドメイン用に追加の補助バインド アカウントを構成することができます。ドメイン用に構成されているプライマリ バインド アカウントと最初の補助バインド アカウントの両方がアクセス不可になった場合、システムでは次の補助バインド アカウントを使用してその Active Directory ドメインに接続します。

前提条件

Active Directory ドメインが Horizon Cloud アカウントのクラウド構成のドメインの 1 つであることを確認するには、[設定] - [Active Directory] に移動し、ドメインがページに表示されているかどうかを確認します。

コンソールでドメインにすでに構成されている次のアカウントに対するユーザー名とパスワード情報があることを確認します。これは、このタスクの実行時にユーザー インターフェイスで既存のパスワードを確認することを求められるためです。

- すでに構成されているバインド アカウントのパスワード
- ユーザー インターフェイスですでに構成されているドメイン参加アカウントのパスワード

追加するバインド アカウントのユーザー名およびパスワード情報と、これが ドメイン バインド アカウント - 必須の特性 に記載されている要件に準拠していることを確認します。このセクションで説明されているように、プライマリおよび補助ドメイン バインド アカウントには常にスーパー管理者ロールが割り当てられます。これにより、コンソールで管理アクションを実行するためのすべての権限が付与されます。スーパー管理者権限を必要としないユーザーは、ドメイン バインド アカウントにアクセスできないようにする必要があります。

注意： 時間の経過とともに誤ってロックアウトされるのを防ぐため、ドメイン バインド アカウントがこれらの条件（特にアカウント パスワードを期限切れにしたり、変更やロックアウトをすることはできないこと）を満たしていることを確認してください。このアカウント設定を使用する必要があります。これは、Active Directory を問い合わせるためにこのアカウントがシステムでサービス アカウントとして使用されるためです。

手順

1 コンソールで、[設定] - [Active Directory] の順にクリックします。

2 補助バインド アカウントを追加する Active Directory ドメインをクリックします。

3 表示されるドメイン バインド設定の横にある [編集] をクリックします。

4 [Active Directory の編集] ダイアログ ボックスで、プライマリ バインド アカウントのパスワードを入力します。

ここでパスワードを入力すると、[ドメイン バインド] ボタンをクリックして変更を保存できるようになります。

5 詳細プロパティを展開し、[補助ドメイン バインド アカウントの追加] をクリックします。

補助アカウント情報のセクションがダイアログ ボックスに追加されます。

6 アカウント認証情報を入力します。

注： ユーザー名のフィールドには、`ourbindaccount2` のようにユーザー名のみを指定します。ここにドメイン名を含めないでください。

7 [ドメイン バインド] をクリックします。

8 表示される以降の各ウィンドウで、[保存] をクリックして既存の設定を確認します。

[ドメイン参加] ウィンドウが表示されたら、ドメイン参加アカウントのパスワードを入力してから、[保存] をクリックします。

結果

プライマリおよび補助バインド アカウントがアクセス不可になった場合は、補助バインド アカウントがシステムで使用できるようになります。

手順を繰り返して複数の補助バインド アカウントを追加できます。補助バインド アカウントのパスワードを変更する、または削除するには、[Active Directory の編集] ウィンドウの詳細プロパティ領域に表示される対応するリンクを使用します。

Horizon Universal Console 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

このドキュメントのトピックでは、ユーザーが Horizon Universal Console にログインして Horizon Cloud 環境で作業する際にユーザーに付与する必要がある 2 種類のロールに関するベスト プラクティスについて説明します。ロールの 1 つは、Horizon Universal Console ユーザー インターフェイス自体のさまざまな部分を有効または無効にするために使用されます。もう 1 つは、そのロールが割り当てられたユーザーによって呼び出すことができ

るアクションを決定するために使用されます。特定のユーザーに付与する 2 つのロールの最終的な組み合わせが、そのユーザーに求められる結果を反映していることを確認する必要があります。

重要： ロールの 1 つはユーザーがコンソールに表示できるものを管理し、もう 1 つはアクションの呼び出しを管理するため、特定のユーザーが持つ 2 つのロールの全体的な組み合わせが、そのユーザーに求められる結果を反映していることを確認する必要があります。次のセクションでは、ベスト プラクティスの組み合わせについて説明します。これらのベスト プラクティスに従わないと、矛盾が発生する可能性があります。たとえば、割り当てられたロールがここで説明されているガイダンスに一致しない場合、ユーザーがコンソールにログインした後、ユーザーに実行させたいアクションを実行できなかったり、実行させたくないアクションを実行できたりする可能性があります。したがって、[全般設定] ページの [My VMware アカウント] 領域のユーザーのロールを、[役割と許可] ページでそのユーザーの Active Directory グループに割り当てられているロールに一致させることが重要です。

次のセクションでは、一般的な組織の標準シナリオに基づいて使用する 2 種類のロールとベスト プラクティスの組み合わせについて説明します。

注意: クラウドベースの Horizon Universal Console のツアーで説明されているように、第 1 世代のコンソールは動的であり、第 1 世代のテナント環境の最新の構成に適した機能を反映しています。このドキュメントで説明されている機能へのアクセスは、以下の要因（ただしこれらに限定されない）に依存する場合があります。

- その機能が最新の第 1 世代の Horizon Cloud ポッド マニフェスト、Horizon ポッドのバージョン、または Horizon Cloud Connector のバージョンでのみ使用可能なシステム コードに依存するかどうか。
- 機能が初登場したときに、リリース ノートに記載されているように制限付きで機能へのアクセスが提供されるかどうか。
- 機能に特定のライセンスまたは SKU が必要かどうか。

このドキュメントに機能の記載があり、第 1 世代のコンソールにその機能が表示されない場合は、まずリリース ノートを読み、その機能のアクセスが制限されているかどうか、およびテナントで有効化をリクエストする方法について確認します。または、このドキュメントに記載されている機能を使用する資格があり、コンソールにその機能が表示されない場合は、VMware Horizon Cloud Service の担当者に問い合わせるか、担当者がいない場合は Customer Connect でサポート リクエストを発行する方法 (VMware KB 2006985)の記載内容に従って、サービス リクエストを Horizon Cloud Service チームに発行することができます。

割り当てられたロールを持つ Active Directory グループ内のユーザーに対してコンソールのユーザー インターフェイスのさまざまな部分を有効または無効にするロール

これらのロールはシステムで事前に定義されており、Active Directory グループに関連付けられています。個人が Horizon Cloud テナント環境への認証についてされると、コンソールは、個人のアカウントが配置されている Active Directory (AD) グループを検出します。また、コンソールは、コンソールの [役割と許可] ページでこれらのロールのどちらが AD グループに割り当てられているかも識別します。次に、ユーザーがコンソールのユーザー インターフェイス ページ、タブ、およびウィンドウを移動すると、それらのアイテムは、ユーザーの AD グループに割り当てられたロールに応じて有効または無効として表示されます。

重要： これらのロールを個別の AD ユーザー アカウントではなくグループにのみ割り当てることができる点は、同じ AD ドメイン グループにこれらのロールの 2 つを割り当てることを避ける必要があることを意味します。これらのロールの 2 つを同じ AD グループに付与し、そのグループのユーザーがログインした場合、両方のロールがそのユーザーのグループに割り当てられていることをコンソールが識別すると、ユーザー インターフェイス ページを移動するときに無効化されたアイテムが表示される場合があります。これは、2 つのロールのいずれかがそれらのアイテムへのアクセスを妨げるためです。

これらの各ロールは、AD グループのレベルで適用します。これらは個人レベルではなくグループ レベルで適用されるため、同じ AD グループ内のすべての個人は、Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるロールを取得します。管理者は、AD 環境の AD グループに含まれる個人を制御します。したがって、AD 環境内の個人をある AD グループから別のグループに移動するときは、他の割り当てられたロール（My VMware アカウントに割り当てられているロール）と引き続き一致するロールの 1 つを持つグループに移動する必要があります。ある AD グループから別のグループに個人を移動するときは、個人の新しい AD グループに割り当てられたこのロール タイプのロールとの整合性を保つように他の種類のロール（個人の My VMware アカウントに割り当てられているロール）を調整する必要があるかどうかを検証する必要があります。

これらのロールの 1 つの例は、`Help Desk Read Only Administrator` ロールです。[役割と許可] ページで AD グループにそのロールが割り当てられると、コンソールではそのグループの個人がエンド ユーザーのユーザー カードに移動して情報を表示できますが、デスクトップで操作を実行することはできません。

My VMware アカウントにロールが割り当てられているユーザーが呼び出すことができるアクションを決定するロール

他のロール タイプと同様に、これらのロールはシステムで事前定義されています。これらのロールは、[全般設定] ページの [My VMware アカウント] 領域で構成されている My VMware アカウントに関連しています。個人が Horizon Cloud テナント環境への認証についてされると、コンソールは、ログイン セッションの認証に使用された My VMware アカウントに割り当てられているロールを検出します。次に、ユーザーがコンソールでアクションを呼び出そうとすると、システムは、[全般設定] ページでログインしたユーザーの My VMware アカウントに割り当てられているこのロールに応じて、API 呼び出しの実行を許可または禁止します。

その結果、コンソールへの最初の認証後、この割り当てられたロールは他のタイプの割り当てられたロールと連携して機能することが多くなります。

1 ユーザーがコンソールのユーザー インターフェイス ページ、タブ、およびウィンドウを移動すると、ユーザーの AD グループに割り当てられたロールに応じてユーザー インターフェイス要素が有効または無効として表示されます。

2 ユーザーが API 呼び出しを実行するボタンをクリックしてアクションを実行すると、My VMware アカウントに割り当てられたロールがそのアクションの実行を許可しない場合、API 呼び出しは実行されず、アクションは完了しません。

重要： コンソールで、このロールがユーザーの AD グループに割り当てられたロールと連携して動作する場合（後者はアクティブなコンソール要素を決定し、前者は要素がクリックされたときに実行を完了できるアクションを決定します）、特定のユーザーが持つ 2 つのロールの全体的な組み合わせが、そのユーザーに求められる結果を反映していることを確認する必要があります。反映していない場合は、矛盾した結果が生じる可能性があります。ある AD グループから別のグループに個人を移動するときは、My VMware アカウントのロールが新しい AD グループのロールと一致していることを確認し、必要に応じて調整します。次のセクションでは、標準のベスト プラクティスの組み合わせについて説明します。

5 つの標準的なベスト プラクティスのロールの組み合わせ

次の表に従って個人の 2 つのロールが調整されていない場合、矛盾する動作が発生する可能性があるため、次の表に従って組織の個人に付与されたロールを調整することをお勧めします。システムは、AD グループ内の個人の My VMware アカウントに割り当てられたロールよりも制限の少ないロールをそのグループに割り当てることを妨げません。個人が複数の AD グループに属している場合は、[役割と許可] ページでそれらのグループに割り当てられているロールが相互に整合性が取られ、また、個人の My VMware アカウントのロールと整合性が取られていることを確認してください。

[全般設定] ページでのユーザーの My VMware アカウントのロール	[ロールと許可] ページでのユーザーの Active Directory グループのロール	説明
顧客管理者	スーパー管理者	コンソールのすべての領域を表示し、コンソールですべてのアクションを実行するためのフル アクセス。
顧客割り当て管理者	割り当て管理者	コンソールのすべての領域を表示し、エンドユーザーの割り当てとファームの変更および管理に関連するアクションを実行できます。
顧客管理者 (読み取り専用)	デモ管理者	コンソールのすべての領域の表示、設定の表示、追加の選択肢を表示するオプションの選択が可能です。アイテムの削除など、環境を変更するアクションを呼び出す機能はありません。この組み合わせの使用例は、システムへの変更を回避しながら、組織内のユーザーがログインしてシステムの機能を別のユーザーにデモンストレーションすることです。

[全般設定] ページでのユーザーの My VMware アカウントのロール	[ロールと許可] ページでのユーザーの Active Directory グループのロール	説明
顧客ヘルプデスク	ヘルプ デスク管理者	コンソールのヘルプデスク関連領域を表示し、コンソールが提供するすべてのヘルプデスク関連アクションを実行するためのアクセス。この組み合わせの目的は、ユーザーがユーザー カード機能を使用して、エンド ユーザー セッションのステータスを確認し、セッションのトラブルシューティングを実行することです。
顧客ヘルプデスク (読み取り専用)	ヘルプ デスク読み取り専用管理者	コンソールのヘルプデスク関連の領域を表示し、ユーザー カードのエンド ユーザー セッションのステータスを確認するためのアクセス。ヘルプデスク関連のアクションを呼び出す機能は使用できません。

ユーザーを読み取り専用に制限し、コンソールのすべての領域でコンソールへのアクセスを表示する

個人がコンソールのすべてのユーザー インターフェイス ページを参照し、ダイアログを開いてレポートを表示できるようにする一方で、テナント環境で何かを変更するアクションを呼び出すことができないようにするには、次の両方の条件が満たされている必要があります。

- [全般設定] ページの [My VMware アカウント] 領域で、`Customer Administrator Read-Only` ロールを My VMware アカウントに割り当てます。個人のアカウントに別のロールがリストされている場合は、[My VMware アカウント] セクションからその行を一度削除し、次に `Customer Administrator Read-Only` ロールを指定して再度追加することができます。
- [役割と許可] ページで、`Demo Administrator` ロールをその個人の Active Directory グループに割り当てます。

これらの条件が両方とも満たされると、個人はコンソールにログインし、コンソールのすべてのページに移動し、ページを参照し、ダイアログを開いてレポートを表示できるようになります。ただし、環境で何かを変更するアクションの実行は制限されます。

注： [役割と許可] ページは、個々のアカウント レベルではなく、AD グループ レベルで機能するため、組織の要件に応じて、AD グループに適切な個人のアカウントが含まれていることを確認する必要があります。

ユーザーのアクセスをコンソールのヘルプ デスク機能に制限し、実行できる機能をユーザー カードでのアクションに制限する

個人がコンソールにログインして、コンソールのすべての領域ではなく、ヘルプデスク関連の機能にのみアクセスできるようにし、その一方でヘルプデスク関連のアクションを実行できるようにする場合、次の両方の条件が満たされていることを確認する必要があります。

- [全般設定] ページの [My VMware アカウント] 領域で、`Customer Helpdesk` ロールを My VMware アカウントに割り当てます。個人のアカウントに別のロールがリストされている場合は、[My VMware アカウント] セクションからその行を一度削除し、次に `Customer Helpdesk` ロールを指定して再度追加することができます。
- [役割と許可] ページで、`Help Desk Administrator` ロールをその個人の Active Directory グループに割り当てます。

これらの条件が両方とも満たされると、個人はコンソールにログインし、ヘルプデスク関連の機能を参照して、ヘルプデスク関連のアクションを実行できるようになります。

注： [役割と許可] ページは、個々のアカウント レベルではなく、AD グループ レベルで機能するため、組織の要件に応じて、AD グループに適切な個人のアカウントが含まれていることを確認する必要があります。

ユーザーのアクセスをコンソールのヘルプデスク機能に対する読み取り専用アクセスに制限する

個人がコンソールにログインして、ヘルプデスク関連の機能に読み取り専用でアクセスできるようにし、その一方でヘルプデスク関連のアクションは実行できないようにする場合、次の両方の条件が満たされていることを確認する必要があります。

- [全般設定] ページの [My VMware アカウント] 領域で、`Customer Helpdesk Read-Only` ロールを My VMware アカウントに割り当てます。個人のアカウントに別のロールがリストされている場合は、[My VMware アカウント] セクションからその行を一度削除し、次に `Customer Helpdesk Read-Only` ロールを指定して再度追加することができます。
- [役割と許可] ページで、`Help Desk Read Only Administrator` ロールをその個人の Active Directory グループに割り当てます。

これらの条件が両方とも満たされると、個人はコンソールにログインして、ヘルプデスク関連の機能を読み取り専用で使用できるようになります。

注： [役割と許可] ページは、個々のアカウント レベルではなく、AD グループ レベルで機能するため、組織の要件に応じて、AD グループに適切な個人のアカウントが含まれていることを確認する必要があります。

ユーザーのアクセスをコンソールの割り当ておよびファーム関連機能に制限する

個人がコンソールにアクセスして、エンドユーザーの割り当てとファームの管理に関連する操作を実行できるようにし、コンソールのその他すべての領域への読み取り専用アクセスを行えるようにする場合は、次の両方の条件が満たされていることを確認する必要があります。

- [全般設定] ページの [My VMware アカウント] 領域で、`Customer Assignment Administrator` ロールを My VMware アカウントに割り当てます。個人のアカウントに別のロールがリストされている場合は、[My VMware アカウント] セクションからその行を一度削除し、次に `Customer Assignment Administrator` ロールを指定して再度追加することができます。
- [役割と許可] ページで、`Assignment Administrator` ロールをその個人の Active Directory グループに割り当てます。

これらの条件が両方とも満たされると、個人はコンソールにログインし、コンソールのすべてのページに移動して表示し、エンドユーザーの割り当てとファームを作成、変更、または削除するアクションを実行できるようになります。また、仮想マシンの構成、電源管理、リモート アプリケーションの構成など、割り当てとファームの管理に関連する操作を実行することもできるようになります。

注： [役割と許可] ページは、個々のアカウント レベルではなく、AD グループ レベルで機能するため、組織の要件に応じて、AD グループに適切な個人のアカウントが含まれていることを確認する必要があります。

コンソールのすべての領域とアクションに対するフル アクセスをユーザーに許可する

個人にコンソールへのフル アクセスを許可し、コンソールのすべての領域を表示し、テナント環境で何かを変更するアクションを呼び出すことができるようにする場合は、次の両方の条件が満たされていることを確認する必要があります。

- [全般設定] ページの [My VMware アカウント] 領域で、`Customer Administrator` ロールを My VMware アカウントに割り当てます。個人のアカウントに別のロールがリストされている場合は、[My VMware アカウント] セクションからその行を一度削除し、次に `Customer Administrator` ロールを指定して再度追加することができます。
- [役割と許可] ページで、`Super Administrator` ロールをその個人の Active Directory グループに割り当てます。

これらの条件が両方とも満たされると、個人はコンソールにログインし、コンソールのすべてのページに移動し、環境で何かを変更するアクションを実行できるようになります。

注： [役割と許可] ページは、個々のアカウント レベルではなく、AD グループ レベルで機能するため、組織の要件に応じて、AD グループに適切な個人のアカウントが含まれていることを確認する必要があります。

Horizon Cloud テナント環境にログインし、Horizon Universal Console を使用してアクションを実行するための管理者ロールを組織内の個人に付与する

クラウドベースの管理コンソールに対する認証プロセス中に、最初のログイン画面では特定のテナントに関連付けられた既存の VMware Customer Connect アカウントが必要です。会社または組織内の他のユーザーに、その最初のログイン画面にログインする権限を付与するには、個々の VMware Customer Connect アカウントがこの同じテナントと適切なロールに関連付けられている必要があります。個人のアカウントに割り当てられたロールは、その個人がコンソールを使用してテナント内で実行することが許可されるアクションのタイプと一致している必要があります。

注： テナントにユーザーを管理者として追加できるもう 1 つの方法は、ナレッジベースの記事 KB2006985 の手順を使用して、Customer Connect Support で技術以外のサポート リクエストを提出することです。この方法で追加するには、ユーザーのアカウントのドメインが、テナントを作成した最初の購入または試用版の注文のドメインと一致する必要があります。

この手順を使用して割り当てるロールは、ユーザーの認証済みセッションでそのユーザーがコンソールに表示できるもの、および、コンソールに表示されたものに対して実行できるアクションの両方を決定するためにコンソールが使用する 2 種類のロールのいずれかです。VMware Customer Connect アカウントに割り当てられているロールによって、次の項目が決定されます。

- 個人がコンソールのログイン画面を使用してコンソールに対して認証できるか。
- ユーザーがコンソールのすべての領域を表示できるか、または Horizon Cloud 環境内のヘルプ デスク機能など、領域のサブセットのみを表示できるか。

- 表示できるコンソールの領域内で、ユーザーが呼び出すことができる特定のアクション。

重要： ここで説明するこのロールは認証されたセッションで実行できるアクションを管理し、他の Active Directory ドメイン関連のロールはコンソールのどの領域をセッションに表示するかを管理するため、個人が組織内の異なる部署や Active Directory グループに移動した場合でも、2 つのロールの全体的な組み合わせが特定の個人に求められる結果を継続して反映するようにする必要があります。2 種類のロールの詳細と、ロール割り当ての組み合わせのベスト プラクティスについては、Horizon Universal Console 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。

VMware Customer Connect アカウントに関連付けられたロールに加え、追加の Active Directory ドメインをクラウド構成の Active Directory ドメインとして Horizon Cloud テナント環境に登録する、ユーザーの Active Directory グループに割り当てられたロールは、VMware Customer Connect アカウントに関連付けられたロールと連携して使用できるアクセス権をユーザー アカウントに付与します。ユーザー アカウントが属する Active Directory グループに割り当てられたロールは、コンソールの 2 番目のログイン画面で Active Directory アカウントの認証情報を使用してログインしたユーザーが、コンソールのどの要素にアクセスできるかを制御します。これらのロールのリストについては、Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるを参照してください。

重要： これらの手順は vmware.com で VMware Customer Connect アカウントが作成される前に実行することができますが、アカウントが vmware.com で作成されないと、そのアカウントを使用してコンソールにログインすることができません。VMware Customer Connect アカウントは、https://customerconnect.vmware.com/account-registration で登録プロセスを使用して作成されます。

これらの手順は https://cloud.horizon.vmware.com の Horizon Universal Console を使用して実行します。そのコンソールで、VMware Customer Connect アカウントをテナントに関連付けます。コンソールを使用する場所は、テナントにクラウド接続されたポッドがないか、少なくとも 1 つあるかによって異なります。テナントにクラウド接続されたポッドがまだない場合は、Horizon Universal Console の [はじめに] ウィザードの [全般的なセットアップ] セクションを使用してこれらの手順を実行する必要があります。クラウド接続されたポッドが少なくとも 1 つ存在するようになるまで、コンソールでは [はじめに] 以外のページへのアクセスが禁止されます。

注意: クラウドベースの Horizon Universal Console のツアーで説明されているように、第 1 世代のコンソールは動的であり、第 1 世代のテナント環境の最新の構成に適した機能を反映しています。このドキュメントで説明されている機能へのアクセスは、以下の要因（ただしこれらに限定されない）に依存する場合があります。

- その機能が最新の第 1 世代の Horizon Cloud ポッド マニフェスト、Horizon ポッドのバージョン、または Horizon Cloud Connector のバージョンでのみ使用可能なシステム コードに依存するかどうか。
- 機能が初登場したときに、リリース ノートに記載されているように制限付きで機能へのアクセスが提供されるかどうか。
- 機能に特定のライセンスまたは SKU が必要かどうか。

このドキュメントに機能の記載があり、第 1 世代のコンソールにその機能が表示されない場合は、まずリリース ノートを読み、その機能のアクセスが制限されているかどうか、およびテナントで有効化をリクエストする方法について確認します。または、このドキュメントに記載されている機能を使用する資格があり、コンソールにその機能が表示されない場合は、VMware Horizon Cloud Service の担当者に問い合わせるか、担当者がいない場合は Customer Connect でサポート リクエストを発行する方法 (VMware KB 2006985)の記載内容に従って、サービス リクエストを Horizon Cloud Service チームに発行することができます。

手順

1 https://cloud.horizon.vmware.com で Horizon Universal Console にログインします。

2 コンソールで、クラウド接続されたポッドがないか、少なくとも 1 つあるかによって、次のいずれかの方法を使用して、VMware Customer Connect アカウントを環境に関連付けます。

ヒント: My VMware という名前は、VMware Customer Connect の以前の名前でした。両方の名前は、コンソールで同じ意味で使用されます。

クラウド接続されたポッドがない場合

テナントのポッド フリートに少なくとも 1 つのポッドが存在するようになるまで、コンソールでは Horizon Universal Console の [はじめに] ウィザードの [全般的なセットアップ] セクション以外のページへのアクセスが禁止されます。このページで、[全般的なセットアップ] - [My VMware アカウント] - [追加] の順にクリックします。

1 つ以上のポッドがある場合

テナントにクラウド接続されたポッドが少なくとも 1 つある場合は、コンソールの [はじめに] ページに加えて、[全般設定] ページにアクセスできます。[はじめに] ページの [My VMware アカウント] 領域を使用するか、[設定] - [全般設定] - [編集] の順にクリックして [My VMware アカウント] 領域までスクロールします。

すでに環境に関連付けられている VMware Customer Connect アカウントのリストが表示されます。

3 リストの一番下のエントリで表示されるプラス記号のアイコン (⊞) をクリックして、リストに行を追加します。

姓、名、VMware Customer Connect アカウント ID を入力するためのフィールドと、テナントの役割を選択するためのフィールドがある新しい行が表示されます。

4 環境に関連付けるアカウントごとに行を作成し、テナントの役割の選択などの、必要な情報を各行に入力します。

別の役割を選択しない限り、役割はデフォルトで顧客管理者になります。ユーザーがコンソールでアクションを実行したときに、情報の表示以外の結果にならないようにする場合は、読み取り専用ロールの 1 つを割り当てます。

ユーザーのアカウントに対するロール	説明
顧客管理者	コンソールのすべてのアクションを実行できます。これには、ポッドのオンボーディングまたはアイテムの削除が含まれます。
顧客割り当て管理者	エンドユーザーの割り当てとファームの変更に関連するアクションを実行できます。仮想マシンの構成、電源管理、リモート アプリケーションの構成など、割り当てとファームの管理に関連する操作も実行できます。
顧客管理者 (読み取り専用)	ポッドのオンボーディングや全般設定の変更など、環境を変更するアクションの呼び出しを防止します。
顧客ヘルプデスク	コンソールのヘルプデスク関連の領域では、ヘルプデスク関連のすべてのアクションを実行できます。
顧客ヘルプデスク (読み取り専用)	コンソールのヘルプデスク関連の領域内では、情報の表示のみを実行できます。これらのコンソール領域内で何かを変更するアクションの呼び出しを防止します。

5 [保存] をクリックして、情報をシステムに保存します。

結果

追加されたすべての VMware Customer Connect アカウント ID が vmware.com に存在する場合、それらを使用して最初の Horizon Cloud ログイン画面で認証することができます。

重要： 完了した手順では、実際の VMware Customer Connect アカウントは作成されません。このようなアカウントは、https://customerconnect.vmware.com/account-registration で登録プロセスを使用して作成されます。

次のステップ

追加されたユーザーの Active Directory アカウントが、Horizon Cloud の役割がまだ関連付けられていない Active Directory グループにある場合は、Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるの説明どおりに手順を完了します。Horizon Universal Console 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 プラクティスで説明されている組み合わせのベスト プラクティスに従ってください。

Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てる

クラウドベースの管理コンソールに対する認証プロセスでは、最初のログイン画面に対して認証した後、環境に登録した Active Directory ドメインに応じて、組織の個人が 2 番目のログイン画面に Active Directory ユーザー アカウントの認証情報を入力します。システムには、さまざまな Active Directory グループに割り当て可能な事前定義済みの役割が提供されています。これらの Active Directory ドメイン関連のロールは、ログインしたユーザーがコンソール内を移動するときに、コンソールのどの領域が表示可能で有効になるか、または表示可能で無効になるかを制御します。組織の適切な Active Directory グループにロールを割り当てて、そのグループのユーザーがコンソールを使用して許可された作業アクティビティを実行できるようにする必要があります。

注意: クラウドベースの Horizon Universal Console のツアーで説明されているように、第 1 世代のコンソールは動的であり、第 1 世代のテナント環境の最新の構成に適した機能を反映しています。このドキュメントで説明されている機能へのアクセスは、以下の要因（ただしこれらに限定されない）に依存する場合があります。

- その機能が最新の第 1 世代の Horizon Cloud ポッド マニフェスト、Horizon ポッドのバージョン、または Horizon Cloud Connector のバージョンでのみ使用可能なシステム コードに依存するかどうか。
- 機能が初登場したときに、リリース ノートに記載されているように制限付きで機能へのアクセスが提供されるかどうか。
- 機能に特定のライセンスまたは SKU が必要かどうか。

このドキュメントに機能の記載があり、第 1 世代のコンソールにその機能が表示されない場合は、まずリリース ノートを読み、その機能のアクセスが制限されているかどうか、およびテナントで有効化をリクエストする方法について確認します。または、このドキュメントに記載されている機能を使用する資格があり、コンソールにその機能が表示されない場合は、VMware Horizon Cloud Service の担当者に問い合わせるか、担当者がいない場合は Customer Connect でサポート リクエストを発行する方法 (VMware KB 2006985)の記載内容に従って、サービス リクエストを Horizon Cloud Service チームに発行することができます。

この手順を使用して割り当てるロールは、ユーザーの認証済みセッションでそのユーザーがコンソールに表示できるもの、および、コンソールに表示されたものに対して実行できるアクションの両方を決定するためにコンソールが使用する 2 種類のロールのいずれかです。

Horizon Universal Console にログインして Horizon Cloud 環境で管理タスクを実行するで、コンソールの最初のログイン画面では、[全般設定] ページを使用してロールに関連付けられている、VMware Customer Connect アカウントが使用されます。これらのアカウントは、以前は My VMware アカウントと呼ばれていました。

2 番目のログイン画面では、[役割と許可] ページを使用してロールに関連付けられている、Active Directory (AD) 認証情報が使用されます。これらの AD ドメイン関連のロールは、コンソールの機能と要素の可視性を決定します。このロールはまた、ユーザーがコンソールを移動するときに、どのユーザー インターフェイス要素が無効として表示されるかを決定します。

たとえば、[割り当て管理者] ロールが割り当てられている AD グループのユーザーは、エンドユーザーの割り当ておよびファームの管理に関連する操作を実行できますが、他のタイプの操作は実行できません。[ヘルプ デスク読み取り専用管理者] ロールが割り当てられている AD グループのユーザーは、エンド ユーザーのユーザー カードに移動して情報を表示することができますが、ユーザー セッションでトラブルシューティング操作を実行できません。一方、[ヘルプ デスク管理者] ロールが割り当てられている AD グループのユーザーは、ユーザー カードに移動して情報を表示したり、ユーザー セッションでトラブルシューティング操作を実行したりできます。[ヘルプ デスク管理者] ロールの場合、AD グループが実行できるトラブルシューティング操作の範囲を制限することもできます。

これらの AD ドメイン関連のロールは、組織内のユーザーが標準のログイン ワークフローを使用してログインする際に使用する VMware Customer Connect アカウントのロールと連動します。したがって、個人が組織内の異なる部署や AD グループに移動した場合でも、2 つのロールの全体的な組み合わせが特定の個人に求められる結果を継続して反映するようにする必要があります。2 種類のロールの詳細と、ロール割り当ての組み合わせのベスト プラクティスについては、Horizon Universal Console 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。

注： Horizon Cloud Service プラットフォームを使用して、cloud.vmware.com の VMware Cloud Services を介して行ったロールの変更は、Horizon Universal Console には表示されません。以下の手順に従って、Horizon Universal Console で直接ロールを変更する必要があります。

注意： スーパー管理者の役割は、どの Active Directory ユーザー アカウントが Horizon Cloud テナント アカウントにログインしてコンソールで管理操作を実行できるかを管理することです。これには、ここに示す Active Directory グループに役割を割り当てる手順も含まれます。スーパー管理者の役割に割り当てられた Active Directory グループが 1 つしか存在しない場合、別の管理者グループをこのスーパー管理者の役割に追加するまで、その管理者グループを Active Directory システムから削除したり、Active Directory システムに表示される GUID を変更したりしないでください。Active Directory システムからグループを削除したり、Active Directory システムの GUID が変更されるような変更を行ったりしても、その変更は Horizon Cloud 制御プレーンに伝達されないため、Horizon Cloud はスーパー管理者の役割を持つ Active Directory グループを正しく認識できなくなります。そのグループがスーパー管理者ロールに割り当てた唯一のグループである場合、スーパー管理者アクセス レベルでログインすることができた Active Directory アカウントは、ログインして管理操作を実行することができなくなる場合があります。これには、役割を Active Directory グループに割り当てて、スーパー管理者アクセス権を持つ Active Directory アカウントのセットの再確立も含まれます。ドメインバインド アカウントには常にスーパー管理者ロールが割り当てられます。スーパー管理者ロールに割り当てられている単一の AD グループを削除し、ドメインバインド アカウントがそのグループに含まれていない場合、ドメインバインド アカウントの認証情報を使用してコンソールにログインし、スーパー管理者ロールを新しい AD グループに割り当てる手順を実行してみてください。ただし、ドメインバインド アカウントを使用してログインできない場合は VMware サポートに連絡して、テナント アカウントへの管理アクセスの復元を支援する必要があります。

重要： これらの Horizon Cloud の役割は、グループのみに割り当てることができます。システムは、役割ごとに個別の Active Directory ユーザー アカウントを選べる方法を提供しません。

ロールを個別のアカウントではなくグループにのみ割り当てることができる点は、同じ AD グループに 2 つのロールを割り当てることを避ける必要があることを意味します。スーパー管理者ロールは、このコンソールでのすべての管理アクションを実行するためのすべての権限を付与することを目的としたもので、デモ管理者ロールは読み取り専用ロールです。これらの両方のロールを同じ AD グループに指定すると、そのグループ内のすべてのユーザーは、スーパー管理者ロールの権限を受け取りません。コンソールでのアクションが制限され、環境に対するすべての管理を実行できない場合があります。

デフォルトでは、次の事前定義済みの役割が提供されます。事前定義済みの役割は変更できません。

表 1-13. Horizon Cloud ロールベースのアクセス コントロール グループ

役割	説明
スーパー管理者	AD ドメインの少なくとも 1 つのグループ、そしてオプションでその他に割り当てる必要がある必須のロール。このロールは、コンソールのすべての領域にアクセスし、コンソールで管理アクションを実行するためのすべての権限を付与します。 プライマリ ドメイン バインド アカウントおよび補助ドメイン バインド アカウントには、常にスーパー管理者ロールが割り当てられます。これにより、コンソールで管理アクションを実行するためのすべての権限が付与されます。スーパー管理者権限を必要としないユーザーは、管理者が指定したドメイン バインド アカウントにアクセスできないようにする必要があります。 **注：** 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ポッドがある場合は、ドメイン参加アカウントが、スーパー管理者ロールが付与されるグループの 1 つに属していることを確認する必要があります。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。
割り当て管理者	テナント環境でこの機能が有効になっている場合は、オプションでこのロールを 1 つ以上のグループに割り当てることができます。このロールが割り当てられている AD グループは、コンソールにアクセスして、エンドユーザーの割り当てとファームを作成、変更、および削除できます。このロールが割り当てられているグループは、仮想マシンの構成、電源管理、リモート アプリケーションの構成など、割り当てとファームの管理に関連する操作も実行できます。
ヘルプ デスク管理者	1 つ以上のグループに割り当てることができる役割。このロールの目的は、このロールがある AD グループがユーザー カードの機能を使用して以下のことを行えるようにするために、コンソールへのアクセスを提供することです。 ■ エンドユーザー セッションのステータスを確認する。 ■ セッションでのトラブルシューティングの操作を実行する。 デフォルトでは、このロールが割り当てられている AD グループには、コンソールに一覧表示されている割り当てまたはファームに関連付けられているセッションでトラブルシューティング操作を実行する権限があります。テナント環境でこの機能が有効になっている場合は、オプションでグループの権限を変更し、そのグループのトラブルシューティング操作の範囲を特定の割り当ておよびファームに関連付けられているセッションのみに制限することもできます。グループの権限範囲を変更するには、そのグループの編集アイコンをクリックします。 **注：** AD グループの権限範囲に割り当てまたはファームを含め、後でその割り当てまたはファームを削除しようとすると、その割り当てまたはファームはグループの権限範囲からすぐに削除されます。削除プロセスが失敗し、割り当てまたはファームがまだ存在する場合は、それらにグループが引き続きアクセスできるよう、手動で権限範囲に追加し直す必要があります。
ヘルプ デスク読み取り専用管理者	1 つ以上のグループに割り当てることができる役割。このロールの目的は、このロールがある AD グループがユーザー カードの機能を使用してエンド ユーザー セッションのステータスを確認できるようにするために、コンソールへのアクセスを提供することです。
デモ管理者	1 つ以上のグループに割り当てることができる役割。Horizon Cloud テナント環境にログインし、Horizon Universal Console を使用してアクションを実行するための管理者ロールを組織内の個人に付与すると組み合わせると、このグループのユーザーは設定を表示し、オプションを選択して、コンソールに追加の選択肢を表示できますが、選択によって構成設定が変更されることはありません。

前提条件

- 既存の Active Directory グループに役割を割り当てる前に、Active Directory グループ内のユーザー アカウントのメンバーシップを確認して、ユーザー アカウントが確実に 1 つのみの Horizon Cloud の役割を受け取るようにします。必要に応じて、特定の Active Directory グループを作成します。これらの役割は Active Directory グループのレベルで割り当てられるため、ユーザーの Active Directory アカウントが 2 つの Active Directory グループに属していて、各グループに別の役割が割り当てられている場合は、予期しない結果が発生する可能性があります。コンソールの機能は、以下の優先順位に従って表示されます。

  a [スーパー管理者]

b [割り当て管理者]

c [ヘルプ デスク管理者]

d [デモ管理者]

e [ヘルプ デスク読み取り専用管理者]

この優先順位の結果として、ADGroup1 および ADGroup2 の両方の Active Directory グループにユーザーの Active Directory アカウントが属していて、ADGroup1 に [スーパー管理者] の役割を、ADGroup2 に [ヘルプ デスク読み取り専用管理者] の役割をそれぞれ割り当てられる場合は、コンソールには [スーパー管理者] の役割に従って、その他の役割の機能のサブセットではなくすべての機能が表示されます。この理由は、[スーパー管理者] の役割が優先的に取り扱われるためです。

- また、グループのメンバーの VMware Customer Connect アカウントに割り当てられているロールを確認して、それらのロールが Active Directory グループに割り当てられたロールと一致していることを確認します。Horizon Universal Console 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 プラクティスで説明されている組み合わせのベスト プラクティスに従ってください。

重要： システムは、Horizon Cloud の事前定義済みのすべてのロールに対して、最大 64 個の一意の Active Directory グループの割り当てをサポートします。

手順

1 コンソールで、[設定] - [役割と許可] に移動します。

2 事前定義済みのいずれかの役割を選択し、[編集] をクリックします。

3 検索ボックスを使用して、Active Directory グループを検索し、選択します。

検索結果が表示されるためには、少なくとも 3 文字以上を検索ボックスに入力する必要があります。

グループが選択したグループのセットに追加されました。

4 [保存] をクリックします。

重要： 保存アクションを実行した結果、すべてのロールに割り当てることができる Active Directory グループがシステムでサポートされている最大数を超える場合、システムは選択したグループをロールに保存しません。サポートされている最大値は、このドキュメント トピックの「前提条件」セクションに記載されています。

次のステップ

ドメイン グループ内のユーザーが VMware Customer Connect アカウントに対する適切なロールを持っていることを確認します。Horizon Universal Console 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 プラクティスおよび Horizon Cloud テナント環境にログインし、Horizon Universal Console を使用してアクションを実行するための管理者ロールを組織内の個人に付与するを参照してください。

第 1 世代のテナント - Horizon Cloud 環境の Cloud Monitoring Service (CMS) の有効化または無効化

第 1 世代のテナントのクラウド接続された個別のポッドおよびポッド全体でのキャパシティ、使用状況、および健全性を監視する機能を提供するデータを取得する前に、Cloud Monitoring Service (CMS) を有効にする必要があります。CMS は、Horizon Cloud の中心的なサービスの 1 つです。CMS はテナント レベルで有効になり、その設定はその第 1 世代の Horizon Cloud テナントに接続されているすべてのポッドに適用されます。

Cloud Monitoring Service (CMS) は、監視とレポートの目的で、クラウド接続されたポッドからセッション、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。データは、2 章 第 1 世代のテナント - 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 デスク機能の紹介で説明するように、コンソールのさまざまな場所に表示されます。

ヒント: 通常、Horizon Cloud テナントを初めて使用するときには、CMS がデフォルトでオンになっています。コンソールのページにビジュアル データが表示されない場合は、まず以下の手順に従って [全般設定] ページで CMS がオンになっていることを確認します。

テナントで Cloud Monitoring Service が有効になっている場合は、オプションでエンド ユーザーのセッションに関連するユーザー情報の追跡をオプトインまたはオプトアウトすることもできます。CMS がユーザー セッションについて収集する一般的な情報には、ログインした時間、セッションの期間、およびユーザーごとの平均セッション時間が含まれます。

- ユーザー データの収集をオプトインすると、サービスはこの情報を収集し、第 1 世代の Horizon Cloud 環境を使用している間維持します。「VMware ナレッジベースの記事 KB91183」で説明されているように、このデータは Workspace ONE Intelligence で入手できます。後でユーザー データの収集をしないように決定した場合は、[セッション データ] トグルをオフに切り替えて収集を停止します。その場合、収集したデータを削除することもできます。
- ユーザー データの収集をオプトアウトしたが、監視サービスを有効のままにすると、サービスは一定期間セッション データを収集し、ユーザー名をハッシュしてリアルタイム管理を可能にします。その結果、Horizon ユーザー使用量レポートなどの一部のレポートは使用できません。この場合、システムは、接続されたポッド内のアプリケーションおよびデスクトップに関連する他のデータの収集も継続します。

これらのトグルをオフに切り替えると、以前に収集したデータもすべて削除されます。[セッション データ] トグルを単独でオフに切り替えると、以前に収集されたユーザー関連データは削除されますが、ポッドレベルやセッション関連データなど、他のタイプの収集されたデータはそのまま残ります。[Cloud Monitoring Service] トグルをオフに切り替えると、テナントについて収集されたすべてのデータが削除されます。

注意: デスクトップ データを vRealize Operations Manager に送信しているクラウド接続された Horizon ポッドがある場合、CMS を有効にすると、データは代わりに Cloud Monitoring Service に送信されます。vRealize Operations Manager を引き続き使用してそのデスクトップ セッション データを収集するには、CMS を無効にします。

前提条件

クラウド接続された Horizon ポッドまたは Microsoft Azure のポッドに対して Cloud Monitoring Service を有効にするには、テナントのポッド フリートに少なくとも 1 つのポッドが必要です。

手順

1 [設定] - [全般設定] をクリックして、コンソールの [全般設定] ページに移動します。

2 ページを下にスクロールして、[監視] セクションを見つけます。

3 鉛筆アイコンをクリックして設定を変更します。

- [Cloud Monitoring Service] トグルを使用して、テナント環境のすべてのデータ収集を有効または無効にします。無効にすると、CMS はそのテナント環境内のクラウド接続ポッド全体からデータを収集しません。
- [セッション データ] トグルを使用して、エンド ユーザーのセッションに関連するユーザー情報の追跡をオプトインまたはオプトアウトします。

4 [保存] をクリックして、変更を保存します。

第 1 世代テナント - Horizon Universal Console を使用して Horizon Cloud テナントを VMware Cloud Services Engagement Platform および VMware Cloud Services にオンボーディングする

Horizon Cloud テナントを VMware Cloud Services Engagement Platform にオンボーディングすると、Horizon Cloud がグループまたは組織の VMware Cloud services 組織に関連付けられます。

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。

これらの手順を完了すると、VMware Cloud services の組織にログインし、[マイ サービス] の下の [Horizon Cloud] カードを使用できます。

注： VMware Cloud Services Engagement Platform は、VMware Cloud services という名前でも知られています。これらの 2 つの名前は、Horizon Cloud のドキュメントと Horizon Universal Console で同じ意味で使用される場合があります。

重要： 第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアーに記載されているように、クラウドベースのコンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。機能へのアクセスは、テナントのリージョン クラウド プレーン、クラウドに接続されたポッドがポッドの最新レベルのソフトウェアを実行しているかどうか、機能が特定のライセンスに基づいているかどうかなどの要因によって異なります。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。使用したい機能が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て、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。

Horizon Cloud のテナント レコードが、VMware Cloud Services Engagement Platform 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、Horizon Universal Console の上部に青いバナーが表示されます。このバナーは、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。

次のような状況では、このバナーは表示されません。

- Workspace ONE 環境のコンソールから Horizon Cloud カードをクリックしてコンソールにアクセスする場合。このシナリオでは Workspace ONE コンソールのサービス エリアに Horizon Cloud カードがあり、Horizon Cloud テナントがすでに VMware Cloud Services Engagement Platform にオンボーディングされていることを意味します。
- Horizon Cloud のユーザー レコードが環境を VMware Cloud Services Engagement Platform 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。この機能へのアクセスを要求するには、https://kb.vmware.com/s/article/2006985 の説明に従って VMware サポートにお問い合わせください。

このエンドツーエンドのプロセスでは、VMware Cloud services にアカウントを作成し、VMware Cloud services 内の既存の組織を選択するか、新しい組織を作成します。VMware Cloud services におけるこのプロセスの詳細については、VMware Cloud Services のドキュメント内の VMware Cloud Services への登録および ID およびアクセス権の管理のトピックを参照してください。

手順

1 青いバナーで、[オンボーディング] をクリックします。

オンボーディング プロセスを続行するための新しいボックスが表示されます。次のスクリーンショットは例を示します。

2 [オンボーディング] をクリックします。

VMware Cloud Services Engagement Platform ポータルでオンボーディング プロセスを続行するための別のボックスが表示されます。

3 [次へ] をクリックしてオンボーディング プロセスを続行します。

ブラウザが VMware Cloud services ポータルにリダイレクトします。

4 画面上のすべてのフォームとプロンプトに従って、VMware Cloud services の組織へのこの Horizon Cloud テナント環境のオンボーディングを完了します。

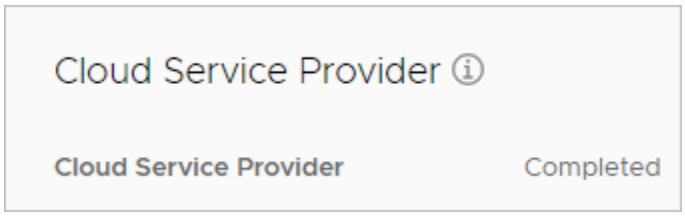
これらの画面上の手順の一部として、この Horizon Cloud テナントに関連付ける組織を選択します。組織と Horizon Cloud テナント間の関連付けは、1 対 1 の関連付けにする必要があります。選択した組織は、他の Horizon Cloud テナントと関連付けられていてはなりません。すべての既存の組織が他の Horizon Cloud テナントにすでに関連付けられている場合は、画面上の手順の一部として、このテナントに関連付ける新しい組織を作成できます。

結果

このプロセスが正常に完了すると、これらの項目が配置されます。

- VMware Cloud Services ポータル (vmw VMware Cloud Services) では、関連する VMware Cloud services 組織にリストされているサービスの中に、[Horizon Cloud Service] が表示されます。このエントリをクリックすると、VMware Cloud services からのクラウド サービス アカウントの認証情報を使用して Horizon Universal Console が自動的に起動し、認証が実行されます。

- Horizon Universal Console の [全般設定] ページには、VMware Cloud services へのオンボーディングが完了したことが示されます。



注： Horizon Cloud テナントと VMware Cloud services 組織を関連付けるプロセスには時間がかかることがあります。現在のステータスを確認するには、[全般設定] ページの [Cloud サービス プロバイダ] セクションの更新アイコンを使用します。30 分以上経過しても `Completed` のステータスが表示されない場合は、https://kb.vmware.com/s/article/2006985 の説明に従って VMware サポートにお問い合わせください。

Active Directory ドメイン登録の削除

状況によっては、お使いの Horizon Cloud 顧客アカウントから Active Directory ドメインの関連付けを削除する必要性が生じる場合や、削除したくなる可能性があります。管理コンソールでは、このアクションに [削除] というラベルが付けられ、ユーザーは、これをテナント環境にバインドされている Active Directory ドメインのリセットであると認識することがあります。最初のポッドが Horizon Cloud 顧客アカウントとペアリングされた直後またはそのすぐ後に、Active Directory ドメインを登録します。登録プロセスが完了すると、そのドメインは全体的な Horizon Cloud 顧客アカウントのクラウド構成ドメインになります。同じ顧客アカウントを使用して Horizon Cloud からデプロイする、または Horizon Cloud に接続するすべてのポッドも、顧客アカウント レコードを介してその最初のクラウド構成の Active Directory ドメインに関連付けられます。同じ顧客アカウント レコードを共有するすべてのポッドは、そのレコード内のクラウド構成ドメインに接続されている必要があります。

テナントにバインドされているドメインを削除する（またはリセットする）ことが望ましい状況の例は次のとおりです。

- 最初のポッドを Microsoft Azure にデプロイし、ドメイン バインドの手順を開始しました。すると何か問題が発生し、ドメイン登録が未完了な状態のままになってしまいました。このような状況では、Active Directory ドメインの情報の一部はクラウド内の顧客アカウント レコードに書き込まれます。しかし、情報が未完成のため、コンソールを使用してドメインの登録を完了する処理を続行できません。
- Microsoft Azure のポッドをデプロイし、テストの Active Directory ドメインを登録し、多くのワークフローを実行することにより、事前検証 (POC) を実行します。その後、新たに開始するためにそのポッドを削除し、本番環境のドメインで、本番環境のポッドを作成します。しかし、最初のテストの Active Directory ドメインがまだ顧客アカウントのクラウド構成ドメインのままであるため、システムはこのテストの Active Directory ドメインを、新しいポッドに関連付けることを想定します。
- 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前に、この Horizon Cloud 顧客レコードを使用して Horizon Cloud Connector のオンボーディング ワークフローを複数の Horizon ポッドに対して実行します。Horizon Cloud Connector のオンボーディング ワークフローは、Horizon ポッドの Connection Server によって認識される Active Directory ドメインの Horizon Cloud に部分的な構成を作成します。部分的な構成は、コンソールで最初の Active Directory ドメイン登録ワークフローを実行すると完了します。このリリースの既知の問題により、コンソールでドメイン登録ワークフ

ローを完了する前に複数の Horizon ポッドを Horizon Cloud に接続すると、登録ワークフローが失敗することがあります。この場合、コネクタの構成ポータルで [接続解除] アクションを使用してこれらのポッドの 1 つ以外のすべてのクラウド ペアリングを元に戻し、ドメインを登録する前に部分的な Active Directory ドメイン登録を削除する必要があります。

管理コンソールには、次の条件が真の場合、Active Directory ドメイン情報を削除するボタンが表示されます。

- [はじめに] ページには、1 つのポッドのみが環境内でデプロイまたはペアリングされていることが表示されるか、最初のポッドをすべて削除したため [キャパシティ] ページに表示されるポッドがないことが表示されます。

  重要： 最初のポッドをすべて削除し、True SSO 構成を使用していた場合、Active Directory ドメイン情報を削除するためのボタンは有効になっていません。最後のポッドを削除する前に、コンソールの [Active Directory] ページから True SSO の設定を削除して、システムが Active Directory 設定の [削除] ボタンを有効にするようにします。

- Microsoft Azure のポッドがある場合、そのポッドは以下のような項目は何も含みません。
  - インポートされた仮想マシン
  - そのポッドで公開された（シールドされた）イメージ
  - ファーム
  - VDI デスクトップ割り当て
  - [Active Directory] ページに表示される、True SSO の設定
  - [ID 管理] ページに表示される ID 管理設定
  - [Active Directory] ページに表示される複数の Active Directory ドメイン

ポッドの詳細ページは、ポッドにインポートされた仮想マシン、公開されたイメージ、ファーム、または VDI デスクトップ割り当てがあるかどうかを示します。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移動できます。

手順

- コンソールで以下の手順のいずれかを実行します。
  - 最初の Active Directory ドメイン登録ワークフローのドメイン バインドの手順またはドメイン参加の手順に失敗して完了しなかったためドメインをリセットする場合、[はじめに] ページの [全般的なセットアップ] セクションを展開します。[Active Directory] の行で、[削除] をクリックします。
  - あるいは、[設定] メニューが表示されている場合は、[設定] - [Active Directory] を使用して、Active Directory ページに移動できます。[削除] をクリックします。

結果

システムによりログアウトされ、最初のログイン画面が表示されます。

次のステップ

Horizon Universal Console にログインして Horizon Cloud 環境で管理タスクを実行する の説明に従って、再びログインします。

第 1 世代のテナント - 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

2

Cloud Monitoring Service (CMS) は、第 1 世代の Horizon Cloud で提供される中心的なサービスの 1 つです。このサービスを使用すると、個々のポッドおよびエージェントを実行している仮想マシンが存在するデプロイ環境に関係なく、クラウド接続されたポッドの個別および全体のキャパシティ、使用率、および健全性を監視できます。

このページを読む前に

このページを読む前に、以下の点を考慮してください。

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。

注： 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、廃止された機能に以前関連していたこのページの情報は、適宜更新されています。

注： このドキュメント ページは、「VMware ナレッジベースの記事 KB91183」で説明されているように、第 1 世代のコンソールへの変更に合わせて更新されています。

簡単な紹介

Cloud Monitoring Service は、テナントのフリート内のポッドおよびエージェントを実行している仮想マシンからキャパシティ、健全性、および使用率に関連するデータを取得します。

リアルタイム データは、Horizon Universal Console 内で使用可能になります。(「VMware ナレッジベースの記事 KB91183」で説明されているように) 履歴データとトレンド データは、Workspace ONE Intelligence コンソール内で使用できます。

サービスはデータをさまざまな [ダッシュボード] ページのタブにフィードして、全体的な健全性を確認し、さまざまなレベルで健全性メトリックとキャパシティ メトリックをドリルダウンするのに役立ちます。

このサービスは、個々のエンド ユーザーをサポートするためのヘルプ デスク操作を実行するユーザー カードのデータも提供します。

サービスの監視機能 - 要件

注： 「VMware ナレッジベースの記事 KB91183」で説明されているように、履歴ダッシュボードとレポートを使用するには、Workspace ONE Intelligence を使用して第 1 世代テナントを構成する必要があります。Workspace ONE Intelligence ドキュメントの「Horizon and DEEM for Horizon」、「Horizon Cloud First-Gen Integration」、「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。

監視サービスの機能を使用するには、第 1 世代のテナント環境に少なくとも次が必要です。

1 1 つのクラウド接続されたポッド。

2 ポッドが通信路を確立している 1 つ以上の Active Directory ドメインに対して Active Directory ドメイン登録が完了していること。

3 その Active Directory ドメイン内の 1 つ以上のグループにスーパー管理者ロールが割り当てられていること。

4 第 1 世代テナント環境で有効になっている Cloud Monitoring Service (CMS) スイッチ。コンソールの [全般設定] ページにスイッチが表示されます。同じスイッチが、同じテナント環境内のすべてのクラウド接続ポッドの監視サービスの使用を制御します。コンソールで、[設定] - [全般設定] - [監視] の順に移動します。

   ネイティブの Amazon EC2 デプロイで Horizon Cloud Connector を使用して Horizon ポッドがクラウドに接続されている場合、アプライアンスで Connection Server 監視サービス (CSMS) を手動で有効にした場合にのみ、そのポッドに対し監視サービスが有効になります。詳細については、ネイティブの Amazon EC2 の Horizon Cloud Connector のサービスを手動で有効にするを参照してください。

制御プレーンにオンボーディングできるポッド タイプについては、Horizon Cloud - サービスの概要を参照してください。

Horizon 展開 - 要件

これらのデプロイ タイプでの監視サービスの使用には、次の要件があります。

- デプロイは Horizon 7 7.13 以降を実行している必要があります。
- ポッドの JMS メッセージ セキュリティ モードは [拡張] に設定されている。モードが [拡張] に設定されていない場合、サービスの監視機能は動作しません。

  ポッドの管理者コンソールを使用して、セキュリティ モードの設定を確認します。必要に応じて、VMware Horizon 7 ドキュメントの『Horizon 7 のアップグレード』にある「JMS メッセージ セキュリティ モードを拡張済みに変更する」トピックの説明に従って、セキュリティ モードを [拡張] に変更します。

- Horizon 展開（ポッドとデスクトップ）は、Horizon リファレンス アーキテクチャでサポートされている Horizon ポッド デプロイ アーキテクチャのいずれかに従って実行する必要があります。VMware Tech Zone の VMware Workspace ONE および VMware Horizon リファレンス アーキテクチャ サイトの Horizon リファレンス アーキテクチャを参照してください。

デスクトップ データを vRealize Operations for Horizon に送信しているクラウド接続された Horizon ポッドがある場合、[全般設定] で CMS トグルを有効にすると、データは代わりに Cloud Monitoring Service に送信されます。vRealize Operations for Horizon を使用して引き続きデスクトップ セッション データを収集するには、[設定] - [全般設定] - [監視] で CMS トグルを無効にします。または、CMS が有効になっている Management Pack for Horizon for vRealize Operations Manager を使用することもできます。

第 1 世代 Horizon Cloud on Microsoft Azure のデプロイ - 要件

これらのデプロイでは、ユーザー カード、および Workspace ONE Intelligence コンソールと Horizon Universal Console の関連する場所での監視データの可用性は、Horizon Universal Console の [全般設定] で CMS トグルをオンにしているかどうか、および Horizon Agents Installer (HAI) を使用してデプロイのデスクトップにエージェント ソフトウェアをインストールするときに選択したオプションによって異なります。

- Workspace ONE Intelligence の履歴セッション データを収集するには、トグルを有効にして、HAI に Horizon Monitoring Service Agent をインストールする必要があります。
- ライブ セッション データを表示するには、HAI にヘルプ デスク プラグインもインストールする必要があります。

注： RDP プロトコルは、Horizon Cloud でサポートされている他のプロトコルと比較して、限定的なメトリックのセットを提供します。Horizon Monitoring Service Agent は、RDP プロトコルによって提供されるそれらのメトリックのデータを返します。

履歴セッション データについて

注： 「VMware ナレッジベースの記事 KB91183」で説明されているように、履歴データは、Workspace ONE Intelligence コンソールの Workspace ONE Intelligence を介して使用できます。第 1 世代テナントのデータに対する Workspace ONE Intelligence コンソールの使用に関するドキュメントについては、Workspace ONE Intelligence ドキュメントの「Horizon and DEEM for Horizon」、「Horizon Cloud First-Gen Integration」、「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。

履歴セッション データは、次のようなデータを指します。

- 過去 7 日間のログオフ セッションのセッション情報。
- 過去 15 分間のアクティブ、アイドル、および切断されたセッションのパフォーマンス トレンド データ（CPU、メモリ、遅延、ディスク トレンド）。

ライブ セッション データが収集されないように第 1 世代テナントの設定が構成されている場合、仮想マシン関連の情報とログイン時間の内訳のデータが収集されますが、次のデータは収集されないため、表示できません。

- クライアント情報。
- ユーザー エクスペリエンス情報。

- リアルタイムのパフォーマンス トレンド。
- プロセス/アプリケーション情報。

第 1 世代の Horizon Universal Console でセッション データ オプションを設定するには、[設定] - [全般設定] - [監視] の順に移動し、[セッション データ] の設定を変更します。

詳しい情報

サービスが提供する統合された可視性、健全性監視、およびヘルプ デスク機能については、次のトピックとそのサブトピック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 世代のテナント - 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 インフラストラクチャの監視 と Horizon Cloud 環境のポッド
- Horizon Cloud 環境内のヘルプ デスク機能

第 1 世代のテナント - 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 Universal Console は、クラウド接続されたポッド全体の健全性を視覚的に把握し、第 1 世代の Horizon Cloud テナント環境のすべてのポッドのリアルタイム メトリックと健全性情報にアクセスするためのワンストップの場所として、[ダッシュボード] ページを提供します。データは、Horizon Cloud の中心的なサービスの 1 つである Cloud Monitoring Service (CMS) によって提供されます。[ダッシュボード] ページは、コンソールの [監視] アイコンからアクセスできます。

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。

このページを読む前に

このページを読む前に、以下の点を考慮してください。

注： 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、廃止された機能に以前関連していたこのページの情報は、適宜更新されています。

この機能が廃止されたため、コンソールのダッシュボードに [インフラストラクチャ] タブが表示されなくなります。

注： 2023 年 6 月 30 日時点で、このドキュメント ページは、VMware ナレッジベースの記事 KB91183 で説明されているように第 1 世代のコンソールへの変更に合わせて更新されています。

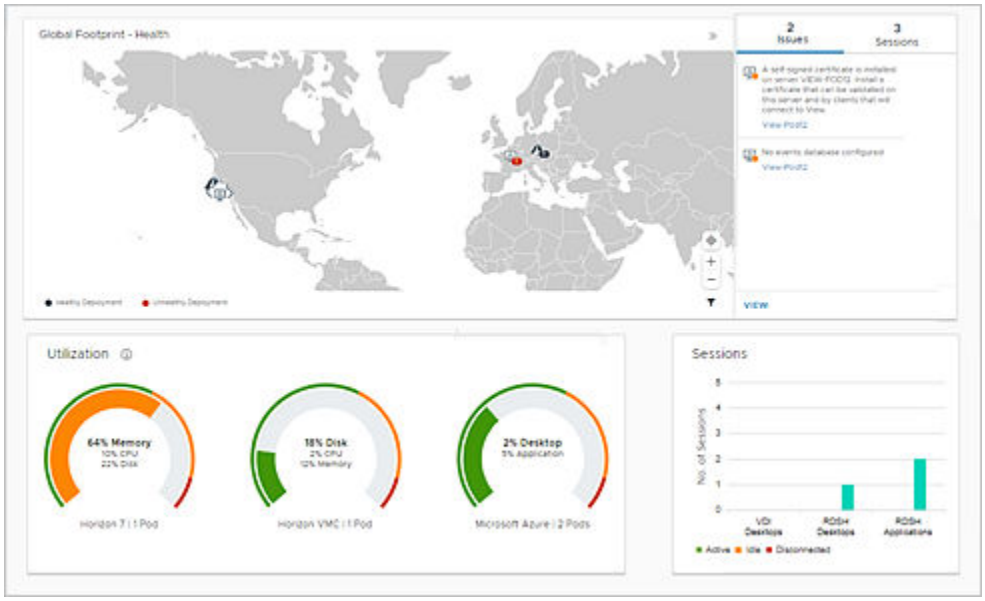
- これらの変更により、第 1 世代コンソールのダッシュボード ユーザー インターフェイスが更新され、ダッシュボードの [概要] タブの [使用率] 領域と [セッション] 領域でのみリアルタイム データにアクセスできるようになります。
- 第 1 世代テナントでユーザー セッション データの監視が無効になっている場合、使用率、傾向、および履歴の分析に関連するレポートは無効になり、Workspace ONE Intelligence では使用できなくなります。監視が無効になっている場合、システムはリアル タイムの管理を可能にするためにそのようなユーザー セッション情報を限られた期間で収集し、ユ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す。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、Workspace ONE Intelligence ドキュメントの「Horizon and DEEM for Horizon」、「Horizon Cloud First-Gen Integration」、「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。

[ダッシュボード] - [概要]

[ダッシュボード] ページの [概要] タブを使用して、クラウド接続されたポッド全体で何が起きているかについてのスナップショット健全性ビューを取得し、必要に応じてドリルダウンして詳細を表示します。Horizon Cloud の中心的なサービスの 1 つである Cloud Monitoring Service は、[概要] タブに表示されるデータを提供します。CMS は、第 1 世代の Horizon Cloud 環境のすべてのクラウド接続されたポッドからこのデータを取得し、ユーザーが使用できるように提示します。

次のスクリーンショットは、4 つのクラウド接続ポッドを持つ [概要] タブを示しています。スクリーンショットには、Microsoft Azure キャパシティを使用する 2 つのポッド、オンプレミスの 1 つの Horizon ポッド、および VMware Cloud on AWS キャパシティを使用する 1 つの Horizon ポッドがあります。オンプレミスの Horizon ポッドはパリにあり、2 つの問題を報告しています。



システムは数分ごとに情報を更新します。手動でページを更新することもできます。

重要： Microsoft Azure にデプロイされたポッドについては、ポッドをデプロイしてから、またはユーザー セッション情報の監視を有効にしてから 1 時間が経過するまで、表示される情報にはユーザー関連のデータは反映されません。

グローバルな占有量

[ダッシュボード] ページの上部には、インタラクティブなグローバル フットプリントが含まれています。このフットプリント マップにはポッドの地理的な場所が視覚的に示され、場所にカーソルを置くと追加情報が表示されます。マップは、さまざまなスケールでマップを表示するためのパンやズームイン、ズームアウトなど、一般的な業界標準のマップ対話機能をサポートしています。ズームインによって詳細を表示すると、同じ場所で一緒にクラスタリングされたポッドを確認するのに役立ちます。最初にマップを表示すると、ズームのデフォルトのスケールにより、ポッド フリートが 1 つのビューに表示されます。

環境に異なるタイプのポッドがある場合は、マップ エリアの右下にあるフィルタ機能を使用して、特定のタイプのポッドの表示と非表示を切り替えることができます。

重要： システムは、次のいずれかの方法を使用して、ポッドに関連付けられている場所情報を使用します。

- ポッドをデプロイして Horizon Cloud に接続するプロセスで、市区町村名を指定する。
- すべてのポッドについて、ポッドの詳細でポッドに関連付けられた場所に指定された都市名に従う。すでにオンボーディングされているポッドに場所を関連付けるには、Horizon Cloud - [キャパシティ] ページの編集ワークフローを使用した、クラウド接続されたポッドのクラウドに関連するいくつかの特性の変更を参照してください。

システムは、その市区町村の参照テーブルを使用して、指定した市区町村に関連付けられた緯度と経度の座標を取得し、ポッドをマップ上のそれらの座標に配置します。

マップの右側にある問題またはセッションに関連するタブのいずれかを選択して、フットプリント マップの特定のビューを選択します。選択したビューに基づいて、マップのポッド アイコンは、健全性（問題）に関連するデータまたはセッションに関連するデータを示します。ポッド アイコンにカーソルを合わせると、コンソールに関連する追加の詳細が表示されます。

問題関連

このビューが選択されている場合（デフォルト）、フットプリント マップは各ポッドの健全性を示します。メインのビジュアル アイコンはそれぞれ、その地理的な場所にあるポッドのセットとポッドの合計数を表します。アイコンの上にマウスを移動すると、その場所のポッドのリストが表示され、ポッドのタイプを示すアイコンと、緑色のドット（ポッドのデプロイが健全）または赤色のドット（ポッドのデプロイが不良）が表示されます。そのポッド リストの [表示] リンクをクリックすると、その場所のポッドについて報告された問題の詳細情報を表示するページが開きます。

マップの右側の領域では、最上部に現在の問題の合計数、その下に上位 5 つの問題が一覧表示されます。この領域の問題にカーソルを置くと、問題が発生している場所のマップにポッド情報のポップアップが表示されます。Horizon ポッドでは、ポッドがオンラインの場合、「制御プレーン サービスとしての Horizon Console の起動」で説明するように、ポッド名はそのポッドの Horizon Connection Server の Horizon Console を起動するためにクリックできるリンクです。ポッドがオフラインの場合、ポッドが再びアクセス可能になるまで、その Horizon Console を起動するためのリンクは使用できません。

問題リストの下部にある [表示] リンクをクリックすると、詳細なデータを表示するページが開きます。このページには、さまざまなタブと、さまざまな並べ替えとフィルタリングのオプションがあります。

- [問題の総数] タブには、すべての問題の一覧と問題ごとの詳細（問題のあるポッドやポッド タイプなど）が表示されます。Horizon ポッドの場合、制御プレーン サービスとしての Horizon Console の起動で説明するように、ポッド名はそのポッドの Horizon Connection Server の Horizon Console を起動するためにクリックできるリンクです。
- [配信] タブには、Connection Server など、ポッド自身のコンポーネントに関連する問題の一覧が表示されます。

セッション関連（VDI と RDSH セッション）

このビューを選択すると、フットプリント マップに各ポッドのセッション関連データが表示されます。メインのビジュアル アイコンはそれぞれ、その地理的な場所にあるポッドのセットとそれらのポッドのセッション合計数を表します。この合計には、接続済み、アクティブ状態、およびアイドル状態のセッションが含まれます。アイコンの上にマウスを移動すると、ポッドのリストがポッドのタイプを示すアイコンとともに表示され、セッション データが表示されます。ポップアップには、セッション タイプ別の現在のセッションの円グラフと、その場所にあるポッドのセッション数の詳細が表示されます。ポッド リストの下にある [表示] リンクをクリックすると、その場所のセッション関連データの詳細を表示するページが開きます。このページには各セッション タイプのチャートが含まれ、ステータス別のセッションと、各セッションの詳細情報を含むセッション リストが表示されます。表示されるセッションのリストは、場所とポッドでフィルタリングできます。情報の各列では、ソート機能とフィルタ機能も使用できます。

マップの右側の領域には、ポッドのエンドユーザー セッションの合計数が表示されます。この合計には、接続済み、アクティブ状態、およびアイドル状態のセッションが含まれます。次に、各ポッドのセッション数とともにポッドが一覧表示されます。リスト内のポッドにマウスを移動すると、ポッドが配置されている場所のマップ上で情報ポップアップが開きます。Horizon ポッドの場合、制御プレーン サービスとしての Horizon Console

の起動で説明するように、ポッド名はそのポッドの Horizon Connection Server の Horizon Console を起動するためにクリックできるリンクです。ポッド リストの下部にある [表示] リンクをクリックすると、詳細なデータを表示するページが開きます。このページには、さまざまな並べ替えとフィルタリングのオプションがあり、選択した並べ替えとフィルタリングのオプションに基づいてセッション関連のデータを示すチャートが含まれています。

[ダッシュボード] - [使用率] 領域

ダッシュボードのメイン概要の [使用率] 領域には、ポッド フリートのリソースのリアルタイム使用率のシステム計算をポッド タイプ別に集計したインタラクティブなグラフが表示されます。これらのグラフに示されているシステムの計算と使用率データの意味は、ポッドのタイプによって異なります。各グラフをクリックして詳細を表示できます。

Microsoft Azure の Horizon Cloud ポッド - ポッド マネージャ ベースのポッド タイプ

このポッド タイプのポッドの場合、[使用率] グラフには、それらのポッドによって割り当てられたキャパシティと、割り当てられたデスクトップおよび RDS ベースのリモート アプリケーションの使用率が表示されます。このデータは、管理者を対象としており、エンド ユーザーが資格のあるデスクトップとアプリケーションを使用するために十分なデスクトップが割り当てられているかどうかを理解するのに役立ちます。チャートのデータでは、全体的なキャパシティの割合が 1 時間に 1 回更新されます。デスクトップおよびアプリケーション セッションのキャパシティの割合は、1 時間ごとに更新されます。

デフォルトでは、チャート化されたデータは、過去 24 時間以内のこのポッド タイプのフリートのポッドの平均データです(時間単位)。

システムが定義する使用率は、アクティブなセッション数を、可能な最大セッション数で除算したものになります (`ActiveSessions / MaxPossibleSessions`)。

VMware SDDC にデプロイされた Horizon ポッド - Connection Server のポッド タイプ

このポッド タイプのポッドの場合、使用率グラフには、CPU、メモリ、およびディスク ストレージの平均使用量の最大値が表示されます。

デフォルトでは、チャートデータは、これらの 24 時間以内に対応するポッド タイプのフリートのポッドで分単位で平均化されたデータです。

ダッシュボード - セッション領域

ダッシュボードのメイン概要の [セッション] 領域には、ポッドのすべての VDI デスクトップ、RDSH デスクトップ、RDSH アプリケーションのアクティブ セッションとアイドル セッションの内訳が表示されます。

[ダッシュボード] - [接続統計情報] 領域

この領域には、すべてのポッドへのエンド ユーザー接続によって使用されているプロトコル、Horizon Client のタイプ、ネットワーク アクセスの形式の内訳が表示されます。

[Horizon Client] チャートには、その他 というラベルのタイプが含まれています。以下の場合、システムは接続にその他 というラベルを付けます。

- 接続でクライアント タイプを報告できない古いバージョンの Horizon Agent が使用されている。

- クラウド接続された Horizon 7 バージョン 7.7 ポッドのデスクトップとアプリケーションにアクセスするために、接続で VMware 認定のシン クライアントまたはゼロ クライアントが使用されている。

Horizon インフラストラクチャの監視 と Horizon Cloud 環境のポッド

Horizon インフラストラクチャの監視 機能が廃止される前に、このページでは機能を有効にするためのシステム要件と手順について説明しました。

注： 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、廃止された機能に以前関連していたこのページの情報は、適宜更新されています。

このページでは機能を有効にする方法について説明し、2023 年 9 月の時点で機能を有効にすることはできなくなりましたので、このページの内容は削除されました。

Horizon Cloud 環境内のヘルプ デスク機能

管理コンソールは、エンド ユーザーの仮想デスクトップおよびアプリケーションの使用状況を監視したり、問題をトラブルシューティングするための 1 つのペインとして使用されます。ヘルプ デスク管理者のコンソールへの役割ベースのアクセスを構成した後、管理者はコンソールにログインし、検索機能を使用してユーザーを調べることができます。特定のユーザーについては、問題のトラブルシューティングを行ったり、特定のデスクトップ メンテナンス操作をいくつか実行したりするために、ヘルプ デスク管理者がそのユーザーのセッションを調べることができます。

自分の組織内で、その環境によって提供される仮想デスクトップやリモート アプリケーションをエンド ユーザーが使用しているときに生じる可能性があるあらゆる問題を対処してエンド ユーザーを支援する役割の人を配置していることが考えられます。また、潜在的にセッションに影響する可能性がある問題を特定するために、エンド ユーザーのセッションの監視や、デスクトップ インスタンスおよびファームの RDSH インスタンスの監視を行う人も配置している場合があります。

コンソールでは、次の項目が、これらのヘルプ デスク関連のタスクの実行をサポートします。

- ヘルプ デスク ワーカーの VMware Customer Connect アカウントに、適切なヘルプ デスク関連のロールとともに、コンソールへのアクセスを提供します。Horizon Cloud テナント環境への認証についてはこれらのアカウントの認証情報を使用します。VMware Customer Connect アカウントでは、Horizon Cloud は [カスタマー ヘルプデスク] と [カスタマー ヘルプデスク (読み取り専用)] という 2 つの事前定義のヘルプ デスク関連のロールを提供します。コンソールの [全般設定] ページまたは [はじめに] ページを使用して、ヘルプ デスク ワーカーの VMware Customer Connect アカウントを追加します。手順については、Horizon Cloud テナント環境にログインし、Horizon Universal Console を使用してアクションを実行するための管理者ロールを組織内の個人に付与するを参照してください。VMware Customer Connect は、My VMware を置き換える名前であり、コンソールのユーザー インターフェイスに以前の名前が引き続き反映される場合があります。
- ヘルプ デスク担当者の Active Directory アカウントに適切な Horizon Cloud ヘルプ デスク関連の役割を付与します。Horizon Cloud テナント環境への認証についてには、Active Directory アカウントの認証情報も含まれています。Active Directory アカウントでは、Horizon Cloud は [ヘルプ デスク管理者] と [ヘルプ

デスク読み取り専用管理者] という 2 つの事前定義のヘルプ デスク関連の役割を提供します。手順については、Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるを参照してください。

注： Active Directory グループ レベルでは、Horizon Cloud の役割が割り当てられます。ヘルプ デスク ワーカーの Active Directory アカウントは Active Directory グループ内にあり、役割が付与される必要があります。

- コンソールの検索機能。ヘルプ デスク ワーカーは、この機能を使用して特定のエンド ユーザーまたは仮想マシン（デスクトップ インスタンスまたはファームの RDSH インスタンス）を検索することができます。
- ユーザー カードの機能。特定のユーザーのユーザー カードを使用することにより、ヘルプ デスク ワーカーはそのユーザーのセッションを調べて問題のトラブルシューティングを行ったり、特定のデスクトップ メンテナンス操作をいくつか実行したりすることができます。ヘルプ デスク ワーカーが利用できる操作は、その人の Active Directory アカウントに割り当てられたヘルプ デスク関連の役割によって異なります。

コンソールの検索機能の使用

管理コンソールの検索機能を使用して、環境内の特定のユーザーまたは仮想マシン (VM) を名前で検索します。

注： このリリースでは、検索機能の範囲には、VMware SDDC の Horizon ポッドからのクラウド仲介された RDSH 割り当ては含まれていません。さらに、仮想マシンの検索は Microsoft Azure のポッドにある仮想マシンにのみ適用されます。

ユーザーまたは仮想マシンのいずれかで検索を実行できます。ユーザーまたは仮想マシンの検索を選択したら、検索テキスト ボックスに検索語を入力します。[検索] テキスト ボックスに少なくとも 3 文字を入力すると、それらの文字で始まる名前が表示されます。さらに文字を入力すると、検索の結果を絞り込むことができます。

注： 仮想マシンの検索では、ファーム内の RDS サーバ仮想マシンおよび Horizon Cloud テナント環境にプロビジョニングされた VDI デスクトップ仮想マシンを検索できます。

検索しているユーザーまたは仮想マシンが表示されたら、それらをクリックして詳細を取得できます。表示される画面は、ユーザーまたは仮想マシンのどちらをクリックしたかによって異なります。

- ユーザーの場合は、そのユーザーのカードが表示されます。詳細については、第 1 世代テナント - ユーザー カード機能（別称：Horizon Cloud のヘルプ デスク）についてを参照してください。

- 仮想マシンの場合は、システムはその仮想マシンを見つけるための画面を表示します。たとえば、リストされた仮想マシンをクリックし、その仮想マシンがファーム内の RDS ホストである場合、システムはそのファームの詳細ページの [ホスト] タブを表示します。

第 1 世代テナント - ユーザー カード機能（別称：Horizon Cloud のヘルプ デスク）について

コンソールのユーザー カード機能をダッシュボードとして使用し、特定のユーザーの割り当て済みリソース（そのユーザーのデスクトップなど）を処理します。このユーザー カード機能は、ヘルプ デスクとも呼ばれます。

注目: このページは、VMware ナレッジベースの記事 KB91183 で説明されているように、第 1 世代のコンソールへの変更に合わせて更新されています。

ナレッジベースの記事で説明されているように、VMware Workspace ONE Intelligence for Horizon は、VMware Horizon Universal、Horizon Apps Universal、および Horizon Apps Standard のサブスクリプション ライセンスを持つ第 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。

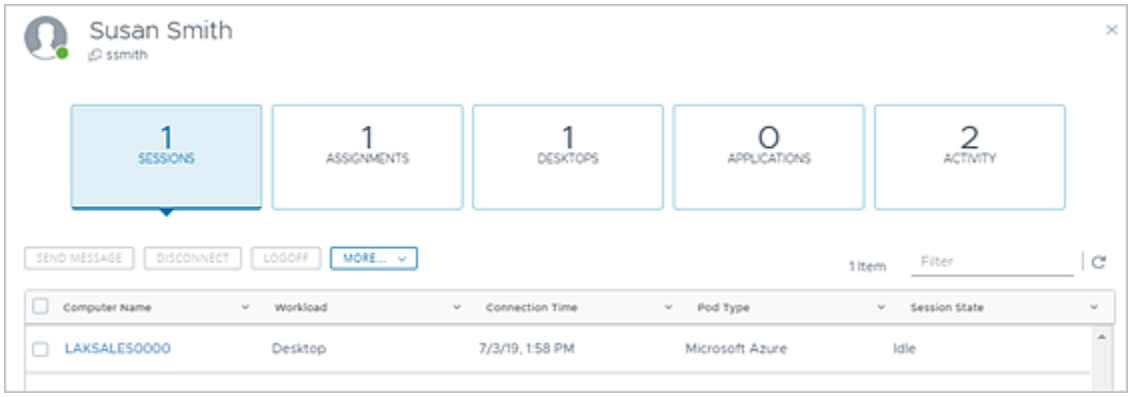
- 第 1 世代コンソールが提供していた履歴ダッシュボードとレポートは、Workspace ONE Intelligence を通じて利用できるようになります。
- 2023 年 6 月 30 日時点で、これらの履歴ダッシュボードとレポートは第 1 世代コンソールでは使用できなくなりました。
- これらの変更により、以前は Horizon Cloud on Microsoft Azure ポッドからのセッションの第 1 世代のユーザー カード ユーザー インターフェイスに表示されていた履歴パフォーマンス データは、Workspace ONE Intelligence でのみ使用できるようになりました。

詳細については、「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。

概要

重要： Horizon ポッドでこの機能を使用するには、Connection Server インスタンスをインストールした後に、ポッドの Connection Server のイベント データベースを構成する必要があります。イベント データベースには、Horizon ポッド関連のイベントに関する情報が、ログ ファイルではなくデータベースのレコードとして格納されます。イベント レポート用のイベント データベースの構成については、Horizon 製品のインストール ガイドを参照してください。

特定のユーザーのカードを表示するには、コンソールの検索機能を使用します。ユーザーの検索方法については、コンソールの検索機能の使用を参照してください。検索結果でユーザーをクリックすると、そのユーザーのカードが表示されます。



ユーザー カード内を移動して画面上のプロンプトに従うことで、この特定のユーザーのコンテキスト、このユーザーの仮想デスクトップおよびアプリケーションに関する情報データを確認できます。さまざまなタイプの情報とデータを表示するには、異なる情報領域をクリックして切り替える必要がある場合があります。

注： このリリースでは、ユーザー カードの一部の領域は、Microsoft Azure にデプロイされたポッドによってプロビジョニングされたアイテムにのみ適用可能です。Microsoft Azure にポッドがない場合、それらの領域には、Microsoft Azure にポッドをデプロイした場合にのみそのページが使用可能であることを示すグラフィックとメッセージが表示されます。表示されるグラフィックの例については、第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアーを参照してください。

セッション

ユーザー カード内を移動して、すべてのクラウド接続ポッドから集計された、ユーザーの現在のセッションに関するリアルタイムの情報を取得します。表示されているセッションに対して実行できるアクションを示します。これらのアクションの詳細については、セッションで実行できるアクションを参照してください。

注： 現在のセッションが存在しない場合、[セッション] タブには最上段に 0 の値が表示されます。

セッションをクリックしてダッシュボードを開きます。セッションのダッシュボードから、トラブルシューティングのためにユーザー セッションを監視できます。セッションのダッシュボードの操作を参照してください。

割り当て

ユーザー カード内を移動して、ユーザーが参加する割り当てに関する情報を取得します。Horizon Cloud での割り当ては、ユーザーが仮想デスクトップまたはアプリケーションの使用資格を付与されるエンティティになります。

注： URL リダイレクトのカスタマイズ割り当ては、ユーザー カードには表示されません。

デスクトップ

ユーザー カード内を移動して、ユーザーの割り当てられた仮想デスクトップに関する、次のような情報を取得します。

- VDI フローティング デスクトップへのアクティブなセッション
- RDSH セッション デスクトップへのアクティブなセッション

- ユーザーに割り当てられた VDI 専用デスクトップ（ユーザーにそのデスクトップへのアクティブなセッションがない場合も含む）。

システムは、次の 2 つの方法のいずれかにより VDI 専用デスクトップをユーザーに割り当てます。

- VDI 専用デスクトップ割り当てのページで [割り当て] アクションを使用して、特定の専用デスクトップをこの特定のユーザーに明示的に割り当てる。
- ユーザーが、自分に資格が付与された VDI 専用デスクトップ割り当てによって定義されたセットからデスクトップを要求する。特定の専用デスクトップをユーザーに明示的に割り当てることなく、VDI 専用デスクトップ割り当ての資格をそのユーザーに付与することができます。ユーザーに資格を付与するには、割り当ての [ユーザー/グループ] 領域を使用します。次に、資格が付与されたユーザーがその割り当て内のデスクトップのセットから初めてデスクトップを起動するときに、ユーザーはその VDI 専用デスクトップを要求し、システムはその VDI 専用デスクトップをユーザーに恒久的に割り当てます。

ユーザー カードは、デスクトップの基盤となる仮想マシン (VM) の操作を実行するためのアクション ボタンも提供します。これらのボタンを使用できるかどうかは、コンソールのロールベースのアクション コントロール (RBAC) から割り当てられたロールによります。

アプリケーション

ユーザー カード内を移動して、ユーザーの割り当てられたリモート アプリケーションに関する情報を取得します。

アクティビティ

ユーザー カード内を移動して、選択した期間におけるユーザー アクティビティに関する情報を取得します。

セッションで実行できるアクション

リストされているセッションに対して実行できるアクションは、セッションのタイプ、ポッドのタイプ、および管理者の権限によって異なります。ユーザー カード内を移動し、画面上のラベルに従って、ユーザー カード内で該当するアクションを見つけます。

アクション	説明	Horizon	Horizon	Microsoft Azure	Microsoft Azure
		VDI デスクトップ	セッションベースのデスクトップ	VDI デスクトップ	セッションベースのデスクトップ
通知メッセージの送信	特定のセッションのログイン ユーザーに固有の通知メッセージを送信することは、ユーザー カードで提供されるアクションの 1 つです。送信されたメッセージは、ユーザーの画面に表示されます。	はい	はい	はい	はい

アクション	説明	Horizon	Horizon	Microsoft Azure	Microsoft Azure
VMware Workspace ONE Assist for Horizon の使用	このアクションにより、選択したエンドユーザー デスクトップ セッションで VMware Workspace ONE Assist for Horizon 製品の機能を使用できるようになります。これらの機能を使用すると、管理者はリモート表示および制御機能を使用して、仮想デスクトップについて従業員を支援できます。アクション ボタンへのアクセスは、テナント環境に VMware Workspace ONE Assist for Horizon 製品を使用するライセンスが付与され、選択したデスクトップの基盤となる仮想マシンおよびその仮想マシンをプロビジョニングしているポッドで追加の最小要件が満たされている場合にのみ使用できます。これらの要件およびこの機能の使用に関する情報については、VMware Workspace ONE Assist ドキュメントにある『VMware Workspace ONE Assist for Horizon と Horizon Cloud』ガイドを参照してください。	はい	いいえ	はい	いいえ
Microsoft リモート アシスタントの使用	ヘルプ デスク ツールでは、このアクションには [リモート アシスタント] というラベルが付けられています。このアクションは、Horizon ポッドからのセッションで使用できます。このアクションでは、公開デスクトップで Microsoft リモート アシスタント機能を使用します。このアクションは、特定のエンドユーザー セッションで開始します。	はい	はい	いいえ	いいえ

アクション	説明	Horizon	Horizon	Microsoft Azure	Microsoft Azure
再起動	このアクションにより、エンドユーザー セッションの基盤となる仮想マシンが再起動されます。	はい	いいえ	はい	いいえ
切断	セッションを切断します。	はい	はい	はい	はい
ログオフ	ユーザーをセッションからログオフさせます。	はい	はい	はい	はい
リセット	エンドユーザー セッションの基盤となる仮想マシンをリセットします。	はい	いいえ	はい	いいえ

セッションのダッシュボードの操作

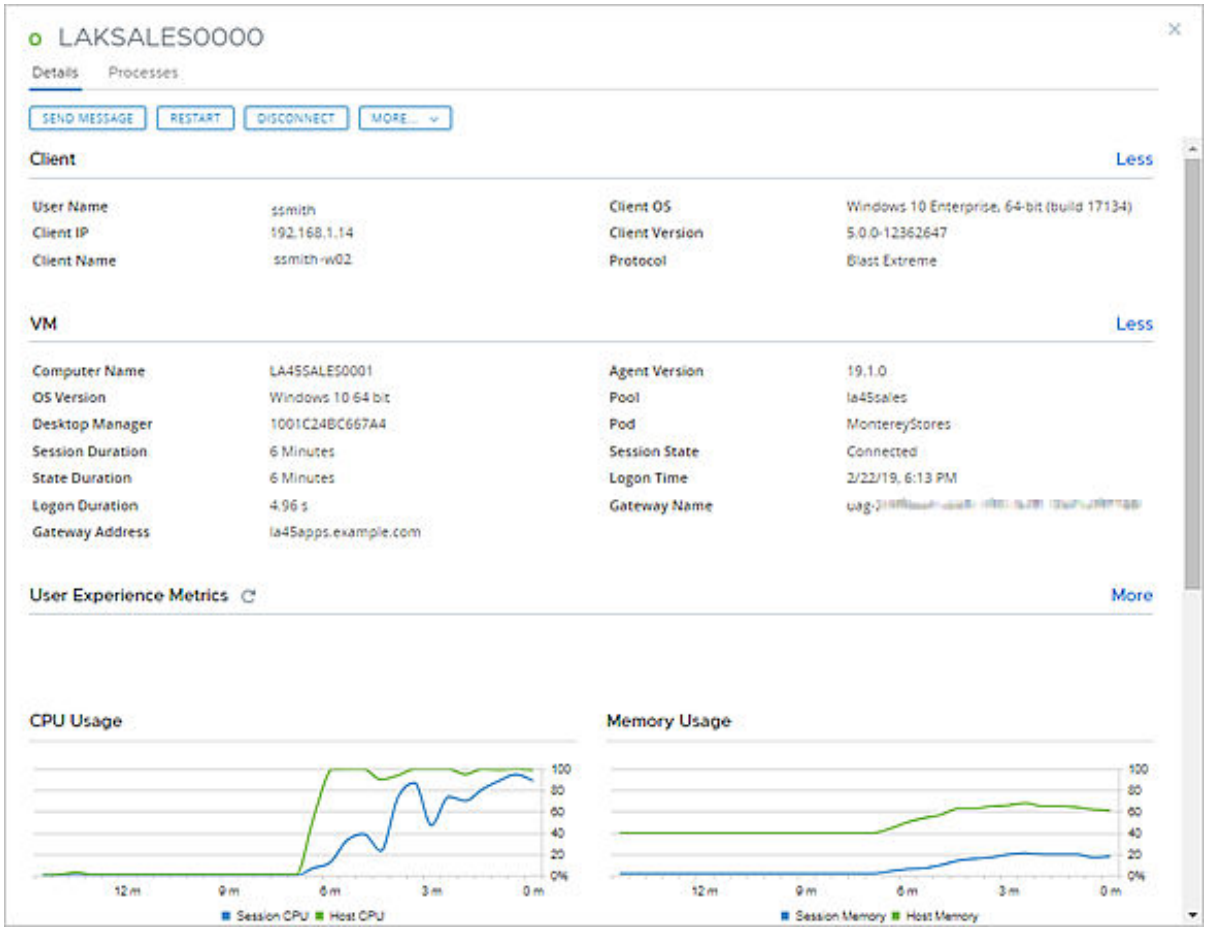
アクティブなセッションの 1 つをクリックすると、そのセッションに関するデータを確認できるダッシュボードが開きます。このダッシュボードの各領域を移動して、ダッシュボードが提供するデータを確認し、ダッシュボードで使用可能なアクションを実行します。

詳細

トラブルシューティングの目的でエンド ユーザーのセッションを監視するために、CPU 使用率、メモリ使用量、ネットワーク遅延、ディスク パフォーマンスなど、セッション関連の詳細情報を使用します。ダッシュボードをスクロールし、画面上のコントロールを使用して表示する詳細情報の量を調整します。

注： RDP プロトコルで使用可能なメトリックは限られています。アクティブなセッションが RDP プロトコルを使用している場合、他のサポートされているプロトコルに比べて、使用可能なメトリックは少なくなります。

次のスクリーンショットは、セッションのダッシュボードで使用可能ないくつかのデータ タイプとアクションの例を示します。


LAKSALES0000
Details
Processes
SEND MESSAGE
RESTART
DISCONNECT
MORE...
Client
Less
User Name
ssmith
Client IP
192.168.1.14
Client Name
ssmith-w02
Client OS
Windows 10 Enterprise, 64-bit (build 17134)
Client Version
5.0.0-12362647
Protocol
Blast Extreme
VM
Less
Computer Name
LA45SALES0001
OS Version
Windows 10 64 bit
Desktop Manager
1001C24BC667A4
Session Duration
6 Minutes
State Duration
6 Minutes
Logon Duration
4.96 s
Gateway Address
la45apps.example.com
Agent Version
19.1.0
Pool
la45sales
Pod
MontereyStores
Session State
Connected
Logon Time
2/22/19, 6:13 PM
Gateway Name
User Experience Metrics
More
CPU Usage
100
80
60
40
20
0%
12 m
9 m
6 m
3 m
0 m
Session CPU
Host CPU
Memory Usage
100
80
60
40
20
0%
12 m
9 m
6 m
3 m
0 m
Session Memory
Host Memory

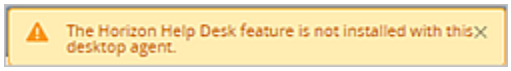
ダッシュボードは、セッションの問題をトラブルシューティングするためにスーパー管理者とヘルプ デスク管理者が使用できるパフォーマンス データのメトリックとアクションを提供します。

プロセス

ダッシュボードでは、セッションで実行中のプロセスおよびアプリケーションに関する情報にアクセスでき、問題のあるプロセスまたはアプリケーションを終了する操作を実行できます。

ヘルプ デスク機能がデスクトップまたはファーム仮想マシンにインストールされていない場合

VDI デスクトップ仮想マシンまたはファームの RDSH 仮想マシンが、ヘルプデスク機能がインストールされていないイメージに基づいている場合、その仮想マシンに接続されているセッションのダッシュボードを開くと、情報アラートが表示されます。



この場合、仮想マシンのデータは報告されません。通常のデータは使用できないため、このようなセッションでは、一部のダッシュボード領域が次のように空白または空で表示されます。

- クライアントおよび仮想マシンに関するほとんどのデータが使用できません。
- ユーザー エクスペリエンスのメトリックとグラフが空です。
- [プロセス] タブが空です。
- [更新] アイコンはクリックできません。
- [タスクの終了] ボタンなど、一部のアクション ボタンは表示されません。

第 1 世代テナント - 第 1 世代 Horizon Cloud がサポートするすべてのポッド タイプのクラウド接続ポッドの管理

3

第 1 世代 Horizon Cloud では、さまざまなタイプのポッドを使用でき、さまざまな環境にデプロイされたポッドをすべて単一のテナント環境に接続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。

クラウド接続されたポッドがクラウド プレーンにオンボーディングされている場合、それらは第 1 世代コンソールの [キャパシティ] ページにリストされます。[キャパシティ] ページは、クラウド接続されたポッドの全体を監視および管理できるワンストップの場所です。ここでポッドをテナント環境に追加したり、ポッドの特性を編集したり、ポッドを削除したりできます。[ポッド] タブを使用して、ポッドをエンティティ全体として操作する以外に、[キャパシティ] ページのその他のタブでは、サイト（クラウド接続されたポッドの定義済みコレクション）を構成し、ポッドのキャパシティ関連リソース（保存された認証情報など）の設定を構成できます。

[キャパシティ] ページの概要

[キャパシティ] ページは、コンソールの [設定] アイコンからアクセスできます。[キャパシティ] ページには複数のタブがあります。これらのタブについて考えられる役割の 1 つは、クラウド接続されたポッド、サイト、キャパシティ関連リソースに対する CRUD（一般的な作成、読み取り、更新、削除）操作へのアクセスを提供することです。

作成操作

[ポッド] タブには、ポッド フリートに新しいポッドを追加するワークフローを開始するための [新規] アクションが表示されます。[サイト] タブには、新しいサイトを定義するための [新規] アクションが表示されます。[リ

ソース] タブには、新しいウィンドウを開く [管理] アクションが表示されます。この新しいウィンドウから、新しい Microsoft Azure サブスクリプション情報を追加して Horizon Cloud に保存できます。

注： KB-92424 で示されているように、[新規] アクションは、第 1 世代の制御プレーンの提供終了 (EOA) からの承認された例外がある場合にのみ使用できます。

読み取り操作

[ポッド] タブは、特定のポッドの詳細をドリルダウンして調べるためのアクセス ポイントでもあります。リストされたポッドの名前を選択し、ポッドに関する詳細を表示するページを開きます。[リソース] タブで、リストされたリソースの名前を選択し、リソースに関する詳細を表示するページを開きます。[サイト] タブでは、[編集] ボタンを使用して、リストされているサイトの詳細を表示できます。

更新操作

[ポッド] タブは、ポッドの編集可能な特性を変更するための [編集] アクションを提供します。ポッドに対して編集できる特性は、ポッドのタイプ、ポッドの既存の特性、およびそのポッド タイプと特性に対してどのような変更がサポートされているかによって異なります。同様に、[サイト] タブには、サイトの編集可能な特性を変更するための [編集] アクションがあります。[リソース] タブの [管理] アクションは、リソースの編集可能な特性を変更するためのエントリ ポイントです。

削除操作

[ポッド] タブは、Horizon Cloud テナントのクラウド接続ポッドからポッドを削除するための [削除] アクションを提供します。[サイト] タブには、そのタブで定義されているサイトを削除するための [削除] アクションが表示されます。[リソース] タブの [管理] アクションは、Microsoft Azure サブスクリプションの保存された認証情報など、保存されたキャパシティ関連のリソースを削除するためのエントリ ポイントです。

ポッド： ポッドレベルの情報

[ポッド] タブは、Horizon Cloud テナント環境のクラウド接続されたポッド、そのステータス、およびそのリソースの使用率に関する処理状況についての概要を示します。また、ここから、新しいポッドのデプロイの開始、ポッドの特性の編集、またはテナント環境からのポッドの削除など、ポッドレベルの管理ワークフローを開始することもできます。ポッドのタイプごとに、[ポッド] タブに固有の情報が表示されます。

注意: ここで使用される用語：

- Horizon Cloud ポッドは、VMware Horizon Cloud on Microsoft Azure のポッド マネージャ テクノロジーに基づいて構築されました。
- Horizon ポッドは、VMware Horizon の Connection Server テクノロジーに基づいて構築されました。

表 3-1. [ポッド] タブのポッド別の情報列

列	詳細
ステータス	オンラインなど、ポッドの健全性ステータスを示すアイコン。表示される各種ステータスの意味については、ポッド： 健全性ステータスの表示を参照してください。
名前	ポッドの現在の名前が表示されます。

表 3-1. [ポッド] タブのポッド別の情報列 （続き）

列	詳細
タイプ	ポッドがポッド フリートでサポートされるタイプの 1 つであるかどうかに応じて、ポッドのタイプが表示されます。コンソールのこの列に表示される内容の例として、`On-Premises` と `VMware Cloud on AWS` があります。
バージョン	Horizon Cloud ポッドの場合、この列には基盤となるポッド マネージャ仮想マシンのマニフェスト情報からのソフトウェア バージョンが表示されます。この数字は、ポッド マネージャ仮想マシンが現在実行されているソフトウェア バイナリのバージョンを反映しています。 Horizon ポッドの場合、この列にはポッドを Horizon Cloud に接続している Horizon Cloud Connector のソフトウェア バージョンが表示されます。
状態	この列には、ポッドのデプロイの現在の状態が表示されます。状態の意味は、デプロイがポッド マネージャ テクノロジーまたは Connection Server テクノロジーのどちらに基づいて構築されているかによって異なります。これらのポッド タイプ間のソフトウェア テクノロジーの違いの簡単な説明については、サービスの概要を参照してください。 **ポッド マネージャ ベースのポッド** このタイプのポッドは、コンソールの自動化されたポッド デプロイ ウィザードを実行すると、Microsoft Azure サブスクリプションでインスタンス化されます。[キャパシティ] ページには、このタイプのポッドは常に `Managed` として表示されます。このようなポッドは常に Horizon Cloud 制御プレーンを使用して管理できるためです。コンソールを使用してポッドのすべての側面を管理できます。また、コンソールの 2 章 第 1 世代のテナント - 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 デスク機能の紹介も活用できます。 **Connection Server ベースのポッド** [キャパシティ] ページには、このタイプのポッドは `Monitored` または `Managed` として表示されます。監視対象状態は、これらのポッドを最初に Horizon Cloud にオンボーディングした後のデフォルト状態です。監視対象状態のポッドは、サブスクリプション ライセンス サービスに加えて、2 章 第 1 世代のテナント - 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 デスク機能の紹介を提供するそれらのコンソール機能にアクセスできます。 このタイプのポッドが特定の要件を満たしている場合は、そのポッドを管理対象状態に移行できます。管理対象状態のポッドは、監視対象状態のポッドのコンソール機能を使用できることに加えて、このポッド タイプでの使用がサポートされているすべての Horizon 制御プレーン サービスにアクセスできます。
場所	現在ポッドに関連付けられている地理的な場所を表示します。ポッドに関連付けられた場所を変更するには、[キャパシティ] ページの [編集] アクションを使用して、ポッドを別の場所に関連付けます。Horizon Cloud - [キャパシティ] ページの編集ワークフローを使用した、クラウド接続されたポッドのクラウドに関連するいくつかの特性の変更を参照してください。
サイト	Universal Broker を構成している場合、この列には、現在ポッドに関連付けられているサイトの名前が表示されます。Universal Broker のサイトの構成を参照してください。

表 3-1. [ポッド] タブのポッド別の情報列 （続き）

列	詳細
デスクトップとアプリケーションの使用率	テナント環境では、デスクトップとアプリケーションの使用率は、最大可能なセッション数に対するアクティブな使用中のエンドユーザー セッション数の割合という観点からのユーザー アクティビティの測定値です。 **注：** このリリースでは、Microsoft Azure のフリートにあるポッド マネージャ ベースの Horizon ポッドのデスクトップとアプリケーションの使用率のみが報告されます。 ポッド レベルでは、[デスクトップとアプリケーションの使用率] 列には、以下に従って計算された割合が表示されます。 1 ポッドに接続されているアクティブなデスクトップ セッションとリモート アプリケーション セッションをすべて合計します。 2 構成されたファームと VDI デスクトップ割り当てセッションの最大値に基づき、ポッドに構成されているすべての提供可能なデスクトップ セッションとリモート アプリケーション セッションを合計します。 3 1 番目の合計を 2 番目の合計で除算し、100 を掛けて使用率を算出します。 例として、ポッドには次のものが含まれるとします。 ■ 1 台の RDSH 仮想マシンと、仮想マシンあたり 10 個の同時セッション用に設定された 1 つのデスクトップ ファーム（そのファームからの 10 個の潜在的なセッション）。 ■ 2 台の RDSH 仮想マシンと、仮想マシンあたり 20 個の同時セッション用に設定された 1 つのアプリケーション ファーム（そのファームからの 40 個の潜在的なセッション）。 ■ アプリケーション ファームからリモート アプリケーションへの 1 つのアクティブなエンド ユーザー接続 潜在的なセッションの数が 50（デスクトップ ファームから 10、アプリケーション ファームから 40）で、アクティブなセッションの数が 1 であるため、1 / 50 = 2% となり、[デスクトップとアプリケーションの使用率] 列に表示されるポッドの割合は 2% になります。
使用済み容量	テナント環境では、キャパシティの使用率とは、ポッドがデプロイされる基盤となるキャパシティ インフラストラクチャ内でのポッドの使用に利用できる潜在的なキャパシティの合計のうち、使用中のポッドの仮想 CPU リソース (vCPU) が占める割合を示す測定値を意味します。 **注：** このリリースでは、フリートにあるポッド マネージャ ベースのポッドに対してのみキャパシティの使用率が報告されます。このようなポッドのキャパシティ使用率は、サブスクリプション全体のリージョンあたりの合計 vCPU 割り当てに基づいています。同じサブスクリプション内のすべてのポッドは、同じキャパシティの使用率を報告します。 たとえば、このようなポッドの場合、vCPU のキャパシティ使用率は、Microsoft Azure サブスクリプションの Microsoft.Compute で確認できるリージョンあたりの合計 vCPU 割り当ての値になります。インポートされた仮想マシン、シールドされたイメージ、ファーム RDSH インスタンス、および VDI デスクトップ インスタンスに使用される vCPU に加え、このようなポッドはそれぞれ、サブスクリプションのリージョンあたりの合計 vCPU 割り当てのうち、そのマネージャ仮想マシンに 4 つの vCPU、それぞれの Unified Access Gateway 仮想マシンに 4 つの vCPU を使用します。
エージェントのバージョン	v2204 リリースとそのリリースの Horizon Cloud ポッド マニフェスト以降、この列にはポッドのマニフェストに一致するエージェントのバージョンが表示されます。以前のマニフェストの場合、ポッドが v2204 リリースのマニフェスト以降に更新されるまで、この列は空になることがあります。 1 つ以上のポッドで、現在のポッド マニフェストで配布されている基本バージョンとは異なるバージョンのエージェントが実行されている場合、バージョン番号の右側に青いドットが表示されます。ドットをクリックして詳細を表示します。また、エージェントのアップデートがリリースされたときに通知が生成されます。

ポッド： 使用可能なポッドレベルのアクション

[キャパシティ] ページから実行できるポッドレベルの管理アクションの詳細は、アクションに関与するポッドのタイプ（Horizon Cloud ポッド、または Horizon ポッド）によって異なります。ご使用の環境で自動デプロイ ウィザードを使用できるポッド タイプに対してポッドのデプロイを開始できます。

アクション	説明
[新規] - [*ポッドのタイプ*]	**注：** KB-92424 で示されているように、[新規] アクションは、第 1 世代の制御プレーンの提供終了 (EOA) からの承認された例外がある場合にのみ使用できます。 ポッド フリートに新しいクラウド接続されたポッドを追加するワークフローを開始します。最初のポッドの追加後に、ポッドを追加する際にこのアクションを使用します。ポッドの追加方法は、必要なポッドのタイプと、現在の制御プレーン サービス レベルでの使用がサポートされているものによって異なります。 以下のトピックは、ポッドのタイプに基づく詳細な手順にリンクしています。 ■ ポッド マネージャ ベースの新しいポッドをフリートに追加する場合：このユース ケースにはメニュー フロー [新規] - [Microsoft Azure] が適用されます。第 1 世代テナント - Microsoft Azure 上の Horizon Cloud ポッド - 第 1 世代 Horizon Universal Console の [キャパシティ] ページを使用した、ポッド フリートへのポッドの追加の手順を参照してください。 ■ 新しい Connection Server デプロイを追加する場合：これらのデプロイでは、Horizon Cloud Connector を使用します。このユース ケースにはメニュー フロー [新規] - [VMware SDDC] が適用されます。このオプションを使用した後、[ダウンロード] をクリックして、最新の Horizon Cloud Connector アプライアンスをダウンロードするための簡単なパスを選択します。詳細については、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
[編集]	ポッドを選択し、[編集] をクリックして、ポッドの編集可能な特性を変更します。
[削除]	ポッドを選択し、[削除] をクリックして、ポッドをテナントから削除します。 **ヒント:** 削除ワークフローの結果は、ポッドのタイプによって異なります。 ■ ポッド マネージャ ベースのポッドの場合、削除ワークフローによって、ポッドとそのすべてのアーティファクトが Microsoft Azure サブスクリプションから削除されます。 ■ Connection Server に構築されたポッドの場合、削除ワークフローによってポッドが Horizon 制御プレーン サービスから切断され、ポッドはクラウド接続ポッドではなくなります。ポッドのアーティファクトは、Horizon Cloud Connector を使用してポッドをクラウドに接続する前にデプロイ先だったキャパシティ環境にとどまります。このようなポッドの場合、削除ワークフローは、Horizon Cloud Connector ユーザー インターフェイスで Horizon Cloud Connector [接続解除] アクションを使用する場合と同じ結果になります。
[詳細] - [状態の変更]	ポッドが監視対象の状態にあり、特定の要件を満たす場合は、Universal Broker およびマルチクラウド割り当てでの使用のために管理対象の状態に変更できます。 **注：** コンソールには、Connection Server デプロイ タイプに対してのみこのアクションが表示されます。上述したように、ポッド マネージャ ベースのポッドは常に管理対象状態になります。結果として、このようなポッドの状態を変更することはできません。 このワークフローを使用するには、監視対象状態にあるポッドを選択してから [詳細] - [状態の変更] を選択します。詳細については、Horizon Universal Console を使用して、クラウド接続された Horizon ポッドを管理対象状態に変更する

ポッド： 詳細ページ

[キャパシティ] ページでポッドの名前をクリックすると、ポッドの詳細ページが表示されます。ポッドの詳細ページには、そのポッドで実行できる情報とアクションが表示されます。ポッドについて表示できる詳細な特性のタイプは、ポッドのタイプによって異なります。ポッドに対して実行できるアクションのタイプは、ポッドのタイプとポッドの現在の状態によって異なります。ポッドの編集やテナント環境からのポッドの削除など、一部のアクションは、ポッドに対して実行できるワークフローを [キャパシティ] ページから複製します。

表 3-2. タイプに応じたポッドの詳細ページ

タイプ	詳細
Horizon ポッドのデプロイ（Connection Server テクノロジーを使用してデプロイされたポッド）	ページには、[サマリ] および [監査ログ] タブがあります。[監査ログ] タブの詳細については、監査ログの操作を参照してください。 ポッドの [サマリ] タブのアクション ボタンを使用して、現在これらのポッドでの使用がサービスによってサポートされているアクションを実行します。 ■ [編集] ボタンを使用して、ポッドの編集可能な特性を変更します。詳細については、Horizon Cloud - [キャパシティ] ページの編集ワークフローを使用した、クラウド接続されたポッドのクラウドに関連するいくつかの特性の変更を参照してください。 ■ [切断] ボタンを使用して、Horizon Cloud テナント環境からポッドを削除します。クラウド接続された Horizon ポッドを Horizon Cloud での使用から削除するを参照してください。 ■ 更新されたバージョンが利用可能な場合は、[スケジュールの更新] ボタンを使用して、Horizon Cloud Connector 仮想アプライアンスの自動更新をスケジュールします。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。 ■ 制御プレーン サービスとしての Horizon Console の起動に記載されているように、ポッドの Horizon Connection Server に対して Horizon Console を実行するには、[Horizon Console の起動] ボタンを使用します。 ■ [詳細] - [コネクタ ログのダウンロード] ボタンを使用して、Horizon Cloud Connector アクティビティのログ ファイルを収集します。 [バージョン番号] フィールドに表示される数字は、ポッドで現在実行されている Horizon Cloud Connector のバージョンとビルド番号を反映しています。
Horizon Cloud ポッド（ポッド マネージャ テクノロジーを使用してデプロイされたポッド）	ページには、[サマリ]、[システム アクティビティ]、[ユーザー アクティビティ]、および [監査ログ] タブがあります。[監査ログ] タブの詳細については、監査ログの操作を参照してください。 ポッドの [サマリ] タブのアクション ボタンを使用して、現在このタイプのポッドでの使用がサービスによってサポートされているアクションを実行できます。 ■ ポッドの一部のプロパティを編集する。プロパティのすべてが編集可能であるとは限りません。編集ワークフローは、単純なプロパティを変更するだけでなく、ポッドの構成を変更するためにも使用されます。たとえば、編集ワークフローを使用して、新しい SSL 証明書をポッドの Unified Access Gateway インスタンスにアップロードしたり、2 要素認証構成をポッドのゲートウェイ設定に追加したり、既存の 2 要素認証構成を別の構成に切り替えたり、まだゲートウェイ設定がないポッドにゲートウェイ設定を追加したりできます。このタイプのポッドの管理タスクへのリンクのリストについては、Microsoft Azure にデプロイされた Horizon Cloud ポッドの管理を参照してください。 ■ ポッド全体を削除するか、ポッドのゲートウェイ構成を削除します。 ■ システムがポッドに仮想マシンのサブネットを追加しているときに問題が発生した場合、コンソールでは [失敗したネットワークの再デプロイ] アクションを使用できるようになります。このアクションを使用して、システムをトリガして再試行することができます。 ■ ポッド マネージャ仮想マシンに書き込まれたログをダウンロードします。 ■ テナントに Horizon Cloud ポッドのシングルポッド仲介構成があり、このポッドを Workspace ONE Access Connector と統合しているシナリオでは、コンソールは 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するためのアップロード ワークフローを提供します。手順についてはコネクタがポッド マネージャ仮想マシンへの接続を信頼できるように、Workspace ONE Access コネクタ アプライアンスを Microsoft Azure の Horizon Cloud ポッドと統合する場合には、ポッド マネージャ仮想マシンで SSL 証明書を直接構成します。を参照してください。 [バージョン番号] フィールドに表示される数字は、ポッドが現在実行されているソフトウェア バイナリのバージョンを反映しています。このバージョンは、ポッドのマニフェスト番号またはポッドのビルド番号と呼ばれることがあります。ポッド ソフトウェアの更新版をポッドで使用できる場合、画面にはポッドに適用できるマニフェスト番号を含むメッセージが表示されます。

表 3-2. タイプに応じたポッドの詳細ページ （続き）

タイプ	詳細
	ポッドの詳細ページからポッドのサブスクリプション情報を編集することもできます。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、更新を参照してください。 ポッドの詳細ページから、このようなポッドが Microsoft Azure サブスクリプション制限を使用しているレベルを調べることもできます。Horizon Universal Console を使用して、サブスクリプションによる Microsoft Azure 制限の現在の使用率を調べるを参照してください。

ポッド： 健全性ステータスの表示

Cloud Monitoring Service (CMS) は、各ポッドからの情報を取得し、その情報を使用して [キャパシティ] ページと [ダッシュボード] ページにポッドの健全性を示します。[キャパシティ] ページの [ステータス] 列に表示される健全性ステータスの意味は、次のセクションに記載されています。[キャパシティ] ページでは、ステータス アイコンの上にカーソルを置くと、報告されたステータスの基盤となる詳細を表示できます。

オンライン

ポッドには健全性の問題はありません。ポッドのコネクタ サービスは オンライン ステータスで、すべてのポッドのサービスが動作しています。

準備完了

ポッドには健全性の問題はありません。ポッドのデプロイまたは更新プロセスの完了など、ポッドが オンライン に移行しているときに、[キャパシティ] ページに 準備完了 のステータスが一時的に表示されることがあります。

エラー

ポッドには重大な健全性の問題がいくつかあり、対処する必要があります。重大な問題は、ポッドの正常な動作に影響します。

警告

CMS が、ポッドから健全性ステータスを取得しましたが、いくつかの問題があります。これらの問題はポッドの操作にとって重大ではないため、ポッドは正常に動作します。

オフライン

CMS は、ポッドで接続サービスが実行されていないことを検出しました。

- ポッド マネージャ ベースのポッドの場合、このステータスは通常ポッドのマネージャ仮想マシンが実行されていないことを意味します。この状況はまれであり、通常、Microsoft Azure ポータルを使用してポッド マネージャを手動でシャットダウンした場合、または Microsoft Azure クラウドに障害が起きている場合に発生します。
- クラウド接続された Horizon Connection Server デプロイの場合、このステータスは、Horizon Cloud Connector と制御プレーンの間に接続がないことを意味します。Horizon Cloud Connector が操作可能で実行中であることを確認します。

不明

CMS は、ポッドから健全性ステータスを取得できません。Horizon ポッドの場合、通常このステータスは、Horizon ポッドへの API 呼び出しで情報を取得できないことを意味します。たとえば、Horizon Cloud Connector インスタンスまたは Connection Server インスタンスに問題があり、必要なデータを提供できない場合などです。

サイト

[サイト] タブは、環境が Universal Broker を使用するように構成されている場合に表示されます。Horizon Cloud 環境のサイトの詳細については、Universal Broker 環境でのサイトの操作およびそのサブ トピックを参照してください。

リソース

制御プレーンでは、各タイプのリソース キャパシティに存在するポッドと連携するために、特定のタイプの情報が必要です。この情報は、リソース キャパシティを Horizon Cloud 環境に関連付けるときに制御プレーンの構成セットに保存されます。[リソース] タブには、次のものがあります。

- それらの保存された構成設定の概要。
- それらの設定を管理するための [管理] アクション。現在、このタブには、制御プレーンで Horizon Cloud on Microsoft Azure のポッド マネージャ ベースのデプロイの実行と管理に使用する、保存された Microsoft Azure サブスクリプション情報を管理する機能が用意されています。Horizon Cloud：Microsoft Azure サブスクリプション情報の削除、編集、および追加を参照してください。

次のトピックを参照してください。

- 制御プレーン サービスとしての Horizon Console の起動
- 第 1 世代テナント - 第 1 世代 Horizon Universal Console の [キャパシティ] の概要と、Horizon Cloud のポッド フリートへのポッドの追加
- Horizon Cloud - [キャパシティ] ページの編集ワークフローを使用した、クラウド接続されたポッドのクラウドに関連するいくつかの特性の変更
- クラウド接続された Horizon ポッドを Horizon Cloud での使用から削除する

制御プレーン サービスとしての Horizon Console の起動

クラウド接続された Horizon ポッドを管理するには、そのポッドの Horizon Connection Server に対して Horizon Console を実行します。Horizon Universal Console から起動すると、Horizon Console は Horizon 制御プレーン サービスから統合クラウド サービスとして実行され、シングル サインオン (SSO) 認証をサポートします。

ポッドの詳細ページまたは [ダッシュボード] ページから、特定の Horizon ポッドの Connection Server に対して Horizon Console を実行できます。Horizon Console は、Horizon Horizon Universal Console ログイン セッションの SSO 認証情報を使用して、新しいブラウザ タブで開きます。追加の認証情報は不要です。

Horizon Console をクラウド サービスとして使用すると、次の場合を除き、Horizon Console をネイティブに実行するときと同じポッドの管理機能のすべてにアクセスできます。

- ヘルプ デスク機能。Horizon ポッドに関連する問題に対してトラブルシューティングを行うには、代わりに Horizon Cloud 環境内のヘルプ デスク機能を使用します。
- JMP Server の機能。ユーザーのデスクトップ ワークスペースを定義して管理するには、Universal Broker 環境での割り当ての作成および管理および Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成の説明に従って、代わりにマルチクラウド割り当てを構成します。

Horizon Console の使用方法の詳細については、VMware Horizon ドキュメントを参照してください。

注: Horizon ポッドがクラウド サービスとして Horizon Console を実行するための要件を満たしていない場合、パブリック ネットワークからポッドの Connection Server にアクセスできる場合に限り、SSO 認証なしで Horizon Console のネイティブ インスタンスが開きます。この状況が発生すると、新しいブラウザ タブが開き、ポッドの Connection Server にログインするように求めるネイティブ Horizon Console ページが表示されます。ただし、Connection Server がパブリックからアクセスできない場合（ファイアウォールの内側にあるなど）、ブラウザ タブが開き、接続エラーが表示されます。このような場合は、Connection Server エンドポイントから直接 Horizon Console を実行する必要があります。

前提条件

Horizon 制御プレーンから Horizon Console を実行するには、スーパー管理者ロールで Horizon Universal Console にログインする必要があります。

さらに、Horizon Connection Server のバージョンと Horizon Cloud Connector のバージョンが、現在サポートされている組み合わせの 1 つであることを確認します。2022 年 12 月の時点で、クラウド接続された Horizon ポッドには、Horizon Cloud Connector バージョン 2.1.2 以降を使用することをお勧めします。

手順

- ポッドの詳細ページから Horizon Console を実行します。
  a Horizon Universal Console で、[設定] - [キャパシティ] の順に選択します。
  b [キャパシティ] ページのポッド リストで、管理する Horizon ポッドの名前をクリックします。
  c ポッドの詳細ページで、[Horizon Console の起動] をクリックします。
- [ダッシュボード] ページから Horizon Console を実行します。
  a Horizon Universal Console で、[監視] - [ダッシュボード] の順に選択します。
  b [ダッシュボード] ページの [概要] タブにある [問題] または [セッション] ビューで、管理する Horizon ポッドの名前をクリックします。

次のステップ

クラウド サービスとしての Horizon Console からログアウトすると、Horizon Universal Console のログイン画面にリダイレクトされます。

第 1 世代テナント - 第 1 世代 Horizon Universal Console の [キャパシティ] の概要と、Horizon Cloud のポッド フリートへのポッドの追加

第 1 世代 Horizon Cloud のテナント環境におけるポッドのフリートに最初のクラウド接続ポッドが追加され、Active Directory ドメイン登録が完了したら、コンソールの [キャパシティ] ページにアクセスできます。その時点で、[キャパシティ] ページの [新規] メニューが表示されます。そのメニューを使用して、フリートへのさらなるポッドの追加を開始できます。

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。

コンソールで、[設定] - [キャパシティ] を使用して [キャパシティ] ページを開きます。

フリートへのポッドの追加を開始するには、[新規] をクリックし、追加するポッドのタイプに応じて適切なオプションを選択します。

注： KB-92424 で示されているように、[新規] アクションは、第 1 世代の制御プレーンの提供終了 (EOA) からの承認された例外がある場合にのみ使用できます。

重要： フリートにポッドを追加するためのメニューの選択肢と特定のワークフロー手順は、追加するポッドの正確なタイプと、Horizon Cloud テナント アカウントの構成に応じた使用においてサポートされる機能によって異なります。第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアーで説明するように、コンソールは動的であり、テナント アカウントでの構成内容に応じて機能が表示されたりされなかったりします。期待する機能がコンソールに表示されない場合は、情報に関するサポート リクエストを提出して申請してください。

Microsoft Azure の新しい Horizon Cloud ポッドをフリートに追加する場合

この使用事例では、メニュー フロー [新規] - [Microsoft Azure] を使用します。このフローにより、ポッド マネージャ ベースの Horizon Cloud ポッドのデプロイを自動化するウィザードが開始されます。これらのポッドは、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、これは Microsoft Azure サブスクリプションでのみ動作します。詳細なワークフロー手順については、第 1 世代テナント - Microsoft Azure 上の Horizon Cloud ポッド - 第 1 世代 Horizon Universal Console の [キャパシティ] ページを使用した、ポッド フリートへのポッドの追加を参照してください。

ヒント: この選択肢は、Azure VMware Solution (AVS) 上の Horizon ポッドには該当しません。AVS 上の Horizon ポッドは、Horizon Connection Server テクノロジーをベースとしたポッドです。

新しい Horizon ポッドを追加する場合（Azure VMware Solution (AVS) 上の Horizon ポッドを含む）

Horizon ポッドは、ポッド マネージャ テクノロジーではなく、Horizon Connection Server ソフトウェアをベースとしています。今回のリリースでは、Horizon Cloud Connector を使用してこれらすべてのタイプのポッドを追加します。Horizon ポッドは、オンプレミス環境またはクラウド環境にすでに存在し、実行されている必要があります。このユース ケースにはメニュー フロー [新規] - [VMware SDDC] が適用されます。このオプションを使用した後、[ダウンロード] をクリックして、最新の Horizon Cloud Connector アプライアンスのダウンロード元となる my.vmware.com ダウンロード ページに移動します。アプライアンスをダウン

ロードした後にポッドを接続するためのワークフロー手順については、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。

注意： 特に VMware Cloud on AWS 上の Horizon ポッドに関しては、[新規] - [VMware SDDC] をクリックした後、そのタイプに対して [追加] アクションがコンソールに表示される可能性がありますが、そのパスは使用しないでください。現時点では、このパスは汎用的なものではありません。また、公開されているドキュメントはありません。VMware Cloud on AWS に Horizon ポッドを追加するには、[ダウンロード] パスを使用します。

第 1 世代テナント - Microsoft Azure 上の Horizon Cloud ポッド - 第 1 世代 Horizon Universal Console の [キャパシティ] ページを使用した、ポッド フリートへのポッドの追加

第 1 世代 Horizon Cloud テナントのポッド フリートに少なくとも 1 つのポッドがある状態になり、Active Directory ドメイン登録の手順が完了した後、[キャパシティ] ページには、ポッド フリートにポッドを追加するためのメニュー オプションが表示されます。この特定のワークフローは、Horizon Cloud ポッドに適用されます。これらのポッドは、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、これは 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。

注： KB-92424 で示されているように、[新規] アクションは、第 1 世代の制御プレーンの提供終了 (EOA) からの承認された例外がある場合にのみ使用できます。

さまざまなポッド タイプのフリートにポッドを追加する方法の概要については、第 1 世代テナント - 第 1 世代 Horizon Universal Console の [キャパシティ] の概要と、Horizon Cloud のポッド フリートへのポッドの追加を参照してください。

重要： ここでのワークフローは、Azure VMware Solution (AVS) 上の Horizon ポッドには該当しません。この特定のワークフローは、Horizon Cloud ポッドに適用されます。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おり、Horizon ポッドは Connection Server テクノロジーに基づいています。

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。

ウィザードには、複数の手順があります。手順で情報を指定した後に、[次へ] をクリックして次の手順に進みます。

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。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のリストを参照してください。

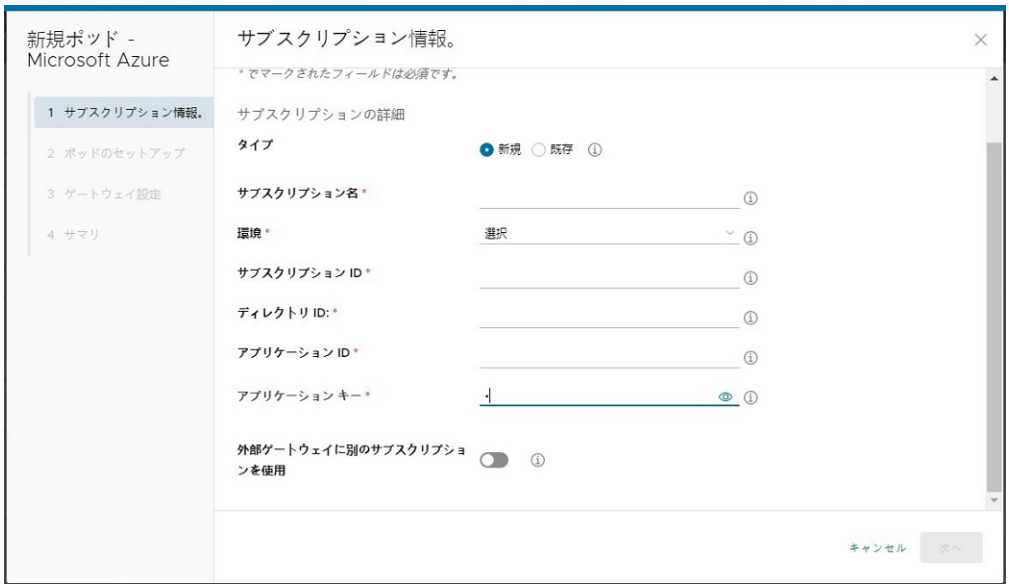
追加のポッドに使用する構成で必須となる項目に加えて、追加のポッドをデプロイする前に、クラウド接続された最初のポッドが完全にデプロイされ、Active Directory ドメイン バインドおよびドメイン参加の手順が完了している必要があります。顧客アカウント レコード内のクラウド接続されたすべてのポッドは同じ Active Directory 情報を共有し、クラウド接続されたそれぞれのポッドはすべてのクラウド構成の Active Directory ドメインとの接続状態を維持している必要があります。詳細については、第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行を参照してください。

テナントが Universal Broker で構成され、ブローカ設定で 2 要素認証が有効になっている場合は、2 要素認証設定を持ち、同じ 2 要素認証タイプを使用する外部 Unified Access Gateway が必要です。

手順

1 コンソールで、[設定] - [キャパシティ] に移動し、[新規] - [Microsoft Azure] をクリックして、ポッド デプロイ ウィザードを起動します。

ウィザードの最初の手順が開きます。



2 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。

既存のサブスクリプションを選択すると、この手順は以前にシステムに入力されたサブスクリプションの情報で自動入力されます。

重要： 新しい情報を入力する場合は、入力するサブスクリプション情報が第 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述されるサブスクリプション要件を満たしていることを確認する必要があります。特に、サービス プリンシパルに必要な役割の権限が付与されていることを確認してください。

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。
[環境]	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。 ■ [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]	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。 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。

3 [次へ] をクリックして、次の手順に進みます。

[次へ] をクリックすると、新しいサブスクリプションを追加するときに、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。
- 指定され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、共同作成者ロール、またはポッド デプロイヤが必要とするロール操作用に構成されたカスタム ロールのいずれかがあるか。
- 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、「アプリケーション登録を作成して Horizon Cloud ポッド デプロイヤに必要なサービス プリンシパルを作成する」と「Microsoft Azure サブスクリプションでの Horizon Cloud に必要な操作」のトピックを参照してください。

値の確認に関するエラー 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。たとえば、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、エラー メッセージが表示されます。

このエラー メッセージが表示される場合は、複数の値が無効になってい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。

4 このウィザードの手順では、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。

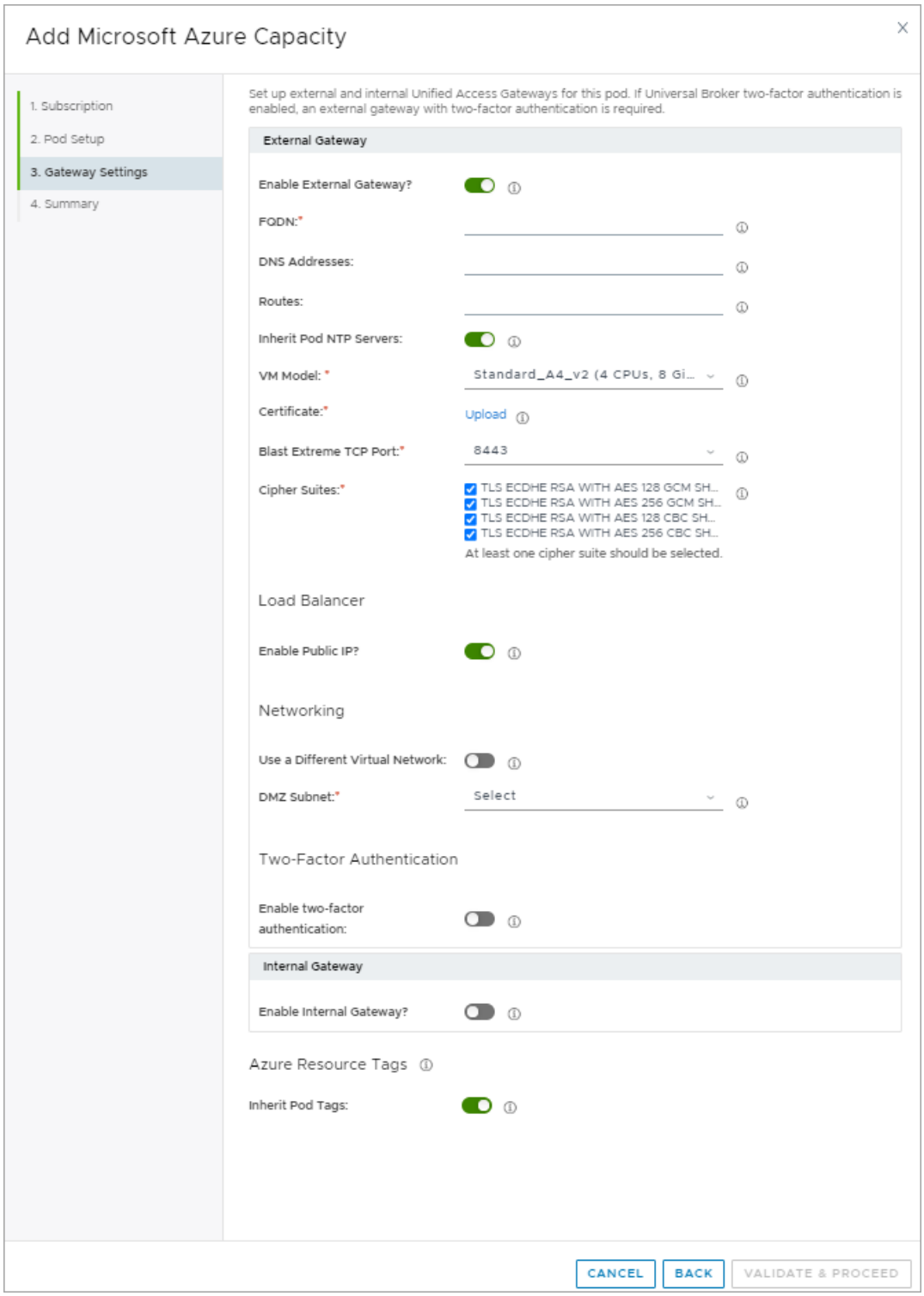
オプション	説明
[サイト]	Microsoft Azure のポッドに Universal Broker を使用するようにテナント環境が構成されていて、追加のポッドをデプロイしているときは、ウィザードに [サイト] が表示されます。ポッドをサイトに関連付けます。既存のサイトの選択、デフォルトのサイト の使用、新しいサイト名の指定のいずれかが可能です。[キャパシティ] 画面の [サイト] タブには、環境内ですでに構成されているサイトが一覧表示されます。
[ポッド名]	このポッドにわかりやすい名前を入力します。管理コンソールでは、他のポッドと区別するために、この名前が使用されます。 **注：** この名前は、Horizon Cloud 顧客アカウントの既存のポッドにおいて一意である必要があります。名前は、[キャパシティ] ページに記載されているポッドの名前と一致してはいけません。
[場所]	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。 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。 [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。 **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。
[Microsoft Azure リージョン]	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。 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。 **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。
[説明]	オプション：このポッドの説明を入力します。

オプション	説明
[Azure リソース タグ]	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。 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。 ■ 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。 < > % & \ ? / ■ 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]	リストから仮想ネットワークを選択します。 [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。
[既存のサブネットを使用]	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。 **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。
[管理サブネット] [管理サブネット (CIDR)]	[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。 **重要：** ■ 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。 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。 [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。 **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。

オプション	説明
[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]	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。 [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。 **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。 [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。 **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には拡張できません。 **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。
[NTP サーバ]	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。 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。 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。
[プロキシを使用]	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。 ポッド デプロイヤは、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。 ■ [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。 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。 

5 [次へ] をクリックして、次の手順に進みます。

以下のスクリーンショットは、次の手順が最初に表示された場合の例です。一部のコントロールは、外部 Unified Access Gateway 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ために、最初のウィザード手順で選択した場合にのみ表示されます。



6 必要なゲートウェイ構成の情報を指定し、オプションで、そのゲートウェイで 2 要素認証構成を指定します。テナントが、Universal Broker 設定ですでに 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、外部の Unified Access Gateway を選択し、ゲートウェイで同じ 2 要素認証タイプを指定する必要があります。

次のトピックの手順を完了させます。

- 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
- 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

注： この手順では、ゲートウェイのリソース グループで、ポッドに指定したものと同じカスタム タグを継承するか、別のカスタム タグを指定するかを選択できます。両方のゲートウェイ タイプで、同じ一連の指定されたタグを使用します。

7 [検証と続行] をクリックします。

[検証と続行] をクリックすると、システムは指定された値の有効性と妥当性を、以下のように検証します。

- サブネットが有効で、サブスクリプション内で選択したリージョンの他のネットワーク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。
- 証明書は正しい PEM 形式になっているか。

ネットワーク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。

すべての項目の検証に問題がない場合、[サマリ] ページが表示されます。

8 概要情報を確認して、[発行] をクリックしてください

Microsoft Azure 環境へのポッドのデプロイを開始します。

結果

ポッドのデプロイに最大で 1 時間ほどかかる場合があります。ポッドが正常にデプロイされるまで、そのポッドの進捗状況のアイコンが表示されます。更新の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。

重要： Microsoft Azure China クラウドに追加のポッドをデプロイする場合、プロセスが完了するまでに 1 時間以上かかることがあります。このプロセスは地理的なネットワークの問題の影響を受け、バイナリがクラウドの制御プレーンからダウンロードされるときにダウンロードの速度が低下することがあります。

次のステップ

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。

Unified Access Gateway 構成を設定するように指定した場合、指定した構成のタイプに応じて、適切な CNAME レコードを DNS サーバに設定するようにします。

- 外部 Unified Access Gateway 構成を設定する場合、デプロイ ウィザードに入力した FQDN を、ポッドの Microsoft Azure パブリック ロード バランサの自動生成された FQDN にマッピングします。
- 内部 Unified Access Gateway 構成の場合、デプロイ ウィザードに入力した FQDN を、ポッドの Microsoft Azure 内部ロード バランサのプライベート IP アドレスにマッピングします。

ポッド詳細ページで必要なロード バランサ情報を確認する手順については、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 を参照してください。

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 オファー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 オファー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

- 他のポッドをもう 1 台追加する場合は、以前のポッドで使用したものと同じサブスクリプションを使用するか、組織で必要な場合は別のサブスクリプションを使用することができます。別のサブスクリプションを使用しようとする場合は、『デプロイ ガイド』に記載されている手順を実行して、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、およびアプリケーション キーを取得する必要があります。使用するサブスクリプションが、確実にそのガイドに記載されている要件を満たしている必要があります。特に、サービス プリンシパルに、サブスクリプション内の該当するレベルで付与される適切なロールの権限が付与されていることが必要です。「Horizon Cloud のドキュメント」ページから、オンラインのスタート ガイド ドキュメントに移動することができます。

- テナントが Microsoft Azure のポッドに対して Universal Broker を使用するように構成されている場合、ポッド デプロイ ウィザードを実行して新しいポッドを追加するときに、サイトを指定する必要があります。既存のサイトを選択するか、新しいサイトを指定できます。
- ポッドをデプロイするリージョンに VNet があり、VNet が Microsoft Azure で必要な仮想ネットワークを構成するに記載されている要件を満たしているかを確認します。

  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できる必要があります。
- 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。

- デプロイヤが必要なサブネットを自動的に作成するようにしたくない場合は、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。

  重要： 最初のポッドをデプロイした後に追加ポッドをデプロイする際、既存のポッドですでに使用されている既存のサブネットを再使用しないでください。ポッドですでに使用されているサブネットを共有しようとしないでください。別のポッドがすでに使用しているサブネットを選択すると、その既存のポッドとそのサブネットを使用してデプロイするポッドの操作が中断されます。

  ポッドごとに個別の VNet を使用することをお勧めします。この推奨事項は、Horizon Cloud の使用前および使用中に知っておくべきことで説明されている、単一のサブスクリプションにデプロイするポッドの数に関して考慮すべきガイダンスに基づいています。単一のサブスクリプション内の Microsoft Azure の制限を回避するために、サブスクリプションごとに 1 つのポッドがある場合は、これらの制限に達する可能性を回避します。Microsoft Azure では各サブスクリプションに専用の VNet が必要であるため、サブスクリプションごとに 1 つのポッドを使用するベスト プラクティスに従う場合は、各ポッドに個別の VNet を使用するベスト プラクティスに自動的に準拠することになります。

- デプロイヤで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、デプロイヤ自体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の 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。この場合の、`ID` はゲートウェイのデプロイヤ 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、デプロイヤは 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、Horizon Cloud ポッド デプロイ ウィザード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で選択します。また、Microsoft Azure サブスクリプションでの Horizon Cloud によって要求される操作で説明するように、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 - 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。

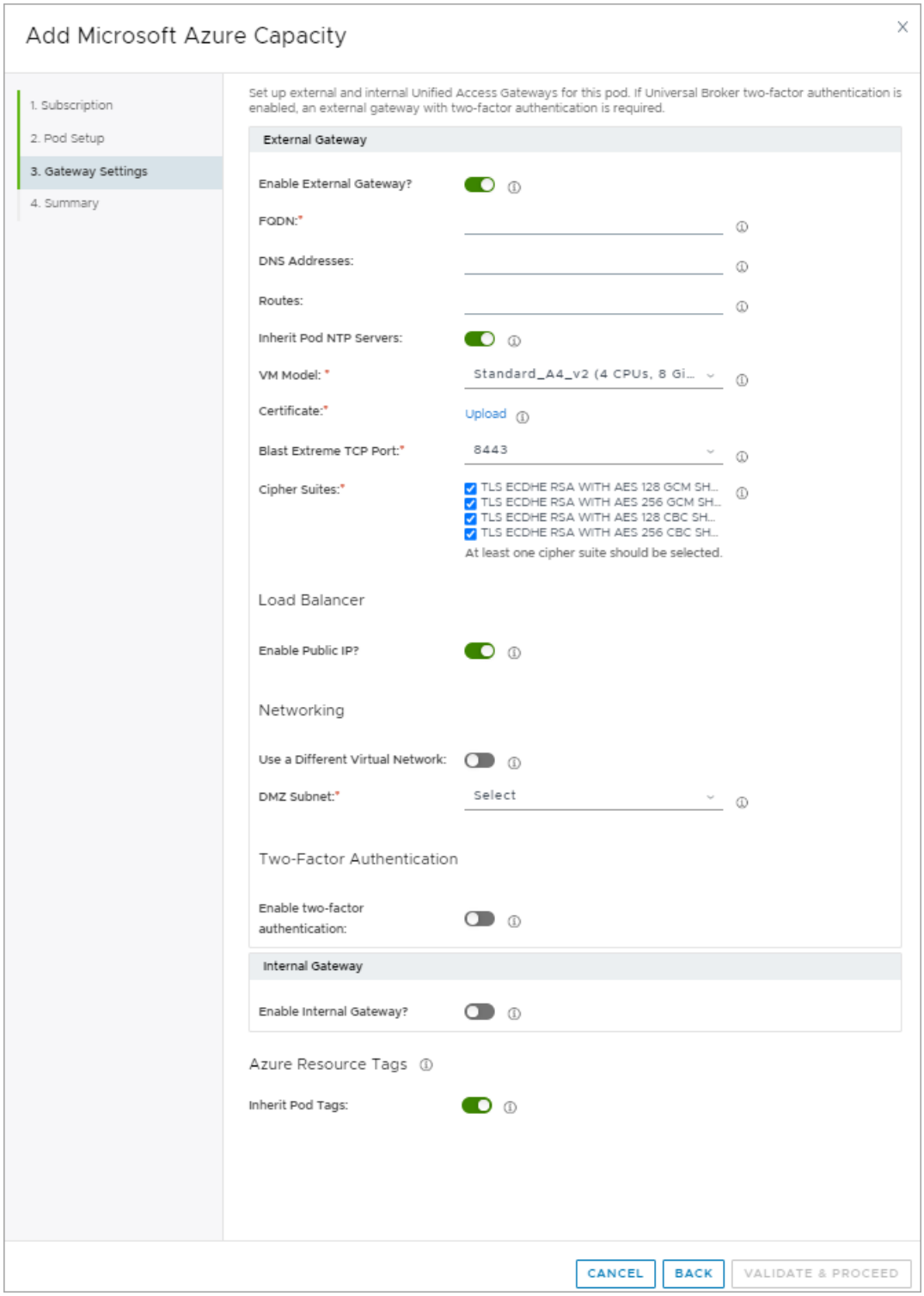
外部ゲートウェイ構成の場合、ポッドの VNet とは別の VNet に構成をデプロイするオプションもあります。VNet をピア接続する必要があります。このタイプの構成では、ポッドをハブ - スポーク ネットワーク トポロジなど Microsoft Azure のより複雑なネットワーク トポロジーにデプロイできます。

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。



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。

また、テナント環境が Universal Broker を使用するように構成されている場合、サービスはクラウド制御プレーンからこの FQDN に接続でき、外部ゲートウェイ構成で構成されている 2 要素認証設定が Universal Broker 用に構成されたものと一致することと、クラウド接続されたポッド フリート内の他のすべての Unified Access Gateway インスタンスの設定と一致することを検証できる必要があります。

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?]	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。 **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。 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。
[FQDN]	`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。 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。 **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。
[DNS アドレス]	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。 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。 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 サーバと通信できる必要があります。 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。 [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。
[ルート]	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。 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。 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`）。

オプション	説明
[ポッドの NTP サーバの継承]	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。 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。 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。
[仮想マシン モデル]	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。 **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。
[証明書]	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。
[Blast Extreme TCP ポート]	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。 **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。
[暗号スイート]	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。 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。

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?]	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。 **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。 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。
[Horizon FQDN のパブリック IP アドレス]	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。デプロイヤは、この IP アドレスを Unified Access Gateway 構成の設定で構成します。

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]	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。 **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。 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。
[別の仮想ネットワークを使用] - オフ	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。 ■ [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。 **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。 ■ [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	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。 **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。 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。 ■ 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 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 バランサは、プライベート IP アドレスで構成されます。
[FQDN]	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。 **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。
[DNS アドレス]	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。 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。 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 サーバと通信できる必要があります。 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。 [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。
[ルート]	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。 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。 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`）。
[ポッドの NTP サーバの継承]	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。 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。

オプション	説明
[仮想マシン モデル]	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。 **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。
[証明書]	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。
[Blast Extreme TCP ポート]	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。 **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。
[暗号スイート]	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。 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。

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]	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。 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。
[Azure リソース タグ]	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。 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。 ■ 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。

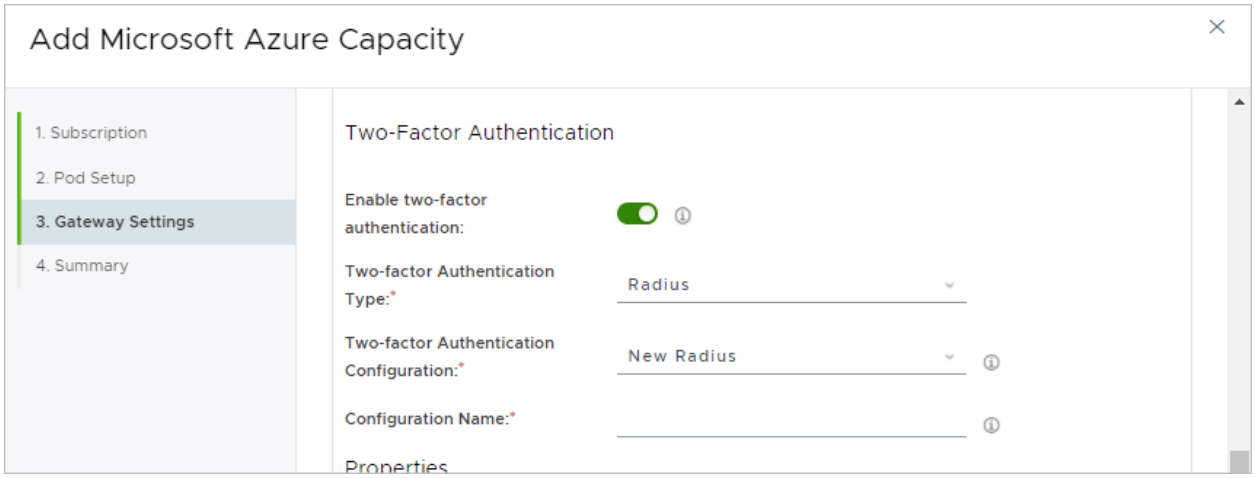
結果

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 - Microsoft Azure 上の Horizon Cloud ポッド - 第 1 世代 Horizon Universal Console の [キャパシティ] ページを使用した、ポッド フリートへのポッドの追加の最後の手順を完了してください。

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。



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

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]	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。 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。 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`）。

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。

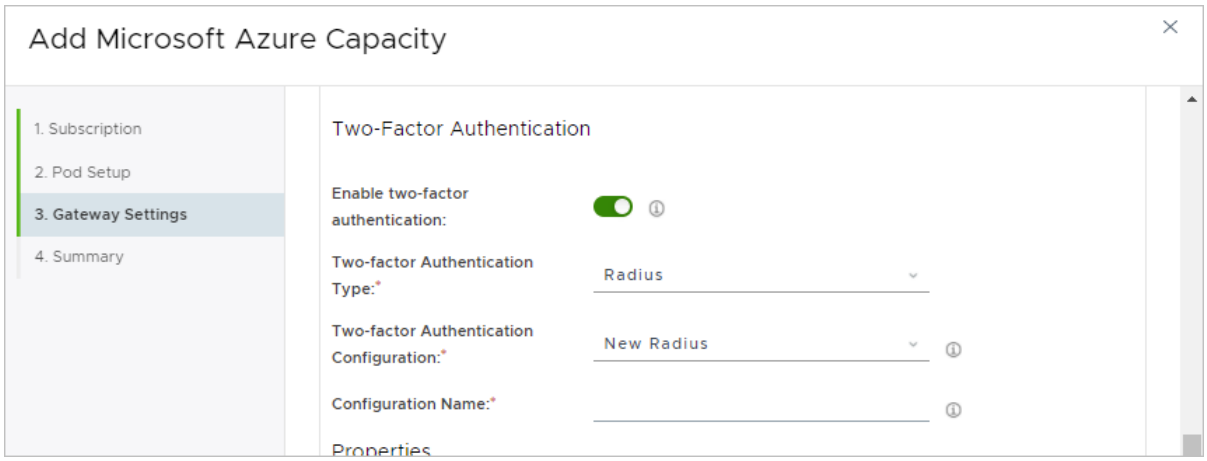
- RSA SecurID Authentication Manager サーバの IP アドレス。
- RSA SecurID Authentication Manager サーバまたはそのロード バランサ サーバに自己署名証明書がある場合は、[ポッドの追加] ウィザードで CA 証明書を指定する必要があります。証明書は PEM 形式である必要があります（ファイル タイプ `.cer`、 `.cert`、または `.pem`）。

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]	必要に応じて、ユーザーに RADIUS ユーザー名とパスコ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 DisplayHint user name and passcode` としてエンドユーザーに表示されます。ここで、*DisplayHint* はこのフィールドで指定するテキストです。 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。
[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]	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： ■ 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。 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。 **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。
[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、アカウンティング 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 - 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がチェックされ、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。Vnet 設定の詳細については、Horizon Cloud デプロイ ガイド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、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がチェックされ、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。

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。

Horizon Cloud - [キャパシティ] ページの編集ワークフローを使用した、クラウド接続されたポッドのクラウドに関連するいくつかの特性の変更

Horizon Universal Console の [キャパシティ] ページの [編集] ワークフローを使用して、Horizon Cloud テナントのクラウド接続されたポッドのクラウドに関連するいくつかの特性を変更および更新できます。

注意: クラウドベースの Horizon Universal Console のツアーで説明されているように、第 1 世代のコンソールは動的であり、第 1 世代のテナント環境の最新の構成に適した機能を反映しています。このドキュメントで説明されている機能へのアクセスは、以下の要因（ただしこれらに限定されない）に依存する場合があります。

- その機能が最新の第 1 世代の Horizon Cloud ポッド マニフェスト、Horizon ポッドのバージョン、または Horizon Cloud Connector のバージョンでのみ使用可能なシステム コードに依存するかどうか。
- 機能が初登場したときに、リリース ノートに記載されているように制限付きで機能へのアクセスが提供されるかどうか。
- 機能に特定のライセンスまたは SKU が必要かどうか。

このドキュメントに機能の記載があり、第 1 世代のコンソールにその機能が表示されない場合は、まずリリース ノートを読み、その機能のアクセスが制限されているかどうか、およびテナントで有効化をリクエストする方法について確認します。または、このドキュメントに記載されている機能を使用する資格があり、コンソールにその機能が表示されない場合は、VMware Horizon Cloud Service の担当者に問い合わせるか、担当者がいない場合は Customer Connect でサポート リクエストを発行する方法 (VMware KB 2006985)の記載内容に従って、サービス リクエストを Horizon Cloud Service チームに発行することができます。

コンソールの動的な性質により、実際の環境では、ここでの説明とは異なるエントリとラベルが表示されることがあります。テナントの現在の構成でサポートされている場合は、[ポッドを編集] ワークフローを使用して次の項目を変更できます。

- ポッドの名前と説明
- ポッドに関連付けられた場所
- ポッドのゲートウェイ関連の特性

コンソールに表示される場所は、世界の都市名に基づいています。システムは、都市の地理座標を使用して、ポッドを表すアイコンをコンソールの [ダッシュボード] ページのインタラクティブ マップに配置します。ポッドに関連付けられた地理的な場所を、位置関連のドロップダウン リストに表示されていない場所に変更する場合は、関連するエントリ フィールドで都市の名前の入力を開始します。

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。

手順

1 コンソールで、[設定] - [キャパシティ] の順にクリックして [キャパシティ] ページに移動します。

2 ポッドを選択し、[編集] をクリックして、[ポッドを編集] ワークフローを開始します。

3 [ポッドを編集] ウィンドウで、選択したクラウド接続されたポッドのタイプに応じて、下記のガイダンスや画面上のガイダンスに従います。画面上のガイダンスと下記の説明が異なる場合は、画面上のガイダンスが優先されます。

タイプ	説明
Horizon ポッド	ウィザードの [ポッドのセットアップ] の手順のフィールドとコントロールを使用して更新を行います。ポッドに関連付けられた地理的な場所を [ポッドの場所] ドロップダウン リストに表示されていない場所に変更する場合は、[新規] を選択し、ドロップダウン リストをクリックして、目的の場所名の入力を開始するエントリ ボックスを取得します。 ポッドの外部 FQDN などのゲートウェイ関連項目を更新するには、[ゲートウェイの設定] の手順のフィールドとコントロールを使用します。画面に表示される指示に従います。
Microsoft Azure の Horizon Cloud ポッド	[ポッドの詳細] の手順のフィールドとコントロールを使用して、更新を行い、変更をシステムに保存します。ポッドに関連付けられた地理的な場所を [場所] ドロップダウン リストに表示されていない場所に変更する場合は、[編集] をクリックし、目的の場所の名前を [市区町村名] フィールドに入力し、フィールドに保存します。 ポッドの外部ゲートウェイ FQDN などのゲートウェイ関連項目を更新し、FQDN に一致する証明書をアップロードするには、[ゲートウェイの設定] の手順のフィールドとコントロールを使用します。画面に表示される指示に従います。

4 変更を保存してウィザードを終了します。それには、必要に応じて [次へ] をクリックし、変更を保存してウィザードを終了するためのボタンを表示します。

クラウド接続された Horizon ポッドを Horizon Cloud での使用から削除する

Horizon ポッドを Horizon Cloud にクラウド接続するビジネス上の理由は、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という単純なユースケースから、クラウド接続された Horizon ポッドでサポートされるすべてのクラウド ホスト型サービスを活用することまで、多岐にわたります。これらのユースケースが不要になった場合、コンソールの [キャパシティ] ページの [削除] ボタンを使用して、クラウド接続されたポッドを、Horizon Cloud での使用から削除または切断することができます。Horizon Cloud から切断されると、そのポッドはクラウド接続されなくなり、サブスクリプション ライセンスを使用したり、そのポッドでクラウドにホストされたサービスを使用したりできなくなります。

ヒント: [キャパシティ] ページの [削除] アクションに加えて、ポッドの詳細ページには、同じ処理を実行する **切断** アクションがあります。

前提条件

そのポッドが含まれる割り当てからポッドを削除します。Horizon Cloud テナント環境でのマルチクラウド割り当ての編集を参照してください。

これらの手順を完了し、システムがポッドを切断するアクティビティを完了したときに、オンプレミスの Horizon ポッドがオフラインまたは使用できなくなると、システムはポッドの Connection Server と通信して Horizon グローバル データベース内のクラウド管理関連の適切なプロパティをクリアできなくなります。このプロパティは、ポッドが Horizon Cloud で使用中であることを Horizon Connection Server に通知します。この状況では、ここで手順を実行した後、さらに Horizon グローバル データベースを手動で編集して、クラウド管理関連のプロパティをクリアする必要があります。

手順

1 [キャパシティ] ページで、Horizon Cloud での使用から削除するポッドを選択します。

2 [削除] をクリックします。

以下の場合、通知メッセージが表示されます。

- ポッドが 1 つ以上の割り当てに含まれている場合は、ポッドを切断できないことを示すメッセージが表示されます。ポッドを削除する前に、まず割り当てからポッドの関連付けを解除する必要があります。
- ポッドがオフラインまたは使用できない場合、切断プロセス後もポッドはクラウド管理プロパティを Horizon グローバル データベースに保持するという警告メッセージが表示されます。プロセスを続行するかキャンセルするかを指定できます。

結果

切断プロセスを続行すると、ポッドは Horizon Cloud から切断され、ポッドの名前は管理コンソールのページに表示されなくなります。

次のステップ

切断中にポッドがオフラインまたは使用不可であるという通知メッセージが表示された場合は、Horizon のグローバル データベースを手動で編集して、ポッドのクラウド管理プロパティをクリアします。プロセス中にオフラインだった Horizon ポッドからクラウド管理プロパティをクリアして Horizon Cloud から切断するを参照してください。

プロセス中にオフラインだった Horizon ポッドからクラウド管理プロパティをクリアして Horizon Cloud から切断する

Horizon Cloud 管理コンソールの [削除] または [切断] ボタンを使用して、クラウド接続されたポッドを Horizon Cloud での使用から削除し、そのポッドがオフラインまたは使用不可であった場合でも、ポッドを Horizon Cloud から切断できます。ただしこの場合、Horizon Cloud がポッドと通信できなかったときにシステムは自動的にこれらのプロパティを削除できなかったため、続いて Horizon グローバル データベースからポッドのクラウド管理プロパティを削除する必要があります。削除しないと、クラウド管理プロパティによって、ポッドの名前変更やポッド フェデレーションからの削除ができなくなります。

前提条件

オンプレミス ポッドを Horizon Cloud から切断します。クラウド接続された Horizon ポッドを Horizon Cloud での使用から削除するを参照してください。

手順

1 ポッドの Connection Server にドメイン管理者権限でログインします。

2 Connection Server で、[ファイル] - [Windows 管理ツール] - [ADSI 編集] の順に選択します。

3 Horizon グローバル データベースへの接続を構成します。

a コンソールで、[ADSI 編集] を右クリックし、[接続先] をクリックします。

b [名前] テキスト ボックスに、**`Horizon 7 Global Database`** と入力します。

c [識別名または命名コンテキストを選択または入力する] を選択します。テキスト ボックスに、次の名前情報を入力します。

```
dc=vdiglobal,dc=vmware,dc=int
```

d [ドメインまたはサーバを選択または入力] を選択します。テキスト ボックスに、次のサーバ情報を入力します。

```
localhost:22389
```

e [OK] をクリックします。

Horizon グローバル データベースへの接続が確立されます。

4 [Horizon 7 グローバル LDAP データベース [localhost:22389]] - [DC=vdiglobal,dc=vmware,dc=int] に移動して、プロパティ ツリーを展開します。

5 ポッドからクラウド管理プロパティをクリアします。

a [DC=vdiglobal,dc=vmware,dc=int] で、[OU=Properties] および [OU=Pod] に移動します。

b [OU=Pod] リストでターゲット ポッドを見つけて右クリックし、[プロパティ] を選択します。

ポッドが、Horizon Administrator または Horizon Console の名前でリストに表示されます。

c [pae-CloudManaged] 属性の値を 0 に設定します。

値を 0 に設定すると、ポッドからクラウド管理プロパティがクリアされます。

6 グローバル資格からクラウド管理プロパティをクリアします。

a [DC=vdiglobal,dc=vmware,dc=int] で、[OU=Entitlements] に移動します。

b [OU=Entitlements] リストでグローバル資格を見つけます。グローバル資格を右クリックして、[プロパティ] を選択します。

グローバル資格が、Horizon Administrator または Horizon Console の名前でリストに表示されます。

c [pae-CloudManaged] 属性の値を 0 に設定します。

値を 0 に設定すると、グローバル資格からクラウド管理プロパティがクリアされます。

第 1 世代テナント - Day-2 Horizon Cloud Connector タスク

4

このドキュメント ページでは、Horizon Cloud Connector 仮想アプライアンスで通常実行される Day-2 タスクを紹介し、各タスクで実行される操作のページへのリンクを提供します。

個々の操作ページへのハイパーリンクについては、このページの下部にある操作へのリンクセクションまでスクロールしてください。

簡単な紹介

Horizon Cloud Connector 構成ポータルは、Horizon Cloud Connector 仮想アプライアンスが Horizon ポッドの Connection Server と正常にペアリングされ、ポッドが第 1 世代テナントに接続された後、各種の管理およびメンテナンス タスクを実行するためのアクセスを提供します。これらのタスクのいくつかは構成ポータルを使用して実行されますが、タスクによっては仮想アプライアンスのオペレーティング システムにアクセスし、アプライアンス上で構成ファイルを更新する必要があります。

一般的な Day-2 タスク

一般的なタスクには以下が含まれます。

- Horizon Cloud Connector 仮想アプライアンスの CA 署名付き証明書の構成。Horizon Cloud Connector 仮想アプライアンスの CA 署名付き証明書の構成のトピックを参照してください。
- 仮想アプライアンスの root ユーザーのパスワード有効期限ポリシーの設定。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のトピックを参照してください。
- 仮想アプライアンスへの自動更新をサポートする設定の構成。Horizon Cloud Connector 仮想アプライアンスの自動更新のトピックを参照してください。

  注： 仮想アプライアンスの自動更新を構成するには、VMware Horizon Cloud オペレーション チームがお使いの Horizon Cloud ユーザー アカウントでその機能を有効にする必要があります。デフォルトでは、その機能は有効ではありません。その機能の使用をリクエストするには、サービス リクエストを開くか、VMware の担当者にお問い合わせください。

- 仮想アプライアンスの固定 IP アドレスの更新。Horizon Cloud Connector 仮想アプライアンスの固定 IP アドレスの更新のトピックを参照してください。
- 仮想アプライアンスへの SSH アクセスの有効化および無効化。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。

- ネイティブ Amazon EC2 のデプロイの場合:アプライアンスのデプロイ時にデフォルトで有効化されない仮想アプライアンス内のサービスを有効にします。アプライアンスが、一部のサービスが無効の状態でデプロイされ、すでにポッドとペアリングされており、その後これらのサービスの一部を有効にする場合、手動の手順に従ってアプライアンスのサービスを有効にしてから、構成ポータルで[再構成フロー]を実行する必要があります。[再構成フロー]を実行すると、新しく有効になったサービスからの通信を、対応するクラウドプレーン サービスに対して受信できるようになります。ネイティブ Amazon EC2 のデプロイを有効化する手順については、『デプロイ ガイド』のトピックネイティブ Amazon EC2 のサービスを手動で有効にするを参照してください。
- 仮想アプライアンスのプロキシ設定と非プロキシ ホストの管理。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。
- 仮想アプライアンスの時刻と NTP サーバの同期。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 コンポーネントの健全性ステータスの確認。
- 仮想アプライアンスの手動での更新。Horizon Cloud Connector 仮想アプライアンスの手動更新を参照してください。
- 構成ポータルで同じポッドに Connection Server の詳細を再構成する場合は、[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。

  重要： 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 アカウントの認証情報に変更が生じる場合は、この [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変更する必要があります。
- この Connection Server インスタンスと制御プレーン間の接続を削除する場合は、[接続解除] をクリックします。

Horizon Cloud Connector 構成ポータルへのログインについて

Horizon Cloud Connector 構成ポータルを使用して実行できるタスクについては、第 1 世代テナント環境に有効な VMware Customer Connect 認証情報を使用してポータルにログインし、そこからタスクを実行します。ブラウザで次のいずれかを指定します。

- Horizon Cloud Connector アプライアンスの IP アドレス（`https://IP-address/`）
- DNS サーバで、完全修飾ドメイン名 (FQDN) を IP アドレスにマッピングする正引きおよび逆引きレコードを作成した場合、その FQDN

注： 第 1 世代テナント環境に登録済みの Active Directory ドメインがある場合、最初のログイン手順後に有効な Active Directory ドメインの認証情報でログインする必要があります。Horizon Cloud テナント環境への認証についても参照してください。

操作へのリンク

次のページとそのサブページを使用して、それぞれの操作とその手順にアクセスします。

次のトピックを参照してください。

- Horizon Cloud Connector 2.0 以降 - 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
- Horizon Cloud Connector 仮想アプライアンスの CA 署名付き証明書の構成
- Horizon Cloud Connector 2.4 以降 - 送信トラフィック用に SSL オフロードを構成している場合は、Horizon Cloud Connector でカスタムの CA 署名証明書を構成して Horizon 制御プレーンへの接続を許可する
- Horizon Cloud Connector 仮想アプライアンスの固定 IP アドレスの更新
- Horizon Cloud Connector root ユーザーのパスワード有効期限ポリシーの設定
- Horizon Cloud Connector の root パスワードまたは ccadmin パスワードのリセット
- 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
- 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
- Horizon Cloud Connector 2.4 以降：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
- Horizon Cloud Connector の DNS 設定の変更
- Horizon Cloud Connector 1.6 以降のプロキシ設定の変更
- Horizon Cloud Connector 1.5 以前のプロキシ設定の変更
- Horizon Cloud Connector 仮想アプライアンスと NTP サーバの同期
- Horizon Cloud Connector 2.0 以降：SNMP を使用したアプライアンスの監視
- Horizon ユニバーサル ライセンスの監視
- Horizon Cloud Connector 仮想アプライアンスの手動更新
- Horizon Cloud Connector 仮想アプライアンスの自動更新の構成
- Horizon Cloud Connector 仮想アプライアンスの更新のトラブルシューティング
- Horizon Cloud Connector アプライアンスのログ ファイルの収集
- Horizon Cloud Connector の既知の考慮事項
- 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 2.0 以降 - 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

この記事では、クラスタ内のプライマリ ノードとワーカー ノードで実行されている Kubernetes ポッドに依存する、Horizon Cloud Connector 2.0 以降のシステム アーキテクチャについて説明します。このアーキテクチャで、ノードの高可用性機能、および Horizon ユニバーサル ライセンスを含むコア Horizon Cloud Connector サービスのフォルト トレランス機能をサポートする方法を説明します。

バージョン 2.0 以降、Horizon Cloud Connector はデュアル ノード クラスタ、ノード レベルの高可用性、サービス レベルのフォルト トレランスに対するサポートを提供します。Horizon Cloud Connector 2.0 以降では、すべてのサービスがノード上の Kubernetes ポッドとして実行されます。

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。

Horizon Cloud Connector クラスタについて

Horizon Cloud Connector クラスタは、以下のメンバーから構成されます。

- Horizon Cloud Connector 仮想アプライアンスのプライマリ ノード
- Horizon Cloud Connector 仮想アプライアンスのワーカー ノード

最小要件として、クラスタにプライマリ ノードをメンバーとして含む必要があります。プライマリ ノードを含む既存のクラスタに対してワーカー ノードの追加と削除ができます。

プライマリ ノードについて

プライマリ ノードは、Horizon Cloud Connector クラスタの管理に必要な制御プレーン サービスを実行する Horizon Cloud Connector アプライアンスの仮想マシン (VM) です。

プライマリ ノードは、次のサービスのプライマリ インスタンスも実行します。

- Horizon Cloud Connector アプリケーション サービス。これには、アプライアンス構成ポータルにリストされている以下のサービスが含まれます。
  - Connector クライアント サービス
  - クラウド プロキシ サービス
  - Connection Server プロキシ サービス
- クラウド ブローカ クライアント サービス (CBCS)（Universal Broker をサポート）
- Connection Server 監視サービス (CSMS)
- イメージ ローカリティ サービス (ILS)（オプションの Horizon Image Management Service をサポート）
- VMware Cloud Services のエンゲージメント プラットフォームに Horizon Cloud テナントをオンボーディングした後に使用可能になったサービス。詳細については、第 1 世代テナント - Horizon Universal Console を使用して Horizon Cloud テナントを VMware Cloud Services Engagement Platform および VMware Cloud Services にオンボーディングするを参照してください。

プライマリ ノードをデプロイして Horizon ポッドとペアリングするには、Horizon Cloud テナント環境への最初のポッドとして、VMware SDDC に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に記載されているガイドラインに従ってください。

ワーカー ノードについて

ワーカー ノードは、次のサービスのレプリカ インスタンスを実行する Horizon Cloud Connector アプライアンスのセカンダリ仮想マシンです。

- Horizon Cloud Connector アプリケーション サービス。これには、Horizon Cloud Connector 構成ポータルにリストされている以下のサービスが含まれます。
  - Connector クライアント サービス
  - クラウド プロキシ サービス
  - Connection Server プロキシ サービス
- VMware Cloud Services のエンゲージメント プラットフォームに Horizon Cloud テナントをオンボーディングした後に使用可能になったサービス。詳細については、第 1 世代テナント - Horizon Universal Console を使用して Horizon Cloud テナントを VMware Cloud Services Engagement Platform および VMware Cloud Services にオンボーディングするを参照してください。

ワーカー ノードを Horizon Cloud Connector クラスタに追加することで、これらのサービスをスケール アップして、サービスのプライマリ インスタンスとレプリカ インスタンス間でロード バランシングされる増大したワークロードをサポートできます。ワーカー ノードをクラスタから削除すると、サービスはプライマリ ノードで実行されている単一インスタンスにスケール ダウンされます。

注： このリリースでは、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 インスタンスのみをサポートします。CBCS、CSMS、ILS、およびクラスタ管理サービスを含む、その他のすべてのサービスは、プライマリ ノード上で単一インスタンスとして実行されます。

ワーカー ノードをデプロイするには、Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector クラスタへのワーカー ノードの追加で説明されている手順に従ってください。ワーカー ノードをクラスタから削除するには、Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector クラスタからのワーカー ノードの削除で説明されている手順に従ってください。

ノード レベルの高可用性の概要と仕組み

詳細については、Horizon Cloud Connector 2.0 以降 - ノード レベルの高可用性の設定を参照してください。

サービス レベルのフォルト トレランスは、さまざまな停止シナリオでどのように機能しますか。

このセクションでは、さまざまな停止状態において、デュアル ノード Horizon Cloud Connector クラスタがフォルト トレランスと Horizon ユニバーサル ライセンスの継続的な可用性をどのようにサポートするかを説明します。

注： このリリースでは、前のセクションで説明したように、Horizon Cloud Connector は Horizon Cloud Connector アプリケーション サービスのフォルト トレランスのみをサポートします。その他すべてのサービスは、プライマリ ノード上で単一インスタンスとして実行され、その単一インスタンスに障害が発生した場合は使用不可になります。

1 [フレームワーク サービスに障害が発生した場合]

前述のように、Horizon Cloud Connector フレームワーク サービス（Connector クライアント サービス、クラウド プロキシ サービス、Connection Server プロキシ サービス）は、プライマリ ノードとワーカー ノードでデュアル インスタンスとして実行します。あるノードでフレームワーク サービスに障害が発生した場合、そのサービスのレプリカ インスタンスが他のノードで引き続き実行され、確実に Horizon Cloud Connector フレームワーク サービスと Horizon ユニバーサル ライセンスが完全に動作するようにします。

たとえば、プライマリ ノードでクラウド プロキシ サービスに障害が発生した場合、ワーカー ノード上のクラウド プロキシ サービスのレプリカ インスタンスが引き続き実行されます。完全に動作するフレームワーク サービスにより、Horizon Cloud ライセンス サービスは 24 時間ごとにポッドと同期し続けることができます。

2 [ワーカー ノードに障害が発生した場合]

注： この停止シナリオは、ノード レベルの HA が構成されていない場合にのみ適用されます。Horizon Cloud Connector 2.0 以降 - ノード レベルの高可用性の設定で説明したように、ノード レベルの HA を構成する場合、vSphere HA によってワーカー ノードの高可用性が確保されます。

ワーカー ノード全体の動作が失われた場合、プライマリ ノード上の単一インスタンスと Horizon ユニバーサル ライセンスが完全に動作し続けるため、すべてのサービスが中断することなく引き続き実行されます。

ワーカー ノードが完全に動作する状態に復旧するまで、Horizon Cloud Connector アプリケーション サービスは一時的にスケール ダウンします。

3 [プライマリ ノードに障害が発生した場合]

注： この停止シナリオは、ノード レベルの HA が構成されていない場合にのみ適用されます。Horizon Cloud Connector 2.0 以降 - ノード レベルの高可用性の設定で説明したように、ノード レベルの HA を構成する場合、vSphere HA によってプライマリ ノードの高可用性が確保されます。

プライマリ ノード全体の動作が失われた場合、Horizon ユニバーサル ライセンスは 25 日間の同期猶予期間に入ります。この期間中、ライセンスは有効なままとなり、ポッドは完全に動作し続けます。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。

Horizon Universal Console を使用して、ポッドの管理タスクを引き続き監視および実行できます。ただし、次の制限が適用されます。

- Horizon Cloud Connector クラスタがエラー状態になります。
- ワーカー ノードから Horizon Cloud Connector 構成ポータルにアクセスできません。
- Universal Broker、Cloud Monitoring Service、Horizon Image Management Service は一時的に使用できなくなります。

Horizon Cloud Connector 2.0 以降 - ノード レベルの高可用性の設定

この記事では、Horizon Cloud Connector アプライアンスのプライマリ ノードとワーカー ノードに高可用性 (HA) を設定する方法について説明します。ノード レベルの HA を Horizon Cloud Connector に設定するには、まず vSphere HA クラスタを作成してから、vSphere 仮想マシン監視機能を有効にする必要があります。

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。

Horizon Cloud Connector ノード レベル HA の仕組み

Horizon Cloud Connector のプライマリ ノードとワーカー ノードは、ポッドの vSphere 環境に仮想マシン (VM) としてデプロイされます。

vSphere HA 機能は、仮想マシンとそれらが常駐する ESXi ホストを vSphere HA クラスタにプール化することにより、これらの仮想マシンに高可用性を提供します。クラスタ内のホストは監視され、障害発生時には、その故障したホスト上の仮想マシンが別のホスト上で再起動されます。詳細については、vSphere HA の動作を参照してください。

vSphere は、HA クラスタに加えて、仮想マシン監視機能を提供します。VMware Tools のハートビートまたは I/O アクティビティが設定時間内に受信されない場合、仮想マシン監視機能によって各仮想マシンが再起動されます。プライマリ ノードまたはワーカー ノード仮想マシンが再起動した後、そのノードで Horizon Cloud Connector サービスが完全に動作可能になるまでに約 10 分かかることがあります。詳細については、仮想マシンとアプリケーションの監視を参照してください。

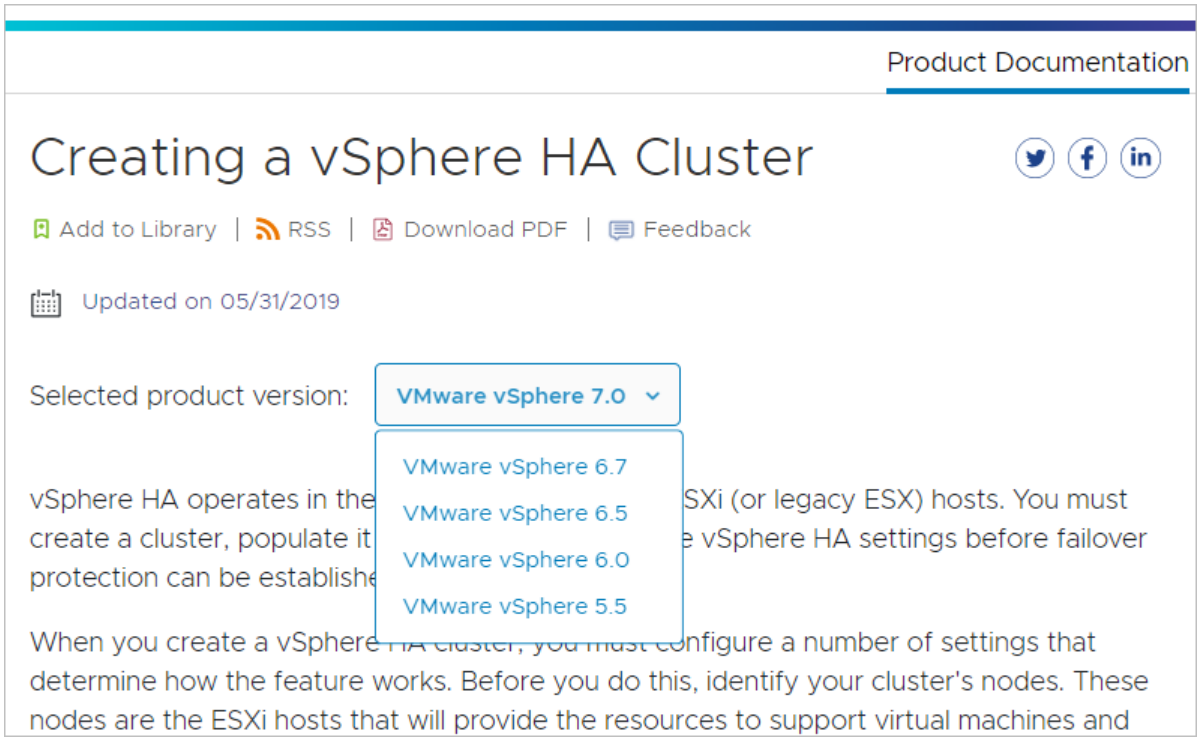
予定外のダウンタイムまたは停止が発生した場合、vSphere HA クラスタと仮想マシン監視により、Horizon Cloud Connector プライマリ ノードとワーカー ノードの高可用性が提供されます。

手順

次の手順を使用して、Horizon Cloud Connector ノード レベルの HA を設定します。

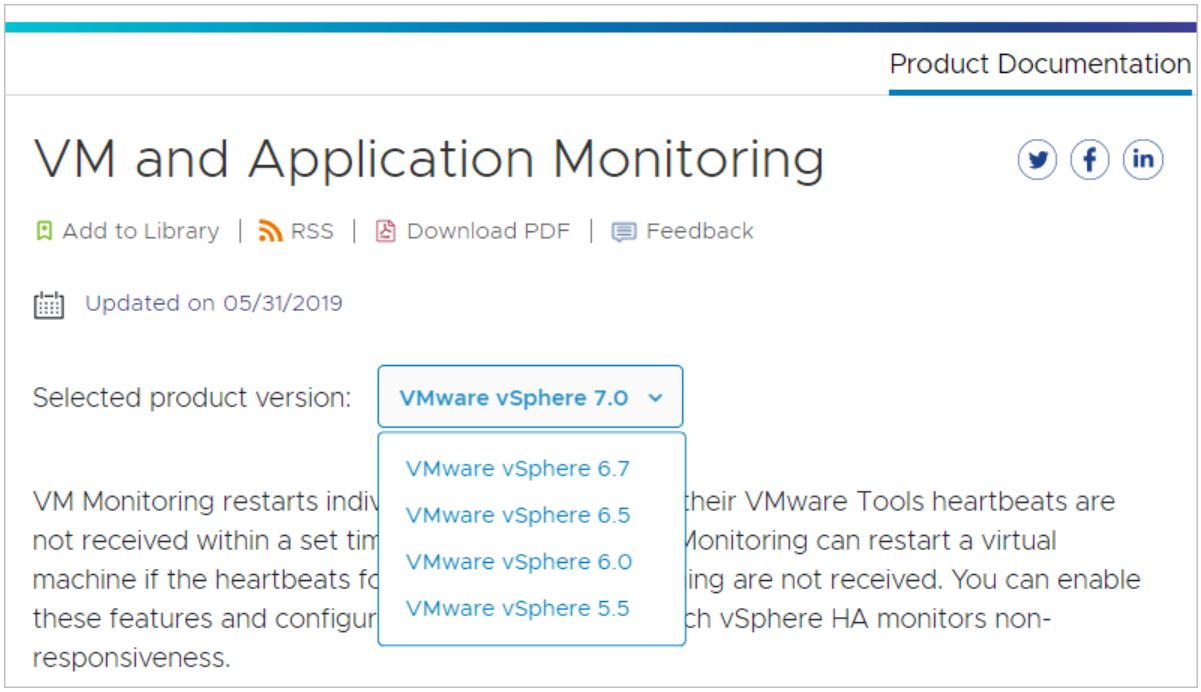
1 ポッドの vSphere 環境に vSphere HA クラスタを作成します。

詳細な手順については、vSphere HA クラスタの作成を参照してください。この記事には、vSphere 7.0 の手順が記載されています。別の vSphere バージョンの手順を確認するには、記事の上部にある [選択されている製品バージョン] メニューからそのバージョンを選択します。



2 vSphere の仮想マシン監視機能を有効にします。

仮想マシンの監視を有効にするを参照してください。ここには、vSphere 7.0 の手順が記載されています。別の vSphere バージョンの手順を確認するには、記事の上部にある [選択されている製品バージョン] メニューからそのバージョンを選択します。



注： 仮想マシン監視を構成するときに、監視感度のレベルを構成できます。監視感度を高度にすると、障害が発生したことが迅速に判断されます。監視感度を低くすると、実際に障害が発生してから仮想マシンがリセットされるまでの間、サービスが中断される時間が長くなります。ニーズに対して効果的な解決となるオプションを選択します。詳細については、仮想マシンとアプリケーションの監視を参照してください。

Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector クラスタからのワーカー ノードの削除

ワーカー ノードを Horizon Cloud Connector クラスタから削除するには、以下の手順を実行します。ワーカー ノードをクラスタから削除すると、Horizon Cloud Connector アプリケーション サービスはスケール ダウンされ、プライマリ ノードでの単一インスタンスとして実行されます。

前提条件

クラスタから削除するワーカー ノード仮想マシンの IP アドレスを取得します。

手順

1 クラスタのプライマリ ノードへの SSH セッションを開き、削除コマンドを実行します。ここでの *<WORKER_IP>* は、ワーカー ノードの IP アドレスです。

```
/opt/vmware/sbin/primary-cluster-config.sh -rs <WORKER_IP>
```

中断されることなく削除コマンドを実行できるようにします。このコマンドは、ノードからの各レプリカ サービスの削除を説明する進行状況の出力が表示されます。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 *<WORKER_IP>* と *<PRIMARY_IP>* は、それぞれワーカー ノードとプライマリ ノードの IP アドレスです。

```
Please run the following command on worker node <WORKER_IP> to complete clean up:
/opt/vmware/sbin/worker-cluster-config.sh -r <PRIMARY_IP>
```

このクリーンアップ コマンドを書き留めます。

2 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クリーンアップ コマンドを実行します。

```
/opt/vmware/sbin/worker-cluster-config.sh -r <PRIMARY_IP>
```

中断されることなくクリーンアップ コマンドを実行できるようにします。

注： コマンドは、各クリーンアップ タスクを説明する進行状況の出力を表示します。構成の手動クリアに関するメッセージは無視してもかまいません。Horizon Cloud Connector クラスタからワーカー ノードを削除する場合、手動クリーンアップは不要です。

出力の最後で、次の例のような行を探します。

```
Please restart this VM to complete the clean up.
```

3 次のいずれかの処理を行います。

- 今後、同じクラスタまたは別のクラスタにワーカー ノードを追加する場合は、ワーカー ノード仮想マシンを再起動します。次に、Horizon Cloud Connector 2.0 以降：Horizon Cloud Connector クラスタへのワーカー ノードの追加に記載されている手順に従ってください。
- クラスタ内でワーカー ノードを再度使用する予定がない場合は、ワーカー ノード仮想マシンをシャットダウンして、vSphere 環境から削除できます。

4 クラスタからのワーカー ノードの削除を検証するには、プライマリ ノード仮想マシンで次のコマンドを実行します。

```
kubectl get nodes -o wide
```

コマンド出力で、ワーカー ノードがクラスタのメンバーとしてリストされなくなっていることを確認します。

Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector ノード上のサービスのステータスの監視

この記事では、Horizon Cloud Connector クラスタのプライマリ ノードまたはワーカー ノードで実行されているサービスの健全性ステータスを表示する方法について説明します。この情報は、Horizon Cloud Connector 構成ポータルを使用して確認できます。

手順

1 Web ベースの Horizon Cloud Connector 構成ポータルを起動するための URL を取得します。

この URL は、vSphere Client を使用してノードをパワーオンした後に、ノードの青いコンソール画面に表示されます。URL は `https://<IP address>` の形式になります。ここでの *<IP address>* はプライマリ ノードまたはワーカー ノードの IP アドレスです。

2 ブラウザを使用して、プライマリ ノードまたはワーカー ノードに対し以前に取得した URL に移動します。

構成ポータルが開き、Horizon Cloud Connector コンポーネントとサービスのステータスを表示する画面になります。

構成ポータルには、クラスタのプライマリ ノードとワーカー ノードの両方で実行されているサービスの健全性ステータスが表示されます。サービスがリンクされたエントリとして表示されている場合は、エントリをクリックして、そのサービスで実行されている Kubernetes ポッドと各 Kubernetes ポッドが存在するノードに関する詳細を表示できます。

次のスクリーンショットは、構成ポータルの健全性ステータス リストの例を示しています。

3 サービスの詳細情報を表示するには、そのリンクされたエントリをクリックします。

ダイアログ ボックスが表示され、そのサービスに対して実行されている個々の Kubernetes ポッドの名前と健全性ステータス、各 Kubernetes ポッドが存在するノード、サービスが再起動された回数などの詳細が表示されます。

Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector クラスタの管理コマンド

このトピックでは、Horizon Cloud Connector クラスタ内のノードの実行中サービスとメンバーシップを確認するために使用できるコマンドをいくつか示します。

次の Kubernetes コマンドを実行するには、クラスタ内の該当するノードへの SSH セッションを開く必要があります。

クラスタ内のすべてのノードで実行されているすべてのサービスを一覧表示する

プライマリ ノードで、次のコマンドを実行します。

```
kubectl get pods -A -o wide
```

このコマンドは、クラスタのプライマリ ノードとワーカー ノードで実行されているサービスのすべてのプライマリ インスタンスとレプリカ インスタンスを返します。

クラスタ内のすべてのメンバー ノードを一覧表示する

プライマリ ノードで、次のコマンドを実行します。

```
kubectl get nodes -o wide
```

このコマンドは、クラスタのメンバーとして登録されているすべてのノードを返します。

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
```

8 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
```

9 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
```

10 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。

11 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 サム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 2.4 以降 - 送信トラフィック用に SSL オフロードを構成している場合は、Horizon Cloud Connector でカスタムの CA 署名証明書を構成して Horizon 制御プレーンへの接続を許可する

Horizon Cloud Connector アプライアンスは、Horizon 制御プレーンとの送信通信を行う必要があります。送信トラフィックに SSL オフロードを構成している場合は、Horizon Cloud Connector トラスト ストア内でカスタムの CA 署名証明書を構成し、制御プレーンへの送信接続を許可する必要があります。

この機能は、Horizon Cloud Connector バージョン 2.4 以降で使用できます。

前提条件

次のものがあることを確認します。

- SSL オフロード構成で使用しているものに応じた、有効な CA 署名証明書（複数の場合があります）。CRT と PEM の両方のファイル形式がサポートされます。

  注： 証明書が有効であることを確認します。証明書が無効な場合、コマンドは証明書をインポートしません。無効な場合、インポート プロセスは特にメッセージを表示することなくその証明書を破棄します。

手順

1 Horizon Cloud Connector 仮想アプライアンス内のディレクトリ `/opt/container-data/hydracerts/` に CA 署名証明書（複数の場合があります）をコピーします。

2 次のコマンドを実行して、証明書をインポートします。

```
/opt/vmware/bin/configure-adapter.py --importCertificates
```

このコマンドは、提供された証明書をインポートするために必要なすべての処理を実行します。ディレクトリのファイルの権限を 644 に変更し、証明書をインポートしてから、アプライアンスの関連する Kubernetes ポッドを再起動して変更を取得します。

この再起動プロセスには数分かかります。

Horizon Cloud Connector 仮想アプライアンスの固定 IP アドレスの更新

Horizon Cloud Connector 仮想アプライアンスの固定 IP アドレスに関する情報は、デプロイされた仮想アプライアンスのコンテナ ファイルに保存されます。Horizon Cloud Connector 仮想アプライアンスの固定 IP アドレスを更新する場合は、別の操作も必要になります。コンテナ設定ファイルを手動で再設定してから、ペアリングされている Horizon ポッドに関連するすべてのデスクトップに新しい固定 IP アドレスの情報を送信する必要があります。

固定 IP アドレスが格納される場所

デプロイされた Horizon Cloud Connector 仮想アプライアンスの固定 IP アドレスは、`-/opt/container-data/cc-settings/ip.conf` ファイルに保存され、アプライアンス内で実行されるコンテナと共有されます。

たとえば、固定 IP アドレスの情報は次のようにファイルに保存されます。

```
cc.address=10.117.163.20
```

プロキシ設定が保存される場所

Horizon Cloud Connector 仮想アプライアンスのプロキシ設定は、`-/opt/container-data/cc-settings/proxy.conf` に保存され、アプライアンス内で実行されるコンテナと共有されます。

たとえば、プロキシ情報は次のようにファイルに保存されます。

```
proxyHost=null
proxyPort=0
proxySsl=false
proxyUsername=null
proxyPassword=
noProxyFor=null
```

前提条件

Horizon Cloud Connector 仮想アプライアンスの新しい固定 IP アドレスを設定し、アプライアンスを Active Directory に参加させます。

手順

1. /opt/vmware/share/vami/vami_config_net を開きます。
2. IP アドレスを更新するには、[メニュー番号を入力] 行に「`6`」と入力し、Enter キーを押します。
3. [eth0 の IPv4 アドレスを構成] の横に「`y`」と入力します。
4. [DHCPv4 サーバを使用...] の横に、「`n`」と入力します。
5. 新しい IP アドレスとサブネット マスクを入力します。
6. 情報が正しいことを確認します。

7 （オプション）デフォルト ゲートウェイを更新するには、[メニュー番号を入力] 行に「2」と入力し、Enter キーを押します。表示されるフィールドの情報を更新します。

8 （オプション）DNS を更新するには、[メニュー番号を入力] 行に「4」と入力し、Enter キーを押します。表示されるフィールドの情報を更新します。

9 vami メニューを閉じます。

10 `-/opt/container-data/cc-settings/ip.conf` ファイルで、次の例に示すように `cc.address` 行を編集します。

```
cc.address=10.117.163.20
```

11 次のコマンドを使用して、Kubernetes クラスタをリセットします。

```
/opt/vmware/appliance/scripts/reset-keys.sh -r
```

```
/opt/vmware/appliance/scripts/reset-keys.sh -i
```

12 次のコマンドを使用して、アプライアンスを再起動します。

```
reboot -f
```

Horizon Cloud Connector root ユーザーのパスワード有効期限ポリシーの設定

Horizon Cloud Connector OVA を vSphere 環境にデプロイする場合、デプロイ プロセスで root ユーザーのパスワードを設定する必要があります。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、ユーザーのセキュリティ 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、root パスワードを定期的に更新する必要があります。

注： Horizon Cloud Connector 仮想アプライアンスにログインした後に、root ユーザーとしてすべてのコマンドを入力する必要があります。パスワード有効期限ポリシーを独自に設定している場合、管理者が定期的にログインし、有効期限が切れる前にパスワードを更新する必要があります。Horizon Cloud Connector 仮想アプライアンスは、パスワードの有効期限を管理者に通知しません。

手順

1 root ユーザーのパスワード有効期限ポリシーを設定をするには、次のコマンドを入力します。

```
chage -M <Max days before password change> -W <Number of days of warning before password expires> root
```

たとえば、パスワードを変更してから 365 日後にパスワードを期限切れにし、パスワードの有効期限の 30 日前から警告を表示するようにするには、次のコマンドを入力します。

```
chage -M 365 -W 30 root
```

2 root ユーザーの現在のパスワード有効期限ポリシーを表示するには、次のコマンドを入力します。

```
chage -l root
```

Horizon Cloud Connector の root パスワードまたは ccadmin パスワードのリセット

元のパスワードを紛失した場合、または変更する場合は、このトピックの手順を使用して、Horizon Cloud Connector アプライアンスの `root` または `ccadmin` ユーザーのパスワードをリセットします。

Horizon Cloud Connector の root パスワードをリセットする

`root` のパスワードをリセットするには、アプライアンスの再起動シーケンスで特定のパラメータを設定する必要があります。

1 vSphere Client を使用して、Horizon Cloud Connector 仮想アプライアンスのコンソールを起動します。コンソール ウィンドウ内をクリックして、コンソールでカーソルをアクティブにします。

2 vSphere Client を使用して、アプライアンスを再起動します。OS のスプラッシュ画面が表示されたら、**e** を入力して GNU GRUB エディタを開きます。

注： OS のスプラッシュ画面は瞬間的に表示されるため、すばやく **e** を入力する必要があります。GNU GRUB エディタを開くことができない場合は、アプライアンスを再起動して再試行してください。

3 GNU GRUB エディタで、`linux` で始まる行を見つけます。この行の最後にスペースを追加し、その後に `rw init=/bin/bash` を追加します。

次のスクリーンショットは、行を変更した後の GNU GRUB エディタの例を示しています。

4 F10 を押して、アプライアンスの再起動を再開します。

5 コマンド プロンプトで、次のコマンドを実行します。

```
pam_tally2 --user=root --reset
```

6 コマンド プロンプトで、`passwd` を入力します。新しい `root` パスワードを入力し、もう一度入力します。

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。

パスワードのリセットが完了すると、次の出力が表示されます。

```
passwd: password updated successfully
```

7 次の一連のコマンドを実行します。

```
umount /
reboot -f
```

アプライアンスが再起動した後、新しい `root` パスワードを使用してログインできます。

Horizon Cloud Connector の ccadmin パスワードをリセットする

ccadmin ユーザーとしてログインできない場合は、次の手順を使用して ccadmin のパスワードをリセットします。たとえば、認証エラーが複数回発生すると、ccadmin アカウントは自動的にロックされます。

1 vSphere Client を使用して Horizon Cloud Connector 仮想アプライアンスのコンソールを起動し、root ユーザーと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ます。

```
pam_tally2 --user=ccadmin --reset
```

3 ccadmin アカウントの新しい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。

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

Horizon Cloud Connector アプライアンスが Horizon ポッドと正常にペアリングされたら、ブラウザベースの Horizon Cloud Connector 構成ポータルを使用して、アプライアンスの SSH 設定を有効または無効にすることができます。バージョン 1.5 以降のアプライアンスでは、SSH がデフォルトでアプライアンスのオペレーティング システムでオフになっています。

これらの手順は Horizon Cloud Connector バージョン 1.5 以降に適用されます。

注： （Horizon Cloud Connector 2.0 以降）これらの手順を使用して、プライマリ ノードへの SSH アクセスのみを有効にできます。ワーカー ノードへの SSH アクセスを有効にするには、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 アクセスの有効化に記載されている手順を代わりに実行する必要があります。

前提条件

次の項目が適切であることを確認します。

- アプライアンスが Horizon ポッドと正常にペアリングされていること。Horizon Cloud Connector アプライアンスが Horizon ポッドと正常にペアリングされている場合にのみ、トグルがある構成ポータル画面にアクセスできます。コネクタをポッドとペアリングする前に、vSphere 環境を使用してアプライアンス コンソールを起動してログインし、コマンド ラインを使用してアプライアンスの SSH を有効または無効にすることができます。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トピックを参照してください。
- Horizon Cloud テナント環境への管理者アクセス権を持つ My VMware 認証情報があること。これらの認証情報は、Horizon Cloud Connector 構成ポータルにログインするために必要です。

- Active Directory ドメインが Horizon Cloud テナント環境に登録されている場合、Horizon Cloud スーパー管理者ロールを持つグループに属する Active Directory アカウントの認証情報が必要です。Active Directory ドメインが Horizon Cloud テナントに登録されている場合、My VMware 認証情報を入力すると 2 番目のログイン画面が表示されます。構成ポータルにアクセスするには、続いて Active Directory アカウントの認証情報を入力する必要があります。Active Directory ドメインが Horizon Cloud テナントに登録される方法およびスーパー管理者ロールの詳細については、第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行および Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるを参照してください。
- ブラウザに構成ポータルを表示する URL アドレスがあること。構成ポータルのログイン画面を表示するには、ブラウザで次のいずれかを指定します。
  - Horizon Cloud Connector アプライアンスの IP アドレス（`https://IP-address/`）
  - DNS サーバで、完全修飾ドメイン名 (FQDN) を IP アドレスにマップする正引きおよび逆引きレコードを作成した場合、その FQDN
- （Horizon Cloud Connector 1.9 以降）`ccadmin` ユーザーの認証に必要な SSH パブリック キーを、次のいずれかの方法で準備していること。
  - 『デプロイ ガイド』のオンプレミスまたは VMware Cloud on AWS にある Horizon ポッド：ポッドの vSphere 環境に Horizon Cloud Connector をダウンロードしてデプロイでの説明に従って、Horizon Cloud Connector OVA ファイルのデプロイ中に SSH パブリック キーを登録済みであること。
  - SSH パブリック キーを生成したが、未登録であること。SSH パブリック キー認証の設定を完了するには、Horizon Cloud Connector 構成ポータルにキーを登録するオプションがあります。

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。

手順

1 前提条件の説明に従って、ブラウザに Horizon Cloud Connector 構成ポータルの URL をロードし、テナント環境で有効な My VMware 認証情報を使用してログインします。

Active Directory ドメインがそのテナント環境に登録されている場合、システムは 2 番目のログイン画面を表示します。前提条件の説明に従って、スーパー管理者ロールを持つ Active Directory アカウントの認証情報を入力します。

構成ポータルに、コネクタ上の管理タスクのアクション ボタンを表示する画面が開きます。

2 次のいずれかの処理を行います。

- （Horizon Cloud Connector 1.5 から 1.8 まで）[SSH を有効にする] トグルを使用してアプライアンスで SSH を有効または無効にします。

  ポータルに表示されるトグルの設定は、アプライアンスの SSH の現在のステータスです。

- （Horizon Cloud Connector 1.9 以降）SSH 構成コントロールにアクセスするには、アプライアンス構成ポータルで [SSH の構成] をクリックします。

SSH の構成ダイアログ ボックスが表示されたら、コントロールを使用して、アプライアンスで SSH を有効または無効にし、以前に生成した SSH パブリック キーを登録します。SSH を初めて有効にする場合、またはすでに登録されているキーを変更する場合は、パブリック キーを登録する必要があります。

ダイアログ ボックスに表示されるトグルの設定は、アプライアンスの SSH の現在のステータスです。

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

このドキュメント ページでは、Active Directory システムで Horizon Connection Server 管理者のパスワードをローテーションする場合に使用する API について説明します。この使用事例では、この API を使用して Horizon Cloud Connector で新しい値を使用します。

この機能は、Horizon Cloud Connector バージョン 2.4 以降で使用できます。

Horizon Cloud Connector は、オンボーディングおよびペアリング プロセス中に入力された管理者認証情報を使用して Horizon Connection Server と通信します。

時間の経過とともに、それらの管理者資格情報は Active Directory ドメインで変更されたり、期限切れになったり、無効になったりする可能性があります。Active Directory ドメインで管理者認証情報が更新されたときに Horizon Cloud Connector アプライアンスに新しい認証情報が通知されない場合、Horizon Cloud Connector は Horizon Connection Server との接続を失います。

管理者のパスワードを更新する必要がある場合は、この API を使用して、アプライアンスに保存されている管理者パスワードを更新し、Active Directory ドメイン アカウントで構成された値と一致させることができます。

API エンドポイント

保存されたパスワードを更新するためのアプライアンス エンドポイントは、`https://appliance-address/viewproxyadapter/local/config/rotate` です

ここで、*appliance-address* は以下のいずれかです。

- `https://IP-address/viewproxyadapter/local/config/rotate`。ここで、`IP-address` はアプライアンスの IP アドレスです。
- `https://FQDN/viewproxyadapter/local/config/rotate`。これは、アプライアンスの IP アドレスを DNS サーバの FQDN にマッピングした場合です。

API メソッド

`PUT`

要求ペイロード

ペイロードには、Active Directory DNS ドメイン名、アカウント名、アプライアンスに保存されているパスワード（以前のパスワード）、および新しいパスワードが必要です。

パスワードは、各文字を引用符で囲み、囲んだ文字をカンマで区切ります。以下の例では、アプライアンスに保存されているパスワードが **abcd!efg** で、**tuvw$xyz** が新しいパスワードです。

```
{
   "domain":"AD-dns-domain-name",
   "userName":"admin-account-name",
   "oldPassword":["a","b","c","d","!","e","f","g"],
   "newPassword":["t","u","v","w","$","x","y","z"]
}
```

API が呼び出されたとき

Horizon Cloud Connector は、API ペイロードで指定した既存の認証情報を Horizon Cloud Connector アプライアンスに保存されている認証情報と比較します。

検証が成功すると、システムは API ペイロードで提供された新しい認証情報を使用して Horizon Connection Server へのログインを試みます。

ログインの試行に成功すると、アプライアンス内のサービスが再ロードされ、新しい認証情報を取得して使用を開始します。

注： この API は、1 分あたり 1 回の要求にレート制限されます。試行回数がレート制限を超えると、HTTP エラー 429（要求が多すぎます）が返されます。

API の承認

承認チェックは、要求ペイロードで提供された `domain`、`userName`、および `oldPassword` を Horizon Cloud Connector で知られている認証情報と比較することによって行われます。既知の認証情報は、オンボーディングおよびペアリング プロセス中に提供されたものか、この API を使用した以前の認証情報のローテーション中に提供されたもののいずれかです。

前提条件

API コマンドを発行する前に、次の項目を確認します。

- Horizon Cloud Connector が、Horizon ポッドと、ポッドの Horizon Connection Server とペアリングされていること。
- Active Directory ドメインの DNS 名と Horizon Connection Server 管理者の認証情報を持っていること。
- Active Directory ドメインで、Horizon Connection Server 管理者アカウントのパスワードが使用する新しいパスワードに更新されていること。
- 以前に使用したパスワード（Horizon Cloud Connector アプライアンスが現在使用している、アプライアンスで認識された既存のパスワード）があること。

手順

- 要求ペイロードを使用して、API エンドポイント `https://appliance-address/viewproxyadapter/local/config/rotate` に `PUT` を発行します。

  次の例では、AD ドメインは `example.com`、アカウントの名前は `CSadmin`、以前のパスワードは **`abcd!efg`**、新しいパスワードは **`tuvw$xyz`** です。

```
{
   "domain":"example.com",
   "userName":"CSadmin",
   "oldPassword":["a","b","c","d","!","e","f","g"],
   "newPassword":["t","u","v","w","$","x","y","z"]
}
```

  パスワードが正常にローテーションされると、返される応答は `200 success` になります。

次のステップ

Horizon Cloud Connector が更新されたパスワードを使用して Horizon Connection Server に接続していることを確認するには、Horizon Cloud Connector 構成ポータルにログインし、更新矢印をクリックして、Connection Server のステータスが緑色で表示されることを確認します。

Horizon Cloud Connector 2.4 以降：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

このドキュメント ページでは、Horizon Cloud Connector で使用される Kubernetes 証明書の有効期限チェックについて説明します。有効期限の 2 か月前に有効期限の警告が表示され、システムが証明書を自動的に更新される仕組みを確認できます。

概要

ナレッジベースの記事 KB90505 で説明されているように、デプロイされた Horizon Cloud Connector には、Horizon 制御プレーンとの安全な通信と接続に使用されるシステム生成の証明書を備えた内部 Kubernetes クラスタがあります。これらのシステム生成の証明書の有効期間は 1 年です。

システム生成の証明書が更新前に有効期限に達して、制御プレーンとのアプライアンスの通信が中断されないようにするために、バージョン 2.4 以降では、Horizon Cloud Connector アプライアンスは次の機能を提供します。

- アプライアンスの Kubernetes 証明書の有効性の週単位の自動チェック
- 有効期限までの現在の日数を画面上に表示。
- 有効性チェックにより証明書の有効期間が 60 日未満と判断された場合、証明書を自動更新。更新プロセス中はアプライアンスのサービスに短いダウンタイムが発生するため、システムの自動更新プロセスは、アプライアンスのローカル時間に従って週末の深夜にのみ実行されます。更新された証明書は、1 年間有効です。

システムの有効性チェック

アプライアンスは、アプライアンスのローカル時間に従って、毎週土曜日と日曜日の深夜に有効性をチェックします。

有効性チェックでは、Kubernetes クラスタの証明書の有効期限が切れるまでの残り日数を評価します。証明書の有効期間が 60 日未満になると、システムは自動的に証明書を更新し、有効期間が 1 年間の新しい証明書を発行します。

画面上の情報を表示すると、ステータスがリアルタイムで計算されます。たとえば、情報を水曜日などの平日に表示すると、その水曜日から有効期限までの残り日数がユーザー インターフェイスに表示されます。

画面の情報は、有効期限までの残り日数に応じたパターンに従います。

残り 120 日以上 - 緑（良好）

画面の情報には、証明書が有効な日数が表示されます。例：`364` **日間有効。**

残り 120 ～ 60 日 - オレンジ（警告）

8 か月が経過すると、画面の情報には、有効期限までの日数と、システムの自動更新より前に証明書を更新するために実行できる更新手順が記載されたナレッジベースの記事 KB90505 へのリンクが表示されます。

更新プロセスによりアプライアンスとそのサービスに短いダウンタイムが発生する可能性があるため、有効期間が 60 日未満になるまで待つのではなく、ナレッジベースの記事の手順に従って証明書を自分で更新することを選択できます。証明書を自分で更新すると、この短いダウンタイムが発生する日時を決めることができます。ナレッジベースの記事に記載されているように、手順にはアプライアンスの再起動が含まれており、すべてのサービスが再初期化されるまでに数分かかる場合があります。

残り 60 日未満 - 赤（エラー）

有効期間が 60 日未満になると、画面の情報には、有効期限までの日数と、システムの自動更新より前に証明書を更新するために実行できる更新手順が記載されたナレッジベースの記事 KB90505 へのリンクが表示されます。

次回システムの有効性チェックが実行され、証明書の有効期間が 60 日未満であると判断されると、システムは自動的に証明書を更新し、新しい証明書を発行します。自動更新では、新しい証明書の有効期間は 1 年間です。

画面上の情報の位置

画面上の有効性情報は、次の場所で表示できます。

- Horizon Cloud Connector 構成ポータルの [Cloud Connector の健全性] リストで、[Kubernetes 証明書] の行の横にあるアイコンにカーソルを合わせると、画面上のメッセージが表示されます。
- 第 1 世代のテナント環境で Active Directory ドメインの登録手順が完了している場合は、Horizon Universal Console の [キャパシティ] ページを使用してポッドの詳細ページに移動し、そのユーザー インターフェイス ページのアイコンにカーソルを合わせることができます。

Horizon Cloud Connector の DNS 設定の変更

DNS サーバの構成が変更された場合は、更新された DNS サーバを含めるように Horizon Cloud Connector アプライアンスのネットワーク設定を変更する必要があります。

Photon OS 上で実行される Horizon Cloud Connector などのアプライアンスの DNS 設定の変更の詳細については、DNS サーバの追加ドキュメントを参照してください。

手順

- 固定 IP アドレスを使用して Horizon Cloud Connector をデプロイした場合は、次の手順を実行します。
  a アプライアンスで、`/etc/systemd/network/10-eth0.network` ファイルを開いて編集します。
  b このファイルの [ネットワーク] セクションに新しい DNS サーバをエントリとして追加します。
  c アプライアンスを再起動します。
- 動的 IP アドレスを使用して Horizon Cloud Connector をデプロイした場合：
  a アプライアンスで、`/etc/resolv.conf` ファイルを開いて編集します。
  b このファイルに新しい DNS サーバをエントリとして追加します。
  c アプライアンスを再起動します。

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]] ...
```

コマンドの使用方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

引数	説明
`--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 1.5 以前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。デプロイ後にプロキシ設定を変更する場合や、プロキシなしのホストを構成する場合は、特定の構成ファイルを変更する必要があります。既知の制限により、Horizon Cloud Connector 1.5 以前ではデプロイ中に指定されたプロキシなしのホスト構成が考慮されません。プロキシなしのホストを構成するには、デプロイ後に特定の構成ファイルを変更する必要があります。

重要： 既知の制限により、Universal Broker と Horizon Cloud Connector 1.5 を使用する予定があり、現在の環境でプロキシ設定を使用する必要がある場合は、OVF テンプレートをデプロイするときにそれらのプロキシを設定する必要があります。Universal Broker は、デプロイ後に構成されたプロキシ設定を認識しません。プロキシなしのホストはデプロイ後にのみ構成できるため、この制限により、Universal Broker でのプロキシなしのホストの使用が Horizon Cloud Connector 1.5 でサポートされていないことになります。

Horizon Cloud Connector 1.5 以前でのプロキシなしのホストの構成

Horizon Cloud Connector OVF テンプレートのデプロイ時に、デプロイ ウィザードでプロキシなしのホストを構成するためのプロンプトが表示されます。ただし、既知の問題により、Horizon Cloud Connector 1.5 以前ではデプロイ中に指定されたプロキシなしのホスト構成が考慮されません。代わりに、デプロイ後に特定の構成ファイルを変更して、プロキシなしのホストを設定する必要があります。

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。少なくとも、ペアリングされたポッドの Connection Server と vCenter Server インスタンスをプロキシなしのホストとして構成します。

注： Horizon Cloud Connector 1.5 以前を新しいバージョンに更新する場合は、プロキシなしのホストを再構成する必要があります。元のプロキシなしのホスト構成は、アプライアンスの更新後に引き継がれません。

仮想アプライアンスをデプロイした後でのプロキシなしのホストの構成の詳細については、VMware ナレッジベースの記事 KB76663「Horizon Cloud Connector のプロキシ設定の問題と修正」を参照してください。

Horizon Cloud Connector 1.5 または 1.4 以前のプロキシ設定の変更

アプライアンスをデプロイした後に Horizon Cloud Connector 1.5 または 1.4 の HTTP プロキシ設定を変更するには、次の手順を実行します。

1 デプロイされた Horizon Cloud Connector 仮想アプライアンスへの Secure Shell (SSH) セッションを開きます。

2 必要に応じて次のファイルでプロキシの詳細を変更します。

- `/opt/container-data/cc-settings/proxy.conf`
- `/opt/container-data/data/hze-core/properties/hydra.properties`
- `/opt/container-data/data/hze-ccc/config/ccc-core/sn.config`

3 必要なサービスを再起動します。

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

Horizon Cloud Connector 1.3 以前のプロキシ設定の変更

アプライアンスをデプロイした後に Horizon Cloud Connector 1.3 以前 HTTP プロキシ設定を変更するには、次の手順を実行します。

1 デプロイされた Horizon Cloud Connector 仮想アプライアンスへの Secure Shell (SSH) セッションを開きます。

2 必要に応じて次のファイルでプロキシの詳細を変更します。

- `/opt/vmware/var/lib/tomcat8/properties/hydra.properties`
- `/opt/vmware/var/lib/tomcat8/properties/sn.config`

3 必要なサービスを再起動します。

```
systemctl restart tomcat8
systemctl restart cccService
```

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。
  a 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。

  b 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。

  a 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。

  b `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
  ```

  c 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。

  d 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
  ```

e 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
```

f 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。

Horizon Cloud Connector 2.0 以降：SNMP を使用したアプライアンスの監視

この記事では、Horizon Cloud Connector アプライアンスの簡易ネットワーク管理プロトコル (SNMP) の設定を有効にして構成する方法について説明します。この構成により、ネットワーク管理システムを介して主要な Horizon Cloud Connector イベントを監視できます。

この機能を使用するには、Horizon Cloud Connector 2.0 以降が稼動している必要があります。

Horizon Cloud Connector での SNMP 監視の仕組み

Horizon Cloud Connector は、特定のイベントが発生したときにアプライアンスから発生する SNMP トラップの使用による監視をサポートします。これらのトラップは、ネットワーク管理システムにトリガ イベントや条件を通知します。

注： Horizon Cloud Connector はトラップ エミッタとしてのみ機能し、`GET`、`GETBULK`、`GETNEXT` の操作の受信など、その他の SNMP 操作はサポートしません。

デフォルトで、Horizon Cloud Connector では SNMP サービスは無効になっています。SNMP トラップを使用するには、この記事の後半で説明するように、まず アプライアンスの SNMP サービスを有効にして構成する必要があります。

MIB（Management Information Base）ファイルでは、管理対象デバイスから提供可能な情報を定義する、トラップ定義が含まれています。MIB ファイルには、オブジェクト識別子 (OID) 別に記述された管理対象オブジェクトと階層別に整理された変数が定義されています。この記事の後半で提供するリンクを使用して、必要な MIB ファイルをダウンロードできます。

SNMP トラップで監視できる Horizon Cloud Connector イベント

アプライアンスの SNMP サービスを有効にして構成すると、Horizon Cloud Connector は以下のイベントの SNMP トラップをサポートします。

- Horizon サブスクリプション ライセンス（別称：Horizon ユニバーサル ライセンス）の同期の失敗
- 以下のような、Horizon Cloud Connector 構成に影響するライフサイクル イベント
  - Horizon ポッドとペアリングするためのアプライアンスの構成または再構成
  - 新しい Horizon Cloud Connector ソフトウェア バージョンへの更新
  - Horizon ポッドからのアプライアンスの取り外し

これらのイベントのいずれかにより、アプライアンスからネットワーク管理システムへの SNMP トラップの送信がトリガされます。

Horizon Cloud Connector の SNMP 監視の構成方法

SNMP 構成プロセスの手順全体の概要は以下のとおりです。

- 手順 1：ネットワーク管理システムで使用する VMware MIB ファイルをダウンロードします。
- 手順 2：ネットワーク管理システムで、Horizon Cloud Connector エンジン ID を構成します。
- 手順 3：Horizon Cloud Connector 構成ポータルで SNMP サービスを有効にして構成します。

各手順の詳細については、以降のセクションを参照してください。

手順 1：VMware MIB ファイルと OID のダウンロード

管理情報の構造 (SMI) に関する RFC 2578 標準は、特定の製品および機能の管理情報ベース (MIB) ファイルの記述に使用される構文です。これらの MIB ファイルは、製品とは別にバージョン管理され、イベント タイプおよびイベント データ関連情報の識別に使用できます。

これらの MIB ファイルをダウンロードするには、VMware ナレッジベースの記事 KB1013445 を参照してください。

MIB ファイルで使用されるオブジェクト識別子 (OID) をダウンロードするには、VMware ナレッジベースの記事 KB2054359 を参照してください。

手順 2：管理システムでの Horizon Cloud Connector エンジン ID の構成

SNMP の有効化プロセス中に、ネットワーク管理システムで使用する一意の SNMP エンジン ID が、Horizon Cloud Connector によって自動生成されます。エンジン ID は、ハッシュ機能によって、SNMP v3 メッセージの認証と暗号化のための鍵を生成するために使用されます。

1 Horizon Cloud Connector 構成ポータルを起動するには、ブラウザで `https://<appliance IP>` を指定します。ここでの *<appliance IP>* はアプライアンス ノードの IP アドレスまたは FQDN です。

2 構成ポータルで、Horizon Cloud Connector の構成ステータス リストの下に表示される SNMP エンジン ID を見つけます。

次のスクリーンショットの例で、構成ポータルに表示される自動生成された SNMP エンジン ID を示しています。

3 ネットワーク管理システムで、SNMP エンジン ID を適切な構成ページに追加します。

手順 3：Horizon Cloud Connector SNMP サービスの有効化と構成

SNMP サービスの設定には、Horizon Cloud Connector 構成ポータルからアクセスできます。

1 Horizon Cloud Connector 構成ポータルを起動するには、ブラウザで `https://<appliance IP>` を指定します。ここでの *<appliance IP>* はアプライアンス ノードの IP アドレスまたは FQDN です。

2 構成ポータルの上部で、[SNMP の構成] をクリックします。

SNMP 構成のダイアログ ボックスが表示されます。次のスクリーンショットで、最初に表示されたときのダイアログ ボックスの例を示しています。

3 [SNMP を有効にする] トグルをオンに切り替えます。

4 SNMP のバージョン、ユーザー名、およびセキュリティ レベルの設定を、次の表の記載どおりに指定します。

設定	説明
[SNMP エンジン ID]	この読み取り専用設定には、Horizon Cloud Connector の自動生成された SNMP エンジン ID が表示されます。
[SNMP バージョン]	この設定では、使用する SNMP のバージョンを指定できます。このリリースでは、SNMP v3 のみがサポートされます。
[SNMPv3 USM ユーザー]	SNMP 監視情報にアクセスできる、SNMPv3 USM（ユーザーに基づくセキュリティ モデル）のユーザーを構成します。ユーザー名は、8 文字から 31 文字の長さで、英数字のみを使用する必要があります。
[SNMPv3 セキュリティ レベル]	SNMP サービスで、プライバシー アルゴリズムの有無にかかわらず、オプションの認証アルゴリズムを使用するかどうかを指定します。認証は、ユーザーの ID を確認するために使用します。プライバシーを使用すると、SNMP v3 メッセージを暗号化してデータの機密性を保証できます。 認証およびプライバシーは、どちらもオプションです。ただし、プライバシーを有効にするには、認証を有効にする必要があります。

5 （オプション）認証を含むセキュリティ レベルを指定した場合は、次の表の記載内容に従って認証の詳細を構成します。

設定	説明
[SNMPv3 認証アルゴリズム]	SNMP ユーザーの ID を確立するために使用する認証アルゴリズムを指定します。
[SNMPv3 認証パスワード]	ユーザーの ID を確立するための認証アルゴリズムに必要なパスワードを構成します。認証パスワードの長さは 8 文字から 31 文字までにする必要があります。
[認証パスワードの確認]	認証パスワードを再入力します。

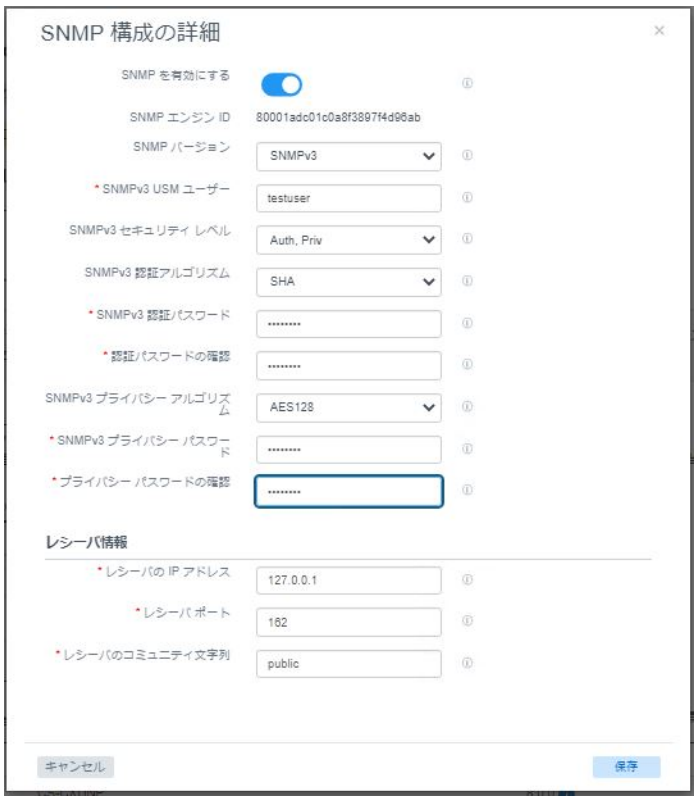
6 （オプション）認証とプライバシーの両方を含むセキュリティ レベルを指定した場合は、次の表の記載内容に従ってプライバシーの詳細を構成します。

設定	説明
[SNMPv3 プライバシー アルゴリズム]	SNMP メッセージの暗号化に使用するプライバシー アルゴリズムを指定します。
[SNMPv3 プライバシー パスワード]	暗号化キーを生成するためのプライバシー アルゴリズムに必要なパスワードを構成します。プライバシー パスワードの長さは 8 文字から 31 文字までにする必要があります。
[プライバシー パスワードの確認]	プライバシー パスワードを再入力します。

7 次の表の説明に従って、Horizon Cloud Connector から SNMP トラップを受信できる、ネットワーク管理システムの詳細を指定します。

設定	説明
[レシーバの IP アドレス]	SNMP トラップを受信できる、ネットワーク管理システムの IP アドレスを指定します。
[レシーバ ポート]	トラップを受信するためのネットワーク管理システムが使用するポート番号を指定します。
[レシーバのコミュニティ文字列]	受信したトラップが Horizon Cloud Connector から発生していることを検証するために、ネットワーク管理システムが使用するコミュニティ文字列を入力します。

次のスクリーンショットは、設定が構成された [SNMP の詳細] ダイアログ ボックスの例を示しています。



8　SNMP サービスの構成が完了したら、変更を保存します。

SNMP サービスの構成を変更すると、coldStart システム トラップが必ず生成されます。Horizon Cloud Connector フレームワーク サービスが再起動すると、warmStart トラップが生成され、ネットワーク管理システムに送信されます。

Horizon ユニバーサル ライセンスの監視

Horizon サブスクリプション ライセンス（別名：Horizon ユニバーサル ライセンス）は、Horizon ポッドのデプロイ、Horizon Cloud Connector、Horizon Cloud ライセンス サービスの間の正常に動作する通信チェーンに依存します。ライセンス サービスは 24 時間ごとに Horizon ポッドと同期します。Horizon Universal Console を使用して、サブスクリプション ライセンスのステータスを監視し、発生する可能性のある同期の問題をトラブルシューティングできます。

ライセンス通信チェーン内のいずれかのリンクが動作できなくなっている場合、ライセンスの同期は失敗し、Horizon ポッドは同期猶予期間に入ります。この期間中もサブスクリプション ライセンスは有効であり、ポッドは動作可能なままなので、同期エラーの原因を調査して修正するための時間があります。同期猶予期間が終了してもエラーが続く場合、ポッドへのサービスが中断され、ポッドが動作できなくなります。同期猶予期間が切れると、エンド ユーザーはポッド上のリモート デスクトップとアプリケーションに接続できなくなります。

この猶予期間の具体的な長さを、製品ドキュメントで公開することは認められていません。特定のテナント レコードの猶予期間を確認するには、サポート リクエストを発行してください。

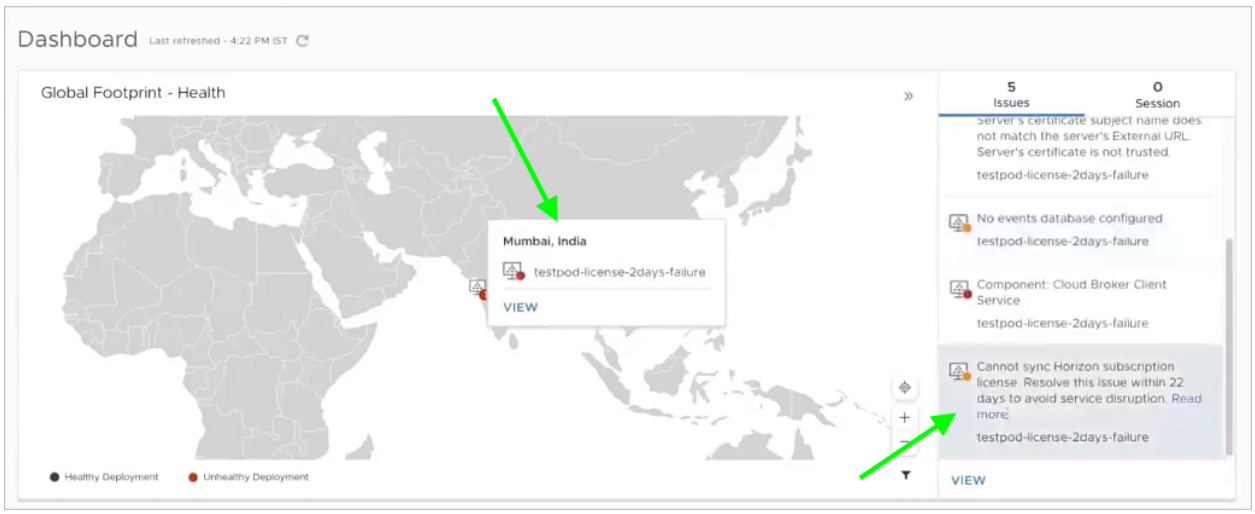
同期エラーが発生した場合に通知するため、以降のセクションで説明するように、コンソールのさまざまな領域にアラート メッセージが表示されます。

[ダッシュボード] ページのサブスクリプション ライセンスのステータス

[ダッシュボード] ページでは、次のように、サブスクリプション ライセンスの同期エラーがレポートされます。

- 対話式のグローバル フットプリント マップで、マップのポッド アイコンの上にマウスを移動すると、ポッドでライセンスの同期エラーが発生していることが示されます。
- [問題] タブには、サブスクリプション ライセンスの同期に関連するエラーがあると一覧表示されます。問題の項目の [詳細を読む] リンクをクリックすると、VMware のナレッジベース記事 KB79509 に直接移動します。. このナレッジベース記事には、ライセンスの同期に失敗の原因となる一般的なエラーのトラブルシューティングに関する詳細なガイドラインがあります。

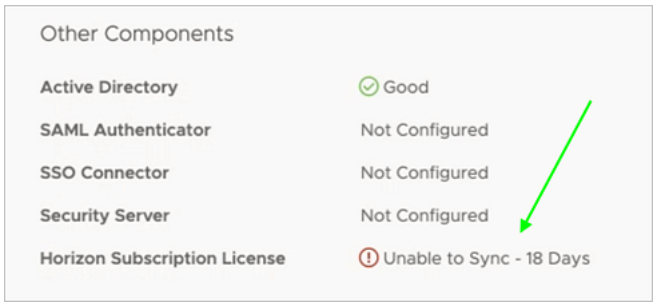
次のスクリーンショットは、ライセンス同期エラーのステータスをレポートしている [ダッシュボード] ページの例を示しています。



[キャパシティ] ページのサブスクリプション ライセンスの健全性ステータス

[設定] - [キャパシティ] にあるポッドの詳細ページでは、ポッドのサブスクリプション ライセンスのステータスを表示できます。

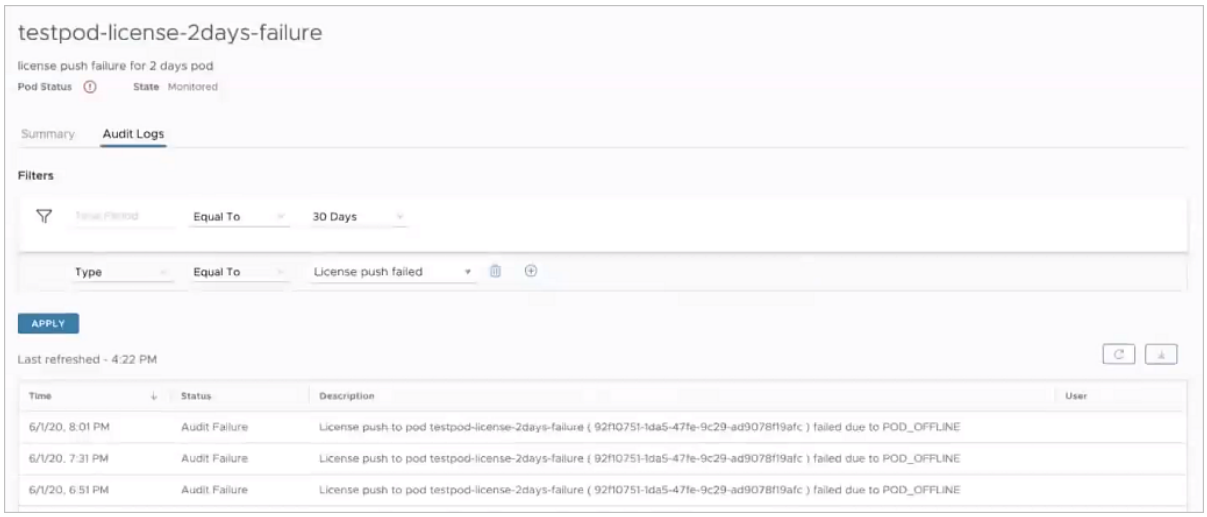
1 ポッドの詳細ページで、[健全性] - [その他のコンポーネント] の下にある Horizon サブスクリプション ライセンスの健全性ステータスを表示します。次の例は、同期の問題が発生しているライセンスの健全性ステータスを示しています。



2 ライセンス同期エラーの詳細を表示するには、健全性ステータスのテキストをクリックします。

コンソールではそのポッドの [監査ログ] ページに移動され、過去 30 日間のライセンス同期イベントのログを表示するフィルタが自動的に設定されます。ログでは、ライセンスが利用できなくなってからの日数と、同期エラーの考えられる原因がレポートされます。

次の例は、Horizon ポッドのオフライン状態により同期に失敗したライセンスのログ レポートを示しています。



3 必要なアクションを実行して、ライセンスの同期が失敗する原因となったエラーを解決します。

一般的なエラーのトラブルシューティングに関する詳細なガイドラインについては、VMware のナレッジベース記事 KB79509 を参照してください。

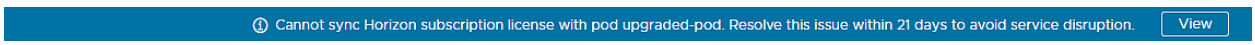
サブスクリプション ライセンスのアラート バナー

同期猶予期間の最初の 4 日間が経過すると、コンソール ウィンドウの上部にアラート バナーが目立つように表示されます。バナーに示されているように、サービスの中断を回避するため、同期猶予期間が切れる前にライセンスの同期エラーを解決する必要があります。

アラート バナーは、同期猶予期間の残り時間の緊急度レベルに従って色分けされます。

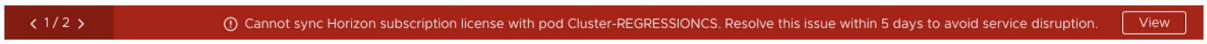
アラート バナーの色	同期猶予期間の残り時間
青	21 ～ 15 日
オレンジ	14 ～ 8 日
赤	7 ～ 1 日 同期猶予期間が切れると、赤色のバナーには、残り 0 日でサービスが中断されたことを示すメッセージが表示されます。

次のスクリーンショットは、ライセンスの同期に失敗して同期猶予期間の残りが 21 日の場合にアラート バナーがどのように表示されるかの例を示しています。



アラート バナーからは次のアクションを実行できます。

- サブスクリプション ライセンスの同期エラーが複数のポッドで発生している場合、次のスクリーンショットで例示するとおり、アラート バナーの左端にスクロール ボタンが表示されます。スクロール ボタンをクリックすると、影響を受けているすべてのライセンスのアラートが表示されます。



- バナーの [表示] ボタンをクリックして、影響を受けているポッドの詳細ページに直接移動します。複数のポッドが同じ同期猶予期間の影響を受けている場合、[表示] ボタンはドロップダウン メニューになり、ポッドの選択ができます。ポッドの詳細ページで利用可能なレポートおよびアクションの詳細については、このトピックの前のセクションを参照してください。

Horizon Cloud Connector 仮想アプライアンスの手動更新

クラウド接続された Horizon ポッド用の最新の機能を取得するには、これらのポッドの Horizon Cloud Connector 仮想アプライアンスを最新バージョンに更新します。この記事では、仮想アプライアンスがデプロイされている環境内で仮想アプライアンスを手動で更新する手順について説明します。

[Horizon Cloud Connector の更新プロセスの概要]

Horizon Cloud テナント アカウントが Horizon Cloud Connector の自動更新用に構成されている場合は、手動更新を実行する必要はありません。自動更新機能により、VMware オペレーション チームがテナント アカウントで新しいバージョンを使用できるようにすると、アプライアンスはクラウド プレーンから自動的に更新されます。詳細については、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。

既存のバージョンは、その 1 つまたは 2 つ上のバージョンに更新できます。つまり、バージョン `N` は `N+1` または `N+2` のいずれかに更新できます。

注： Horizon Cloud Connector 仮想アプライアンスの更新中は、プロキシの SSL 設定を使用できません。

クラウド接続された Horizon ポッドの Horizon Cloud Connector と Connection Server の両方のアップグレードを予定している場合は、アップグレード中にポッドの健全性を監視して確認してください。ポッドの健全性を監視することは、発生する可能性がある問題のトラブルシューティングに役立ちます。クラウド接続された Horizon ポッド上の Connection Server をアップグレードすると、そのポッドの健全性に問題が発生する場合があります。続いて、その問題のあるポッドとペアリングされている Horizon Cloud Connector をアップグレードしようとすると、Horizon Cloud Connector のアップグレードに失敗する場合があります。次のベスト プラクティスに従ってください。

1 クラウド接続された Horizon ポッド上の Connection Server をアップグレードした後に、ポッドが健全であることを確認します。

2 ポッドの健全性ステータスを表示するには、まず Horizon Universal Console にログインし、Active Directory ドメイン バインドを実行します。このステップでは、コンソールの [キャパシティ] ページにアクセスして、ポッドの健全性ステータスが「オンライン」または「準備完了」と表示されていることを確認できます。

3 ポッドが異常な健全性ステータスを示す場合は、Horizon Cloud Connector のアップグレードを試行する前に、VMware のサポートに連絡して、ポッドが関与する接続の問題の解決について相談してください。

[Horizon Cloud Connector 1.10 以前の手動更新ワークフロー]

バージョン 1.10 以前を実行している既存の Horizon Cloud Connector アプライアンスの場合は、この記事に記載されている手順に従って手動で更新します。

[Horizon Cloud Connector 2.0 以降の手動更新ワークフロー]

バージョン 2.0 以降を実行している既存の Horizon Cloud Connector アプライアンスの場合、手動更新のワークフローは、単一ノード クラスタまたはマルチノード クラスタのどちらをデプロイしたかによって異なります。

- プライマリ ノードのみで構成される単一ノード クラスタをデプロイした場合は、この記事に記載されている手順に従って手動更新を実行します。
- プライマリ ノードと 1 つ以上のワーカー ノードで構成されるマルチノード クラスタをデプロイしている場合は、次のワークフローを使用して手動更新を実行します。
  a この記事に記載されている手順に従って、プライマリ ノードの手動更新を実行します。
  b Horizon Cloud Connector 2.0 以降 - Horizon Cloud Connector クラスタへのワーカー ノードの追加に記載されている手順に従って、更新されたバージョンのワーカー ノードをクラスタに追加します。
  c プライマリ ノードとワーカー ノードの古いバージョンをパワーオフし、ポッドの環境から削除します。

前提条件

- 現在のクラウド制御プレーン リリースでサポートされている Horizon Cloud Connector 仮想アプライアンスの最新バージョンをダウンロードします。最新バージョンおよびリリース情報については、Horizon Cloud のドキュメント ページにあるリリース ノートを参照してください。
- 更新が必要な既存 Horizon Cloud Connector 仮想アプライアンスと新しい Horizon Cloud Connector 仮想アプライアンスが同じネットワーク上にあり、新しい仮想アプライアンスが既存の仮想アプライアンスと SSH 通信を確立できることを確認します。
- 仮想アプライアンスがパワーオン状態であることを確認します。アプライアンスがパワーオフの状態は異常です。理由は、Horizon Cloud Connector はクラウド制御プレーンとの接続を維持して、クラウド接続されたポッドの Horizon サブスクリプション ライセンスをアクティブな状態にする必要があるためです。
- 送信トラフィックの SSL オフロード用に Horizon Cloud Connector トラスト ストア内でカスタム CA 署名証明書を構成し、Horizon Cloud Connector バージョン 2.4.0 から以降のバージョンに更新する場合は、新しいアプライアンスの準備が完了した後、カスタム証明書を手動で新しいアプライアンスにコピーし、「Horizon Cloud Connector 2.4 以降 - 送信トラフィック用に SSL オフロードを構成している場合は、Horizon Cloud Connector でカスタムの CA 署名証明書を構成して Horizon 制御プレーンへの接続を許可する」に記載されている手順を実行する必要があります。証明書は、以前の仮想アプライアンスから新しい仮想アプライアンスに自動的に転送されません。

重要： 更新する前に、アプライアンスの `/opt/container-data/hydracerts/` ディレクトリから証明書のバックアップ コピーを保存し、それらを一時的な場所に保存する必要があります。コピーを保存すると、アップグレード後に新しいアプライアンスにコピーできるようになります。既存のアプライアンスがシャットダウンされているため、その後に証明書を取得できなくなります。そのため、アップグレードを開始する前にそのディレクトリから証明書を取得し、準備ができたら新しいアプライアンスにアップロードするために証明書を取得できる一時的な場所に保存する必要があります。

- （オンプレミスおよびオールイン SDDC Horizon ポッド）vSphere Client を使用して、既存の Horizon Cloud Connector 仮想アプライアンスのスナップショットを作成します。
- （フェデレーション アーキテクチャを持つ Azure VMware Solution の Horizon ポッド）次のいずれかの方法を使用して、既存の Horizon Cloud Connector 仮想アプライアンスのスナップショットを作成します。
  - Azure ポータルまたは PowerShell を使用してアプライアンスのスナップショットを作成する方法については、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/snapshot-copy-managed-disk を参照してください。
  - アプライアンスの仮想マシン バックアップを作成する方法については、https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction を参照してください。
- Horizon Cloud Connector 仮想アプライアンスの固定 IP アドレス、DNS アドレス、ゲートウェイ アドレス、およびサブネット マスクを収集します。
- クラウドプレーン テナント アカウントへのログインに有効な Customer Connect アカウント認証情報があることを確認します。「『デプロイ ガイド』のオンボーディング情報」に記載されているように、このアカウントを使用して、Horizon Cloud Connector のオンボーディングおよび管理ポータルにログインします。ポッドに関連付けられている Active Directory ドメインが、コネクタがペアリングされている Horizon Cloud テナントにすでに登録されている場合は、My VMware の認証情報を使用してログインすると、2 回目のログイン画面が表示されます。この 2 回目のログイン画面では、Horizon Cloud テナント環境のスーパー管理者ロールを持つ管理者の Active Directory 認証情報が要求されます。2 回目のログイン画面が表示された場合は、アクセス権限を持つドメイン内の Active Directory アカウントの認証情報が必要になります。このログイン プロセスの詳細については、Horizon Universal Console にログインして Horizon Cloud 環境で管理タスクを実行するを参照してください。
- （オンプレミスおよびオールイン SDDC Horizon ポッド）Horizon Cloud Connector 仮想アプライアンスの `/etc/hosts` ファイルに vCenter Server の FQDN を追加します。これらの手動更新手順を実行するには、この FQDN を使用する必要があります。

  Cloud Connector のバージョン 1.10 以前の場合は、`/etc/hosts` ファイルを編集した後、`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
  ```

Cloud Connector のバージョン 2.0 以降の場合は、`/etc/hosts` ファイルを編集した後、Kubernetes サービスを再起動する必要があります。次のスクリプトを実行します。

```
/opt/vmware/bin/configure-adapter.py  --updateHostAlias
```

重要： コネクタ アプライアンスのバージョン 1.0 はサポートされなくなりました。バージョン 1.0 から更新する場合、Horizon Cloud Connector 仮想アプライアンスのスナップショットを作成した後、アプライアンスのオペレーティング システムにログインし、`chage -E -1 -M -1 tomcat8` コマンドを実行する必要があります。

```
root@example.com [ ~ ]# chage -E -1 -M -1 tomcat8
```

このコマンドは、Horizon Cloud Connector バージョン 1.0 から更新する場合にのみ必要であり、それ以降のバージョンからの更新には必要ありません。

手順

1 Horizon Cloud Connector バージョン 2.4.0 から以降のバージョンに更新し、Horizon Cloud Connector トラスト ストア内でカスタムの CA 署名証明書が構成されている場合は、アプライアンスの `/opt/container-data/hydracerts/` ディレクトリから証明書のバックアップ コピーを保存し、準備ができたら新しいアプライアンスにアップロードするために証明書を取得できる一時的な場所に保存します。

2 Web ブラウザで Horizon Cloud Connector のオンボーディングおよび管理ポータルにログインするには、Horizon Cloud Connector 仮想アプライアンスの IP アドレスを入力するか、その IP アドレスを DNS の FQDN にマッピングした場合は、ブラウザでその FQDN を入力します。

Customer Connect アカウントの認証情報を使用してログインします。この手順では、『デプロイ ガイド』のオンボーディング プロセスの説明に従って、Horizon Cloud テナント アカウントにログインします。ログインに成功すれば、クラウド接続されたポッドの Connection Server で既存の Horizon Cloud 接続が正常に構成されていることになります。Horizon Cloud テナントに Active Directory ドメインが登録されている場合は、2 回目のログイン画面が表示されます。その場合は、Horizon Universal Console にログインして Horizon Cloud 環境で管理タスクを実行するの説明に従って、適切な Active Directory の認証情報を入力します。

3 Horizon Cloud Service を既存の Horizon ポッドに接続して Horizon の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、あるいはその両方を使用するの手順 1 ～ 8 に従って、Horizon Cloud Connector 仮想アプライアンスの最新バージョンをデプロイします。

注： Horizon Cloud Connector 仮想アプライアンスの以前のインスタンスが HTTP プロキシを使用していた場合は、デプロイ ウィザードの指示に従ってプロキシ設定を再構成します。手動による更新中に、プロキシ設定が以前の仮想アプライアンスから新しい仮想アプライアンスに転送されることはありません。

4 ブラウザで IP アドレスを使用して、手順 2 でデプロイした Horizon Cloud Connector アプライアンスのオンボーディング ポータルにログインします。

上記の手順 1 の説明に従って、Customer Connect 認証情報を使用してログインします。Horizon Cloud テナント アカウントに登録済みの Active Directory ドメインがある場合、Active Directory ログイン ウィンドウが表示され、適切な Active Directory 認証情報でログインする必要があります。

5 適切な Connection Server インスタンスで展開した Horizon Cloud Connector アプライアンスの最新バージョンを接続します。

Horizon Cloud Connector の以前のバージョンは、クラウドに接続しているポッドの Connection Server インスタンスに接続します。[Horizon Connection Server に接続] ボックスで、Connection Server の FQDN を入力して、[接続] をクリックします。

6 画面上でサムプリント証明書の検証が要求された場合は、チェック ボックスをクリックして Connection Server のサムプリント証明書を確認します。

注： Connection Server に有効なルート CA 証明書がある場合、この検証はスキップされます。

7 Connection Server のドメイン名、ユーザー名、パスワードを入力して、[接続]をクリックします。

注： Horizon Cloud Connector アクションの監査を効果的に行うには、Connection Server の一意のユーザー名とパスワードを使用します。

8 Horizon Cloud Connector バージョン 1.5 に更新する場合は、[Cloud Connector で SSH を有効にする] トグルを有効にします。

SSH を有効にすると、更新プロセスのために新しいコネクタ アプライアンスは SSH を使用して既存のコネクタ アプライアンスと通信できるようになります。更新が完了したら、このトグルをオフにできます。

9 ダイアログ ボックスで[アップグレード]をクリックします。

10 [古い Cloud Connector のアドレス] テキスト ボックスに、以前の Horizon Cloud Connector 仮想アプライアンスの IP アドレスを入力して、[接続] をクリックします。

11 SSH 接続のサムプリントを検証するチェック ボックスをクリックします。

12 [アップグレード]をクリックします。

新しい Horizon Cloud Connector は、Horizon ポッドとクラウド制御プレーン間のクラウド接続を管理しています。

次のステップ

Horizon Cloud Connector 仮想アプライアンスの以前のインスタンスがカスタムの CA 署名証明書を使用していた場合は、手順 1 で保存したバックアップ コピーを使用して更新された仮想アプライアンスを構成します。証明書は、更新プロセス中に以前の仮想アプライアンスから新しい仮想アプライアンスに転送されません。詳細については、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してください。

- Horizon Cloud Connector バージョン 2.4.x 以降に更新した場合は、「Horizon Cloud Connector 2.4 以降 - 送信トラフィック用に SSL オフロードを構成している場合は、Horizon Cloud Connector でカスタムの CA 署名証明書を構成して Horizon 制御プレーンへの接続を許可する」に記載されている手順を使用できます。
- 2.4.0 より前のバージョンに更新した場合は、「Horizon Cloud Connector 仮想アプライアンスの CA 署名付き証明書の構成」の手順を使用します。

古いバージョンのアプライアンスをポッドの環境から削除します。

将来の更新で、上記の手動の手順を使用する代わりに、Horizon Cloud Connector 仮想アプライアンスの自動更新を有効にするには、Horizon Cloud Connector 仮想アプライアンスの自動更新の構成の情報を参照してください。

Horizon Cloud Connector 仮想アプライアンスの自動更新の構成

Horizon ポッドを Horizon Cloud Connector 仮想アプライアンスの自動更新を実行するように構成できます。この構成により、Horizon Cloud オペレーション チームは、サービスを正常に実行するため、必要に応じてクラウド制御プレーンから仮想アプライアンスでメンテナンス アクションを実行できるようになります。

注： 自動更新には、以下の制限が適用されます。

- 自動更新機能は、オンプレミスにデプロイされた 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 ポッドを更新するには、Horizon Cloud Connector 仮想アプライアンスの手動更新を参照してください。
- 自動更新機能は、単一のデータセンターを管理する単一の vCenter Server のシナリオでサポートされています。単一の vCenter Server によって管理される複数のデータセンターのシナリオはサポートされていません。
- 自動アップグレード ワークフローでは、アプライアンスがデプロイされている vSphere 環境で DHCP を有効にする必要があります。DHCP を使用できない場合、この自動アップグレード ワークフローは失敗します。環境で DHCP を有効にできない場合、または有効にしない場合は、Horizon Cloud Connector 仮想アプライアンスの手動更新。
- 自動更新機能は、最初に Horizon Cloud Connector アプライアンス バージョン 1.6.0.0 以降でサポートされていました。
- 現時点では、ターゲット バージョン 2.0 または 2.1 の Horizon Cloud Connector へのアップグレードでは自動更新機能はサポートされていません。既存の Horizon Cloud Connector アプライアンスをターゲット バージョン 2.0 または 2.1 にアップグレードするには、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手順を実行します。
- 自動更新機能は、単一ノード デプロイのバージョン 2.1 以降を実行している既存の Horizon Cloud Connector アプライアンスでのみサポートされます。1 つ以上のワーカー ノードを追加してマルチノード クラスタをデプロイした場合、自動更新機能はサポートされません。マルチノード デプロイでバージョン 2.1 以降を実行している既存の Horizon Cloud Connector アプライアンスをアップグレードするには、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手順を実行します。
- 送信トラフィックの SSL オフロード用に Horizon Cloud Connector トラスト ストア内でカスタムの CA 署名証明書を構成し、Horizon Cloud Connector バージョン 2.4.0 から以降のバージョンに更新する場合は、Green アプライアンスの準備が完了した後、カスタム証明書を手動で新しいアプライアンスにコピーし、「Horizon Cloud Connector 2.4 以降 - 送信トラフィック用に SSL オフロードを構成している場合は、Horizon Cloud Connector でカスタムの CA 署名証明書を構成して Horizon 制御プレーンへの接続を許可する」に記載されている手順を実行する必要があります。証明書は、自動更新中に以前の仮想アプライアンスから新しい仮想アプライアンスに自動的には転送されません。

  重要： 自動更新を開始する前に、アプライアンスの `/opt/container-data/hydracerts/` ディレクトリから証明書のバックアップ コピーを保存し、それらを一時的な場所に保存する必要があります。コピーを保存すると、アップグレード後に新しいアプライアンスにコピーできるようになります。アップグレード プロセスが開始すると、既存のアプライアンスがシャットダウンされるため、その後に証明書を取得できなくなります。そのため、アップグレードが開始する前にそのディレクトリから証明書を取得し、準備ができたら新しいアプライアンスにアップロードするために証明書を取得できる一時的な場所に保存する必要があります。

注目： 自動更新機能は Horizon Cloud Connector で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ポッドごとに有効にできます。自動更新機能にアクセスするには、VMware の担当者に連絡するか、VMware ナレッジベース (KB) の記事 2006985 に記載されている Customer Connect サポート リクエストを提出して、この機能を明確にリクエストする必要があります。

自動更新の要件

Horizon Cloud Connector アプライアンスの自動更新をサポートするには、次のタスクを実行してシステム環境を準備します。

注： これらを実行できない場合、または実行しない場合は、Horizon Cloud Connector 仮想アプライアンスの手動更新。

1 ポッドによる自動更新の受信を有効にします。デフォルトでは、ポッドは自動更新を受け入れません。自動更新を受信する各ポッドについて特定の要求を提出する必要があります。

   ポッドの自動更新機能を有効にするには、VMware の担当者に連絡するか、VMware ナレッジベース (KB) の記事 KB2006985 に記載されている Customer Connect サポート リクエストを発行します。

2 システム環境が次の要件を満たしていることを確認します。

   - 静的 IP アドレスを持つ既存の Horizon Cloud Connector アプライアンスをデプロイしたこと。
   - 既存の Horizon Cloud Connector アプライアンスは、1.6.0.0 より前のバージョンを実行しています。バージョン 1.6.0.0 はかなり古いバージョンです。自動更新機能がサポートされていた最も古いバージョンです。
   - アプライアンスの更新をデプロイするには、少なくとも 50 GB のデータストア容量が利用可能であること。
   - Horizon Cloud Connector アプライアンスが、ESXi ホストにアクセスできること。
   - Horizon Cloud Connector 構成ポータルで vCenter Server とネットワーク設定を構成していること。詳細な手順については、この記事の次のセクションを参照してください。
   - 未割り当ての固定 IP アドレスは、アプライアンスの更新中に使用できます。このアドレスは、Horizon Cloud Connector アプライアンスの現在のバージョンで使用されている固定 IP アドレスとは異なるアドレスにする必要があります。
   - Horizon Cloud Connector アプライアンスがデプロイされている vSphere 環境で DHCP を有効にしていること。
     - グリーン アプライアンスを初めて起動する場合、IP アドレスは DHCP によって割り当てられます。
     - ブルーおよびグリーン アプライアンスがデプロイされている vSphere 環境で DHCP を有効にする必要があります。
     - グリーン アプライアンスが起動して実行状態になると、そのデフォルト ゲートウェイや DNS サーバとともに、固定 IP アドレスを設定できます。
     - アップグレード ワークフローが完了するまで DHCP が vSphere 環境で有効になっていない場合、ワークフローは失敗します。
   - Horizon Cloud Connector バージョン 2.4.0 以降から更新し、送信トラフィックの SSL オフロード用に Horizon Cloud Connector トラスト ストア内でカスタムの CA 署名証明書が構成されている場合は、アプライアンスの `/opt/container-data/hydracerts/` ディレクトリから証明書のバックアップ コピーを作成し、それらを一時的な場所に保存します。これらのコピーは、アップグレード後に新しいアプライアンスにアップロードする必要があります。証明書は、自動更新中に以前の仮想アプライアンスから新しい仮想アプライアンスに自動的には転送されません。

vCenter Server およびネットワーク設定の構成

自動更新機能により、Horizon Cloud Connector アプライアンスの新しいバージョンが vCenter Server にデプロイされます。これらのデプロイ用にシステム環境を準備するには、まず、更新されたアプライアンスに使用する未割り当ての固定 IP アドレスとネットワーク設定といった、必要なネットワーク情報を指定どおりに収集します。次の手順を実行します。

注： 自動更新機能に必要なデプロイと構成の手順を実行するには、vCenter Server で管理者権限を持つユーザーアカウントを構成する必要があります。vCenter Server およびネットワーク設定を構成するためのオプションが Horizon Cloud Connector 構成ポータルに表示されない場合は、この記事の前のセクション「自動更新の要件」で説明するように、最初にポッドの自動更新機能の有効化をリクエストする必要があります。

1 次のように、必要なネットワーク情報を収集します。

- （現在の Horizon Cloud Connector 1.9 またはそれ以降）更新されたアプライアンスで使用する未割り当ての固定 IP アドレスを決めます。更新中において、既存のアプライアンスに対して構成されている他のすべての必要なネットワーク設定が、更新されたアプライアンスで使用されます。
- （現在の Horizon Cloud Connector 1.6 から 1.8 まで）更新されたアプライアンスで使用する未割り当ての固定 IP アドレスとネットワーク設定を収集します。

2 Horizon Cloud Connector 構成ポータルにログインします。

3 構成画面を開いて vCenter Server の詳細を表示するには、次のいずれかの手順を実行します。

- （Horizon Cloud Connector 1.7 以降）[vCenter Server とネットワークの詳細の設定] ボタンをクリックします。
- （Horizon Cloud Connector 1.6）[Cloud Connector の自動更新の構成] ボタンをクリックします。

4 [Horizon Cloud Connector vCenter Server の詳細] 画面で、vCenter Server の FQDN を入力し、[証明書の取得] をクリックします。証明書情報が表示されたら、[上の証明書を確認したので続行します] を選択します。

5 [Horizon Cloud Connector vCenter Server 認証情報] に、vCenter Server の管理者権限を持つユーザーのログイン認証情報を入力します。

6 [Cloud Connector のアップグレードで使用するその他の固定 IP アドレスの詳細] で、必要に応じて固定 IP アドレスおよびその他のネットワーク設定を構成します。次のガイドラインに従います。

- （現在の Horizon Cloud Connector 1.9 またはそれ以降）新しいアプライアンス バージョンでは、既存のアプライアンス バージョン用に構成されたゲートウェイ、サブネット、および DNS サーバ設定を使用します。[Cloud Connector のアップグレードで使用するその他の固定 IP アドレスの詳細] でこれらのネットワーク設定を構成する必要はありません。

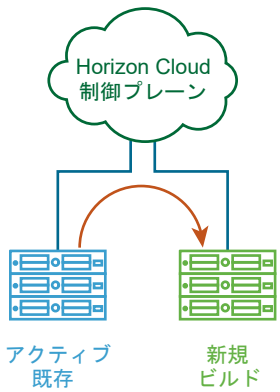
- （現在の Horizon Cloud Connector 1.6 から 1.8 まで）新しいアプライアンス バージョンでは、既存のアプライアンス バージョン用に構成されたゲートウェイ、サブネット、および DNS サーバ設定を使用しません。自動更新機能を使用するには、[Cloud Connector のアップグレードで使用するその他の固定 IP アドレスの詳細] で、新しいアプライアンス バージョン用のこれらの設定を手動で構成する必要があります。

設定	説明
[固定 IP アドレス]	更新中に予約アドレスとして使用する未割り当ての固定 IP アドレスを指定します。このアドレスは、アプライアンスの現在のバージョンで使用されている動作中の IP アドレスとは異なるアドレスにする必要があります。この予約アドレスは、アプライアンスの現在のバージョンに応じて、次のように使用されます。 ■ （現在の Horizon Cloud Connector 1.9 またはそれ以前）更新中、新しいアプライアンス バージョンは予約 IP アドレスを使用して、現在のアプライアンス バージョンが動作している間、一時的にネットワーク アクセスを取得します。更新の最後に、予約 IP アドレスが新しいアプライアンス バージョンから割り当て解除され、動作中の IP アドレスが古いアプライアンス バージョンから新しいアプライアンス バージョンに再割り当てされます。 ■ （現在の Horizon Cloud Connector 2.1 またはそれ以降）更新中、予約 IP アドレスが新しいアプライアンス バージョンに割り当てられ、Horizon Cloud Connector アプライアンスの新しい動作中の IP アドレスになります。古いアプライアンス バージョンの IP アドレスは、Horizon Cloud Connector の次回の自動更新のための新しい予約 IP アドレスになります。この記事の次のセクション「自動更新プロセスの End-to-End のフロー」の手順 6 を参照してください。
[デフォルト ゲートウェイ]	（現在の Horizon Cloud Connector 1.6 から 1.8 までのみ）新しいバージョンのアプライアンスに使用するゲートウェイ構成。
[サブネット マスク]	（現在の Horizon Cloud Connector 1.6 から 1.8 までのみ）新しいバージョンのアプライアンスに使用するサブネット マスク。
[DNS サーバ]	（現在の Horizon Cloud Connector 1.6 から 1.8 までのみ）新しいバージョンのアプライアンスに使用する DNS サーバ。 **重要：** 新しいアプライアンス バージョンに対して、最大 1 台の DNS サーバを構成します。複数の DNS サーバを構成すると、アプライアンスの更新に失敗します。

7 [保存] をクリックします。

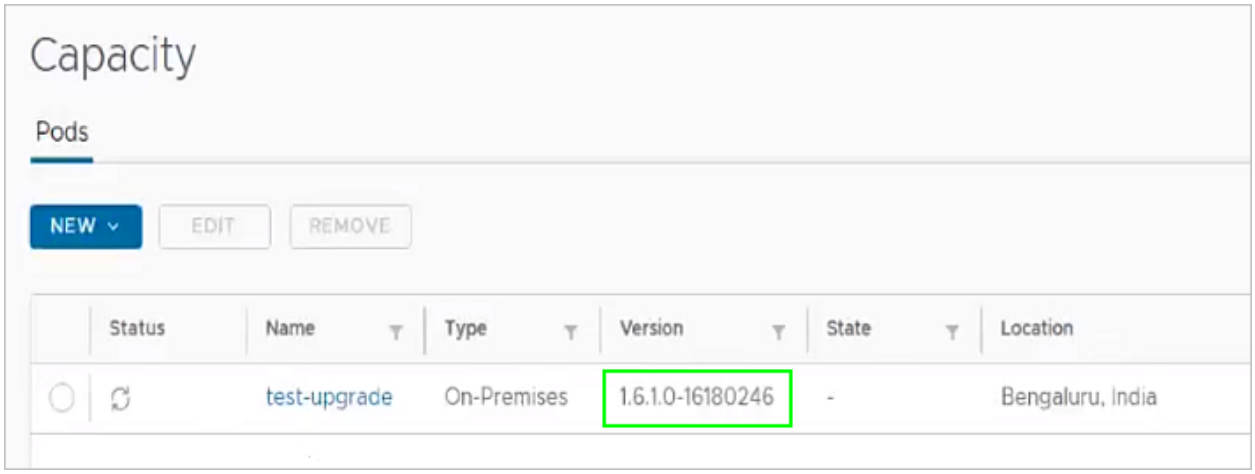
自動更新プロセスの End-to-End のフロー

Horizon Cloud Connector の自動更新プロセスは、「Blue-Green デプロイ」と呼ばれるソフトウェア業界の手法に従っています。



更新対象の既存の Horizon Cloud Connector インスタンスは、Blue アプライアンスと呼ばれます。新しいバージョンの Horizon Cloud Connector は、Green アプライアンスと呼ばれます。

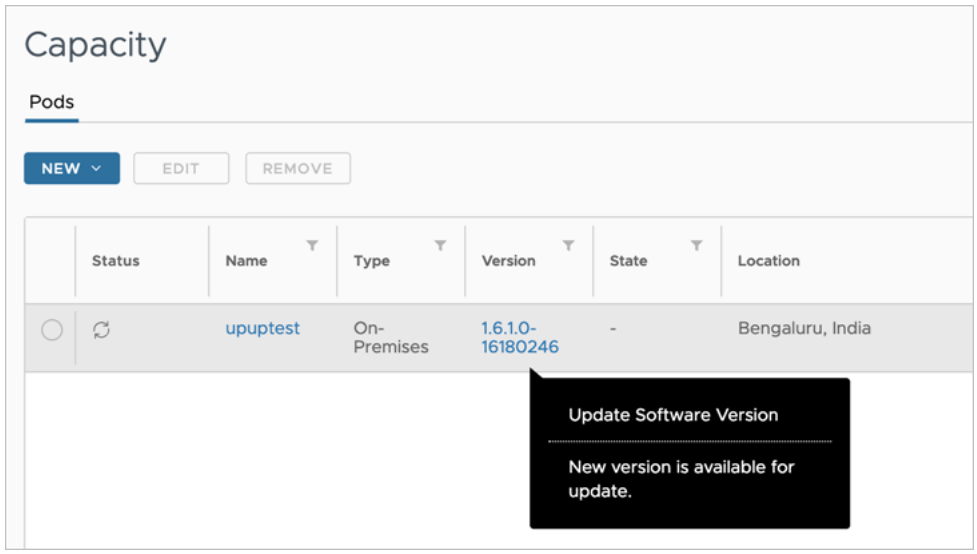
Blue アプライアンスの現在のバージョン番号を表示するには、[設定] - [キャパシティ] - [] の順に選択し、必要に応じて [ポッド] タブをクリックします。バージョン番号は、リスト内のペアになっているポッドの名前の横に表示されます。



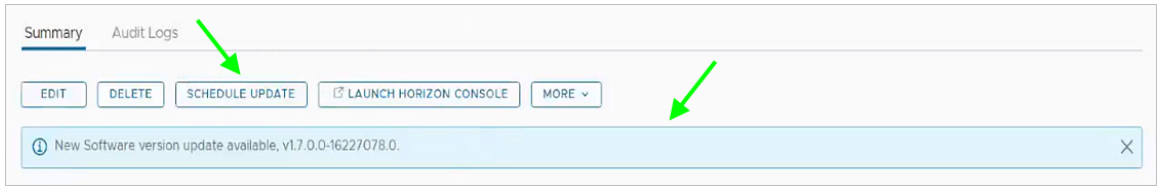
Horizon Cloud Connector オンボーディング ユーザー インターフェイスで vCenter Server とネットワーク設定を構成すると、End-to-End の更新プロセスは次の手順で構成されます。

1 VMware が、Blue アプライアンスと互換性のある Horizon Cloud Connector の更新バージョンをリリースすると、次のいずれかが発生します。

- システム環境が自動更新をサポートするためのすべての要件を満たしている場合、[キャパシティ] ページでポッドのバージョン番号をクリックすると、通知メッセージが表示されます。

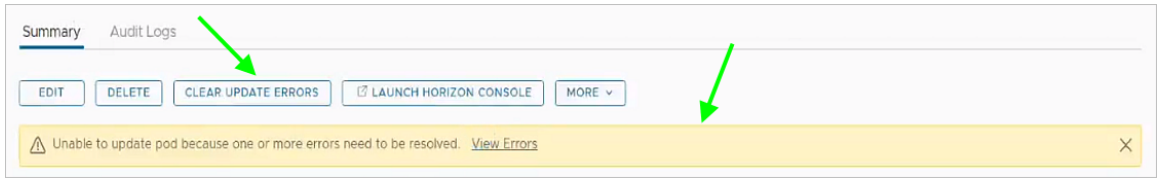


さらに、[スケジュールの更新] ボタンがポッドの詳細ページで使用可能になります。(ポッドの詳細ページを表示するには [設定] - [キャパシティ] - [] の順に選択し、必要に応じて [ポッド] タブをクリックして、リスト内のポッドの名前をクリックします。) このページの通知バナーには、使用可能な更新のバージョン番号が表示されます。



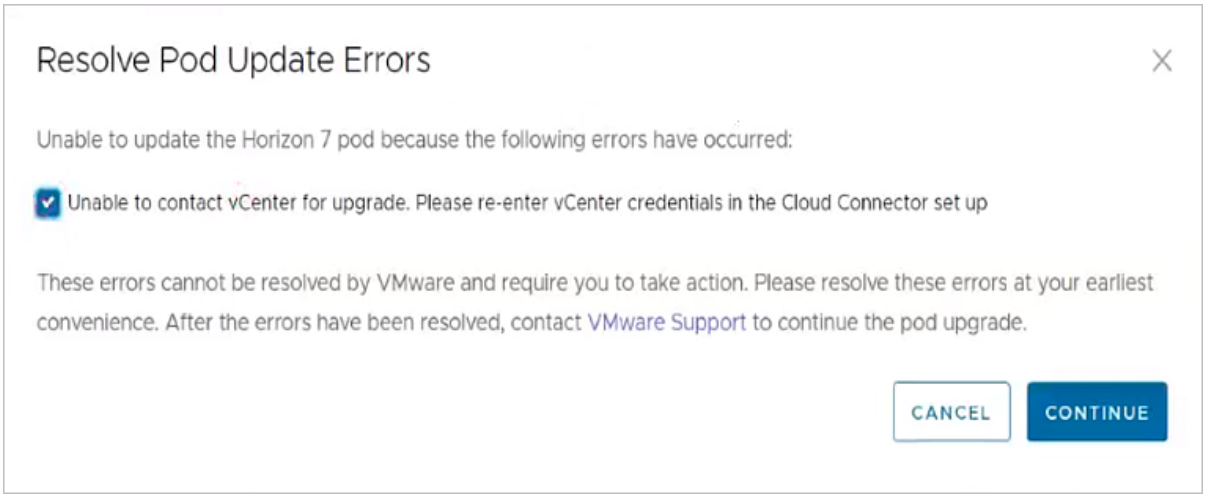
システム環境が自動更新のすべての要件を満たしている場合は、更新プロセスの手順 3 に進みます。

- システム環境が自動更新のすべての要件を満たしていない場合、ポッドの詳細ページには、[更新エラーをクリア] ボタンが表示されます。また、更新を妨げるエラーがあることを通知するメッセージも表示されます。



2 更新を妨げる 1 つ以上のエラー状態がある場合は、それらを解決する必要があります。[更新エラーをクリア] ボタンをクリックするか、またはアラート バナーのリンクをクリックして、[ポッド更新エラーの解決] ダイアログ ボックスを開きます。このダイアログ ボックスのメッセージに従って、必要なアクションを実行するか、または必要な構成を更新して、説明されているエラー状態をクリアします。次に、エラーの説明の横にあるチェック ボックスをオンにし、[続行] をクリックして、エラーが解決されたことを確認します。

次のスクリーンショットは、エラーの解決を確認した後の [ポッド更新エラーの解決] ダイアログ ボックスの例を示しています。

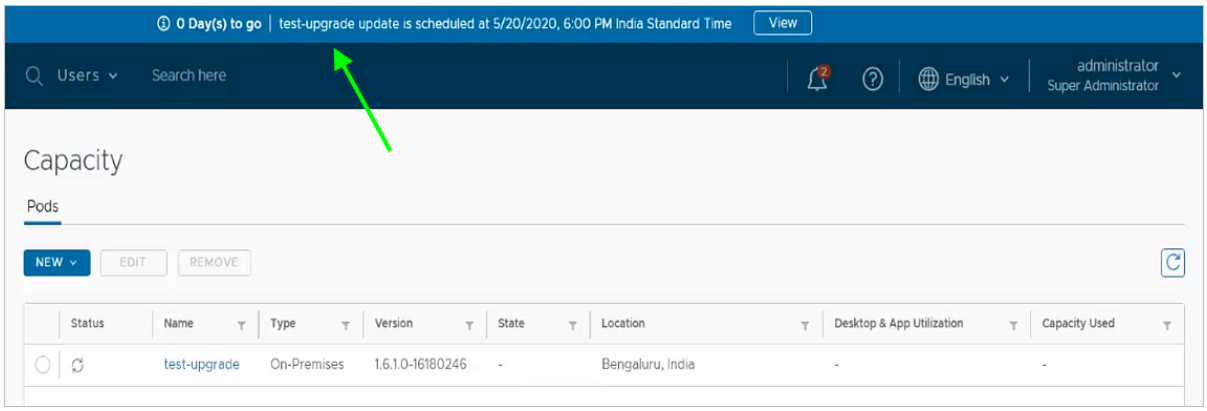


構成の変更が有効になり、管理コンソールにこれらの変更が反映されるまでに最大 30 分かかることがあります。エラーがクリアされると、[更新エラーのクリア] ボタンが [スケジュールの更新] に変わります。

3 更新ワークフローを開始するには、更新を手動でスケジューリングする必要があります。ポッドの詳細ページで、[スケジュールの更新] をクリックします。次に、Horizon Cloud サービスが Blue アプライアンスを Green アプライアンスに更新する日時を設定します。

アップデートが発生するのに都合の良い時刻を決定します。通常は、Green アプライアンスのデプロイや Blue アプライアンスから Green アプライアンスへの移行などの更新プロセスには、最大 90 分かかります。ベスト プラクティスとして、環境が最もビジーでないときにアップデートをスケジューリングします。更新がスケジューリングされると、コンソールの上部バナーにスケジューリングされた更新までの残り時間が表示されます。組織によって要求される場合、スケジュール設定された時刻の前であればいつでも更新時刻のスケジュールを再設定することができます。

次のスクリーンショットは、スケジュールされた更新を示すバナーの例を示しています。



重要：

- 更新をスケジューリングするときに、日付と時刻を指定する必要があります。これは、ブラウザのタイム ゾーンでのローカルの時間です。
- Horizon Cloud Connector バージョン 2.4.0 以降から更新し、Horizon Cloud Connector 内でカスタムの CA 署名証明書が構成されている場合は、スケジュール設定されたアップグレード時間の前に、アプライアンスの `/opt/container-data/hydracerts/` ディレクトリから証明書のバックアップ コピーを作成し、それらを一時的な場所に保存してください。これらのコピーは、アップグレード後に新しい (Green) アプライアンスにアップロードする必要があります。証明書は、自動更新中に以前の仮想アプライアンスから新しい仮想アプライアンスに自動的には転送されません。

4 スケジュールされた日時に、サービスは [Horizon Cloud Connector vCenter Server の詳細] 画面で以前に構成した固定 IP アドレスを使用して、vCenter Server に Green アプライアンスをデプロイします。通常、このデプロイ ステージが完了するまでには約 25 分かかります。ただし、正確な期間はシステム インフラストラクチャのキャパシティと特性によって異なる場合があります。

注： デプロイ、移行、および IP アドレスの再割り当てなどのステージを含む更新中に、更新中の Blue アプライアンスとペアリングされたポッドで管理タスクを実行することはできません。また、Horizon Cloud Connector 構成ポータルのすべてのアクション ボタンは、無効の状態になります。ただし、更新中、Blue アプライアンスは完全に動作したままで、ポッドはクラウド制御プレーンとサブスクリプション ライセンス サービスに接続されたままになります。

5 Green アプライアンスが完全にデプロイされると、サービスは構成を Blue アプライアンスから Green アプライアンスに移行します。通常、この移行ステージが完了するまでには約 10 分かかります。

6 移行が完了したら、次のいずれかが実行されます。

- Blue アプライアンスがバージョン 1.9 またはそれ以前の Horizon Cloud Connector を実行している場合は、予約 IP アドレスが Green アプライアンスから割り当て解除されます。次に、Blue アプライアンスの IP アドレスが Green アプライアンスに再割り当てされ、Horizon Cloud Connector インスタンスの新しい動作中の IP アドレスになります。予約 IP アドレスは、後続の自動更新で使用するために保持されます。

  注： 再割り当てを行うと、1 分未満の短い期間のダウンタイムが生じます。この間、ポッドは制御プレーンと Horizon Cloud サービスへの接続を一時的に失います。この間、エンド ユーザーは、ポッド上のリモート デスクトップおよびアプリケーションへの接続セッションを一時的に失う可能性があります。

  IP アドレスの再割り当てが完了すると、次のようになります。

  - Green アプライアンスが完全に動作し、ポッドの制御プレーンとサブスクリプション ライセンス サービスへの接続がリストアされます。
  - Green アプライアンスは、Blue アプライアンスの名前に新しいバージョン番号をサフィックスとして付加して作成された名前を持ちます。
  - Blue アプライアンスはデータストアに残り、パワーオフされます。

- Blue アプライアンスがバージョン 2.1 またはそれ以降の Horizon Cloud Connector を実行している場合は、予約 IP アドレスは Green アプライアンスに割り当てられたままになり、Horizon Cloud Connector インスタンスの新しい動作中の IP アドレスになります。ポッドは更新プロセス全体を通じて完全に動作し続け、制御プレーンおよび Horizon Cloud サービスに接続されます。

  更新プロセスが完了したら、次の操作が実行されます。

  - Green アプライアンスは、Blue アプライアンスの名前に新しいバージョン番号をサフィックスとして付加して作成された名前を持ちます。
  - Blue アプライアンスはデータストアに残り、パワーオフされます。
  - Blue アプライアンスの IP アドレスは、次回の自動更新のための新しい予約 IP アドレスとして使用されます。

    次の表に示すように、後続の自動更新では、予約 IP アドレスと動作中の IP アドレスが Blue アプライアンスと Green アプライアンス間でスワップされます。次の表に、最初の自動更新に対して Blue アプライアンスが動作中のアドレス 10.108.184.100 で始まり、予約アドレスが 10.108.184.200 として構成されている例を示します。

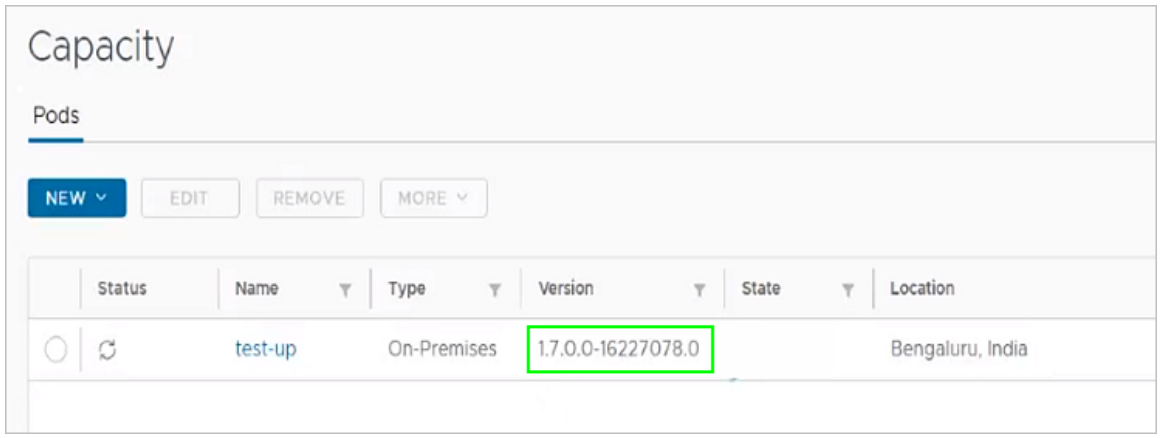
更新	Blue アプライアンスが使用する IP アドレス	Green アプライアンスが使用する IP アドレス
最初の自動更新	10.108.184.100	10.108.184.200
2 回目の自動更新	10.108.184.200	10.108.184.100

更新	Blue アプライアンスが使用する IP アドレス	Green アプライアンスが使用する IP アドレス
3 回目の自動更新	10.108.184.100	10.108.184.200
4 回目の自動更新	10.108.184.200	10.108.184.100

重要： Green アプライアンスの準備ができたら、Horizon Cloud Connector トラスト ストア内でカスタムの CA 署名証明書を構成した場合は、一時的な場所に保存したバックアップ コピーを使用して、それらを新しいアプライアンスで構成する必要があります。「Horizon Cloud Connector 2.4 以降 - 送信トラフィック用に SSL オフロードを構成している場合は、Horizon Cloud Connector でカスタムの CA 署名証明書を構成して Horizon 制御プレーンへの接続を許可する」に記載されている手順を使用します。証明書は、自動更新中に以前の仮想アプライアンスから新しい仮想アプライアンスに自動的には転送されません。

7 更新が正常に完了したことを確認するには、次の手順を実行します。

a [設定] - [キャパシティ] - [] の順に選択し、必要に応じて [ポッド] タブをクリックします。更新されたアプライアンスのバージョン番号は、リスト内のポッドの名前の横に表示されます。



b Green アプライアンスの Horizon Cloud Connector 構成ポータルにログインし、Horizon Cloud Connector コンポーネントの健全性を確認します。

注： Horizon Cloud Connector をバージョン 1.10 以降にアップデートすると、Horizon Cloud サービスが自動的に有効になります。Horizon Cloud Connector バージョン 1.10 以降では、アプライアンスのバージョン 1.8 または 1.9 で使用可能だった基本機能プロファイルはサポートされていません。

自動更新を妨げるエラー状態

一般的なエラー メッセージの例は次のとおりです。

- `Cloud Connector` がオンラインであることを確認します
- `Cloud Connector` は固定 `IP` アドレスを使用してデプロイされていません
- アップグレードのために `vCenter server` に接続できません。`Cloud Connector` のセットアップで、`vCenter Server` の認証情報を再入力してください
- アップグレードを実行するのに十分なディスク容量がありません。必要な最小ディスク容量は `50 GB` です。

必要な構成の変更を行って、指定されたエラーを修正し、自動更新のスケジュールを続行できるようにします。

Horizon Cloud Connector 仮想アプライアンスの更新のトラブルシューティング

Horizon Cloud Connector 仮想アプライアンスの以前のバージョンは、更新プロセスの終了時にのみ無効になります。更新プロセスに何か問題がある場合は、以前のバージョンの Horizon Cloud Connector 仮想アプライアンスにロールバックできます。

注： トラブルシューティング タスクを実行する場合、デプロイされている最新バージョンの Horizon Cloud Connector アプライアンスを取り外さないでください。

手順

1 更新に失敗して、Horizon Cloud Connector 仮想アプライアンスの以前のバージョンにアクセス可能な場合、このバージョンの仮想アプライアンスを引き続き使用できます。ログ ファイルを確認し、新しい Horizon Cloud Connector 仮想アプライアンスの構成情報を確認した後に、更新タスクを再度実行できます。

2 更新に失敗し、Horizon Cloud Connector 仮想アプライアンスの以前のバージョンにアクセスできない場合は、次の手順に従います。

   a 新しい Horizon Cloud Connector 仮想アプライアンスをパワーオフします。

   b 既存の Horizon Cloud Connector 仮想アプライアンスを更新前に作成された仮想アプライアンスのスナップショットに戻します。Horizon Cloud Connector 仮想アプライアンスが Web ブラウザからアクセスでき、ペアリング ステータスが表示されていることを確認します。

   c 更新タスクを実行し、最新バージョンの Horizon Cloud Connector アプライアンスを再度デプロイします。問題が解決しない場合は、VMware のサポートに問い合わせてください。

Horizon Cloud Connector アプライアンスのログ ファイルの収集

Horizon Universal Console または Horizon Cloud Connector 構成ポータルを使用して、Horizon Cloud Connector 仮想アプライアンスのログ ファイルをダウンロードできます。ログを収集するための自動化された方法にアクセスできない場合は、アプライアンスへの SSH 接続を確立してコマンドライン スクリプトを実行することによって、手動でログを収集できます。

Horizon Cloud Connector 構成ポータルの使用

アプライアンスの構成ポータルを使用して、仮想アプライアンスのログ ファイルを .zip 形式でダウンロードできます。このログの収集機能は、Horizon ポッドをクラウド制御プレーンとペアリングする前、最中、後に使用できます。この機能は、バージョン 1.7 以降でサポートされています。

1 Web ブラウザを使用して、Horizon Cloud Connector アプライアンスの URL に移動します。

2 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。必要に応じて、[同意] をクリックして、サービス利用規約のメッセージを継続して続行します。

3 いずれかの構成ポータル画面で、[ログのダウンロード] をクリックします。.zip ログ パッケージの場所を指定して、ログ パッケージを保存します。

Horizon Universal Console の使用

Horizon ポッドと制御プレーンを正常にペアリングし、Horizon Universal Console を使用して Active Directory 登録ワークフローを完了したら、コンソールを使用して .zip 形式の Horizon Cloud Connector ログをダウンロードできます。

1 コンソールで、ポッドの詳細ページに移動します。[設定] - [キャパシティ] を選択します。必要に応じて、[ポッド] タブをクリックし、リスト内のポッドの名前をクリックします。必要に応じて、[サマリ] タブをクリックして、ポッドの詳細ページを表示します。

2 [詳細] - [コネクタ ログのダウンロード] の順に選択します。.zip ログ パッケージの場所を指定して、ログ パッケージを保存します。

コマンド ラインの使用

Horizon Cloud Connector 構成ポータルの [ログのダウンロード] ボタンまたは Horizon Universal Console の [コネクタ ログのダウンロード] アクションにアクセスできない場合でも、コマンドライン スクリプトを実行して、アプライアンスのログ ファイルを手動で収集できます。この機能は、バージョン 1.7 以降でサポートされています。

1 Horizon Cloud Connector アプライアンスへの SSH 接続を開きます。

2 コマンドライン ターミナルで次のスクリプトを実行します。

```
/opt/vmware/bin/configure-adapter.py --archiveLogs
```

スクリプトはログをバンドルし、`/home/logs` ディレクトリ内の .tgz パッケージとしてアーカイブします。スクリプトの出力の末尾近くにリストされている、.tgz アーカイブのファイル名が表示されます。

たとえば、次の抜粋は、Horizon Cloud Connector ログを `/home/logs` の `cc_logs_20200424_154638.tgz` アーカイブに保存したスクリプトの出力を示しています。

```
/opt/container-data/logs/hze-keybox/localhost.2020-04-23.log
/opt/container-data/logs/hze-keybox/localhost_access_log.2020-04-21.txt
--------------------------------------------------------------------------------
Logs archived at /home/logs/cc_logs_20200424_154638.tgz
--------------------------------------------------------------------------------
Archived successfully!
```

3 次に、作成した TGZ ファイルをアプライアンスの `/home/logs` ディレクトリから `/home/ccadmin` ディレクトリにコピーして、権限 (`chmod`) を 644 に変更します。たとえば、`cc_logs_20200424_154638.tgz` という名前のファイルの場合、次のブロックはファイルをコピーしてモードを 644 に変更する例です。

```
cp /home/logs/cc_logs_20200424_154638.tgz /home/ccadmin/
chmod 644 /home/ccadmin/cc_logs_20200424_154638.tgz
```

4 次に、WinSCP などのツールを使用して、`ccadmin` アカウントを使用して TGZ ファイルをローカル システムにコピーできます。

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上書きさ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。新しい証明書を確実に検証するには、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 - 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。特定の名前は 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 4-1. 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	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

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 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 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。 ■ 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	地域別制御プレーン インスタンス。 **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。 ■ 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
注： (Horizon Cloud Connector 2.0 またはそれ以降) この要件は、プライマリ ノードにのみ適用されます。 Horizon Cloud Connector	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。 ■ 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
	■ 日本：kinesis.ap-northeast-1.amazonaws.com ■ 英国：kinesis.eu-west-2.amazonaws.com			
Horizon Cloud Connector	*.digicert.com 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。 ■ ocsp.digicert.com ■ crl3.digicert.com ■ crl4.digicert.com ■ www.digicert.com/CPS 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。	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 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。 ■ 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 ■ 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 4-2. 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機します。
Web ブラウザ	Horizon Cloud Connector	443	HTTPS	ペアリング プロセスの開始を待機します。
ネットワーク上のクラウド接続された Horizon ポ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：https://*<vCenter Server の FQDN>*/sdk	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ポ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：https://*<vCenter Server の FQDN>*/sdk	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 Horizon Cloud Universal Broker とマルチクラウド割り当て

5

このドキュメント ページでは、第 1 世代 Universal Broker の概要、マルチクラウド割り当て (MCA) との関係、およびそれらの MCA を構成するための手順の概要について簡単に説明します。

第 1 世代 Universal Broker

第 1 世代 Universal Broker はクラウドベースのサービスで、実行中のインフラストラクチャに関係なく、複数のポッドのデプロイにまたがるリソースの仲介を可能にします。

このサービスにより、ユーザーとポッドの地理的サイトに基づいてインテリジェントな仲介を決定できます。

マルチクラウド割り当てを作成するには、第 1 世代テナントに Universal Broker を構成する必要があります。マルチクラウド割り当ては、複数のポッドにまたがるプールです。

Horizon 8 ポッド - マルチクラウド割り当てを構成するための手順の概要

Horizon 8 ポッド（Horizon Connection Server テクノロジー ベース）からのリソースのマルチクラウド割り当てを設定するには、次に概要を示す手順を実行します。

1 Horizon ポッド環境のシステム コンポーネントが必要な Universal Broker のシステム要件を満たしていることを確認します。

2 最新バージョンの Horizon Cloud Connector を使用して、参加している Horizon ポッドを Horizon Cloud にオンボーディングします。詳細については、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。

3 参加しているポッドごとに、Universal Broker を操作するために必要なシステム コンポーネントを準備します。

   a Horizon ポッド - Connection Server への Universal Broker プラグインのインストールを参照してください。ポッド内のすべての Connection Server インスタンスにプラグインをインストールする必要があります。

   b Horizon ポッド - Universal Broker で使用する Unified Access Gateway を構成するを参照してください。ポッド内のすべての Unified Access Gateway インスタンスを構成する必要があります。Universal Broker に 2 要素認証を使用する場合は、参加しているすべてのポッドのすべての Unified Access Gateway インスタンスに同じ認証を設定する必要があります。

4 Horizon Cloud テナントの Horizon ポッドのコネクション ブローカとして Universal Broker を選択します。Horizon Universal Console を使用した Universal Broker の有効化の開始を参照してください。

5 Universal Broker を設定します。Universal Broker の設定を参照してください。

6 Horizon Universal Console を使用して、クラウド接続された Horizon ポッドを管理対象状態に変更するで説明するように、マルチクラウド割り当て用の参加しているポッドを有効にします。

7 Horizon Cloud テナントのサイト構成とホーム サイトの関連付けを定義します。Universal Broker のサイトの構成および Universal Broker のホーム サイトの構成を参照してください。

8 参加しているポッド内で、Universal Broker で必要な必須の設定を使用してデスクトップ プールを構成します。Horizon ポッド - マルチクラウド割り当てに使用する既存のデスクトップ プールを準備するおよび Horizon ポッド - マルチクラウド割り当てに適したデスクトップ プールの作成を参照してください。

9 マルチクラウド割り当てを構成します。Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成を参照してください。

Microsoft Azure の Horizon Cloud ポッド - マルチクラウド割り当てを構成するための手順の概要

Horizon Cloud ポッドからのリソースのマルチクラウド割り当てを設定するには、次に概要を示す手順を実行します。

1 Horizon Cloud ポッドでポッド マニフェスト 2298.0 以降が実行されていることを確認します。

注： Universal Broker は [すべて] のテナントの Horizon Cloud ポッドがポッド マニフェスト 2298.0 以降を実行している場合にのみサポートされます。ポッド マニフェスト 2298.0 は、サービスの 2020 年 7 月のリリースで初めて登場しました。

2 ポッドのシステム コンポーネントが必要な Universal Broker のシステム要件 を満たしていることを確認します。

3 Horizon Cloud ポッドのテナント全体のコネクション ブローカとして Universal Broker を選択します。Horizon Universal Console を使用した Universal Broker の有効化の開始を参照してください。

4 Universal Broker を設定します。Universal Broker の設定を参照してください。

5 Horizon Cloud テナントのサイト構成とホーム サイトの関連付けを定義します。Universal Broker のサイトの構成および Universal Broker のホーム サイトの構成を参照してください。

6 マルチクラウド割り当てを構成します。Microsoft Azure の Horizon Cloud ポッド - 第 1 世代環境での VDI マルチクラウド割り当ての作成と表示を参照してください。

次のトピックを参照してください。

- VMware Horizon Service Universal Broker について
- Universal Broker のシステム要件
- Horizon 制御プレーン テナントの Universal Broker サービスのセットアップ
- Universal Broker 環境でのサイトの操作

- View ポッド - マルチクラウド割り当てのためのクラウド接続されたポッドの有効化
- Universal Broker 環境での割り当ての作成および管理

VMware Horizon Service Universal Broker について

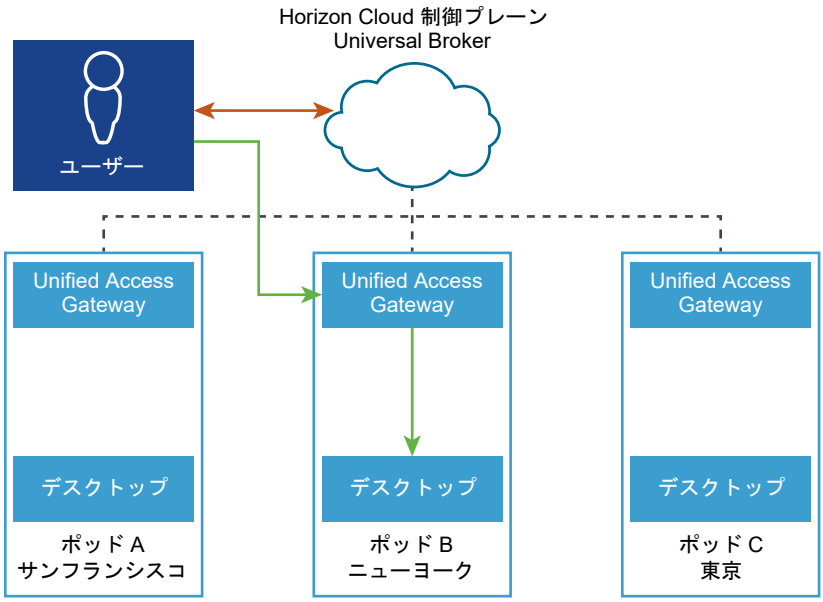
この記事では、Horizon 制御プレーン サービスの 1 つである Universal Broker について簡単に説明します。Universal Broker はクラウドベースのサービスで、実行中のインフラストラクチャに関係なく、複数のポッドのデプロイにまたがるリソースの仲介を可能にします。このサービスにより、ユーザーとポッドの地理的サイトに基づいてインテリジェントな仲介を決定できます。

Universal Broker の概要

VMware の最新のクラウドベースの仲介テクノロジーである Universal Broker は、テナントに次の 1 つ以上がある場合に使用できます。

- Horizon ポッド - Horizon Connection Server テクノロジーに基づくポッド
- Horizon Cloud on Microsoft Azure ポッド、およびポッド マニフェスト 2298.0 以降を実行しているすべてのポッド。

Universal Broker ソリューションのシステム コンポーネントがどのように連携して割り当てに対するユーザーの接続要求を管理するかの詳細については、Universal Broker のシステム アーキテクチャとコンポーネントを参照してください。

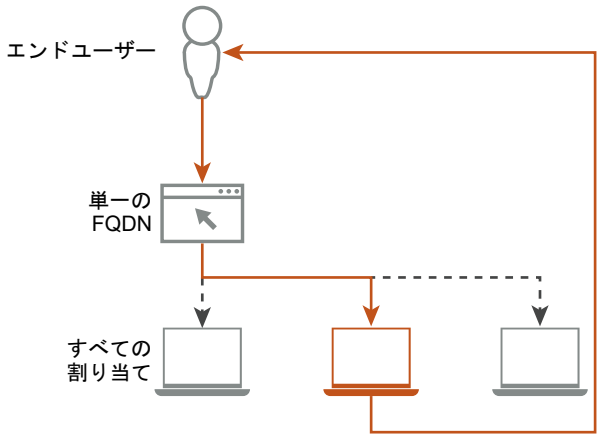


主な特長

Universal Broker は、次の主要な機能を提供します。

- [すべてのリモート リソースの単一の接続 FQDN]

エンド ユーザーは、Universal Broker の設定で定義した完全修飾ドメイン名 (FQDN) に接続することにより、環境内のマルチクラウド割り当てにアクセスできます。ユーザーは、単一の Universal Broker FQDN を使用して、ご使用の環境内の任意のサイトにある任意の参加しているポッドから割り当てにアクセスできます。ポッド間の内部ネットワークは必要ありません。



- [最適なパフォーマンスのためのグローバル ポッド接続と認識]

  Universal Broker は、マルチクラウド割り当てに参加しているすべてのポッドとの直接接続を維持し、各ポッドの可用性ステータスを引き続き認識します。その結果、Universal Broker はエンド ユーザーの接続要求を管理し、これらのポッドから直接仮想リソースにルーティングできます。パフォーマンスの低下や遅延の問題の原因となる、グローバル サーバ ロード バランシング (GSLB) やポッド間のネットワーク通信を行う必要はありません。

- [スマート仲介]

  Universal Broker は、地理的サイトとポッド トポロジの認識に基づいて、最短のネットワーク ルートに沿って割り当てからエンド ユーザーにリソースを仲介できます。

仲介およびエンド ユーザーのデスクトップ プールとリモート アプリケーション

割り当ては、Horizon Universal Console 内の概念的なエンティティです。コンソールを使用して行う割り当ては、エンド ユーザーの仮想デスクトップとリモート アプリケーションのプールを定義し、それらの使用資格をエンド ユーザーに付与する方法です。たとえば、コンソールでは、VDI デスクトップの割り当てまたは RDSH リソースの割り当てを作成し、その割り当ての使用資格をエンド ユーザーに付与します。

Universal Broker は、資格のある割り当てに対するクライアント ユーザーの接続要求を管理し、その要求を満たす適切なリソースへの接続セッションをネゴシエートします。Universal Broker は、地理的な場所とポッド トポロジを認識します。この情報を使用して、Universal Broker は、サイトの構成とリソースの可用性に基づいてユーザーの接続要求を満たすのに最適なリソースを検索します。

ポッド タイプ別に使用可能な割り当てタイプのリストについては、次のセクションを参照してください。

Microsoft Azure にデプロイされた Horizon Cloud ポッドのリソースを使用したエンド ユーザー割り当て

ポッド フリート内の Horizon Cloud ポッドの Universal Broker 構成が完了すると、次の割り当てタイプが可能になります。

- 1 つ以上の Horizon Cloud ポッドからの VDI デスクトップで構成されるマルチクラウド割り当て。詳細については、Microsoft Azure の Horizon Cloud ポッド - 第 1 世代環境での VDI マルチクラウド割り当ての作成と表示を参照してください。
- 単一の Horizon Cloud ポッド内の Microsoft リモート デスクトップ サービス (RDS) ホストからのセッションベースのデスクトップで構成されるセッション デスクトップ割り当て。詳細については、Horizon Cloud ポッド - RDS ベースのセッション デスクトップ割り当てを作成して、エンド ユーザーのために RDS ホストからのデスクトップ セッションを提供するを参照してください。
- Horizon Cloud ポッド内の RDS ホストによってプロビジョニングされたアプリケーションで構成されるリモート アプリケーション割り当て。詳細については、リモート アプリケーション - Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされたリモート アプリケーションのリモート アプリケーション割り当ての作成を参照してください。
- Horizon Cloud ポッド内の VDI デスクトップにホストされている App Volumes アプリケーションで構成される App Volumes アプリケーション割り当て。詳細については、Horizon Cloud：App Volumes 割り当ての作成を参照してください。

クラウド接続された Horizon ポッドからのリソースを使用したエンド ユーザーの割り当て

ポッド フリート内の Horizon ポッドの Universal Broker 構成が完了すると、次の割り当てタイプが可能になります。

- 1 つ以上の Horizon ポッドからの VDI デスクトップで構成されるマルチクラウド割り当て。Horizon Cloud テナントのクラウド接続された Horizon ポッドのリソースに基づいたマルチクラウド割り当ての構成に関する概要情報については、5 章 第 1 世代 Horizon Cloud Universal Broker とマルチクラウド割り当てを参照してください。
- 単一の Horizon ポッド内の Microsoft リモート デスクトップ サービス (RDS) ホストからのセッションベースのデスクトップで構成されるセッション デスクトップ割り当て。詳細については、Horizon ポッド - Universal Broker 環境用の RDSH デスクトップとアプリケーションの構成を参照してください。
- 単一の Horizon ポッド内の RDS ホストによってプロビジョニングされたアプリケーションで構成されるリモート アプリケーション割り当て。詳細については、Horizon ポッド - Universal Broker 環境用の RDSH デスクトップとアプリケーションの構成を参照してください。

注

ほとんどのソフトウェアと同様に、現在のリリースには機能に関する考慮事項と既知の制限がいくつかあります。詳細については、Universal Broker - 機能に関する注意事項と既知の制限を参照してください。

Universal Broker のシステム アーキテクチャとコンポーネント

この記事では、参加しているポッド内および Horizon Cloud 制御プレーンで実行される Universal Broker のシステム コンポーネントについて詳しく説明します。Universal Broker は VMware の最新のクラウドベースの仲介テクノロジーを表し、新しいデプロイでのエンド ユーザー割り当てにはこのコネクション ブローカが推奨されます。

Universal Broker の主な機能の概要については、VMware Horizon Service Universal Broker についてを参照してください。

Universal Broker ソリューションのシステム アーキテクチャは、仲介されたリソースの配置先が Horizon ポッド（Horizon Connection Server テクノロジー ベース）か、Microsoft Azure の Horizon Cloud ポッドかによってやや異なります。

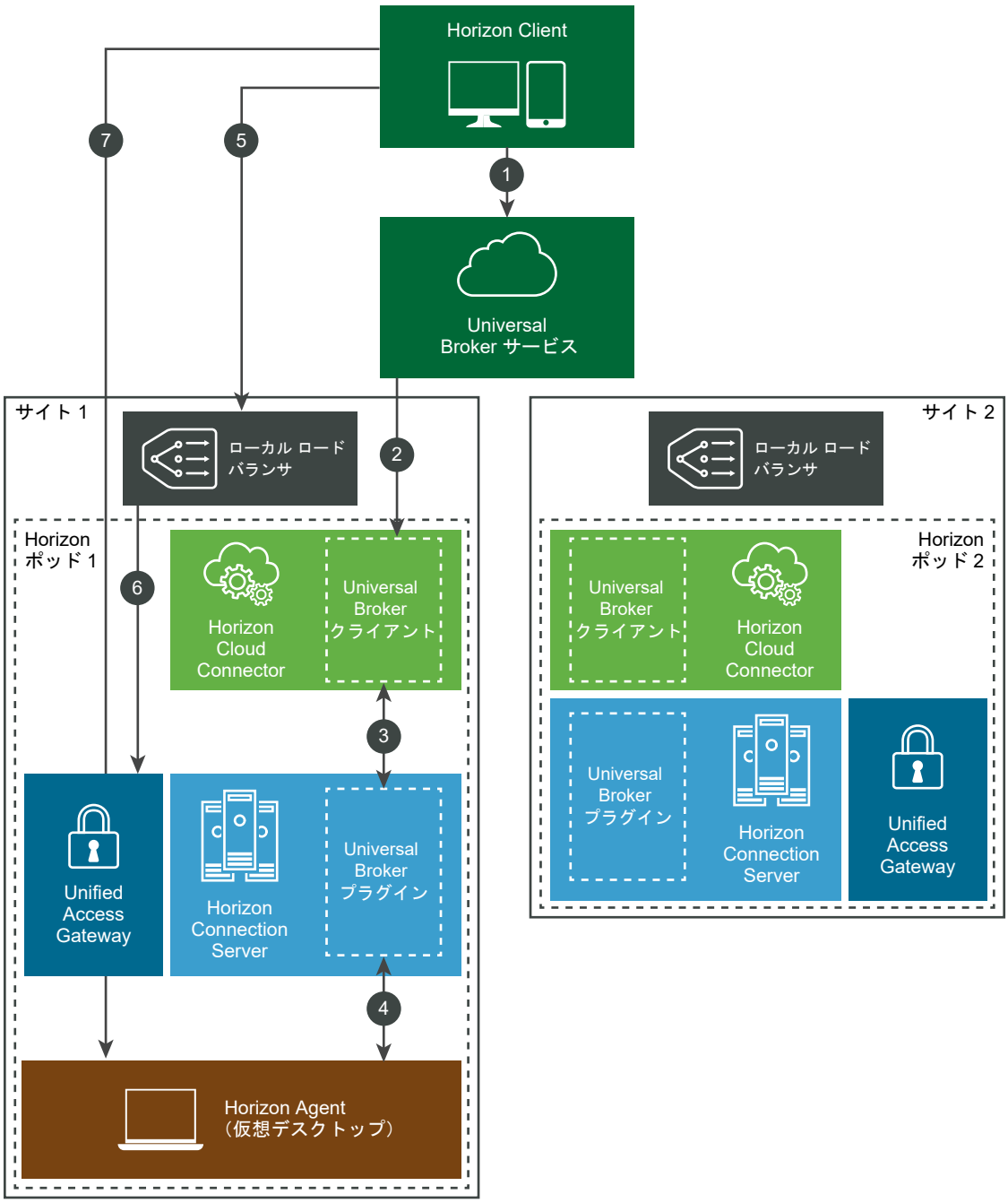
Universal Broker のシステム アーキテクチャ（Horizon ポッド）

次のコンポーネントは、Horizon ポッド（Horizon Connection Server テクノロジー ベース）からのマルチクラウド割り当てのクラウドベースの仲介のための Universal Broker ソリューションを構成しています。

- Universal Broker サービスは、Horizon Cloud に接続された Universal Broker クラウド内で実行されるマルチテナント クラウド サービスです。各ユーザーは、Universal Broker の設定で説明するように、構成された一意の専用 FQDN を使用して、Universal Broker サービスに接続します。
- Universal Broker クライアントは、クラウド接続された各 Horizon ポッドの Horizon Cloud Connector 内で実行されます。このコネクタのバージョン 1.5 以降では、Universal Broker クライアントはそのコネクタの一部であり、Horizon Cloud Connector をポッドとペアリングすると自動的にインストールされます。
- Universal Broker プラグインは、マルチクラウド割り当てに参加するすべてのクラウド接続ポッドの Horizon Connection Server 内で実行されます。Horizon ポッド - Connection Server への Universal Broker プラグインのインストールの説明に従って、参加するポッド内の各 Connection Server インスタンスにプラグインをダウンロードしてインストールする必要があります。

次の図は、Universal Broker が Horizon ポッド環境のコンポーネントと連携して、外部エンド ユーザーから割り当て内のリモート リソースへの接続要求をどのように管理するかを示しています。

注： 次に示すシナリオには、企業ネットワーク外の外部ネットワークに配置され、ポッドに外部 Unified Access Gateway が構成されている Horizon Client が含まれます。



1 Horizon Client から、エンド ユーザーは仲介の FQDN を介して Universal Broker サービスに接続することにより仮想デスクトップを要求します。このサービスは、XML-API プロトコルを使用して Horizon Client ユーザーを認証し、接続セッションを管理します。

2 サイト 1 のポッド 1 がデスクトップの最適なソースであると判断した後、Universal Broker サービスは、ポッド 1 とペアリングされた Horizon Cloud Connector で実行されている Universal Broker クライアントにメッセージを送信します。

3 Universal Broker クライアントは、ポッド 1 内のそれぞれの Connection Server インスタンスで実行されている Universal Broker プラグインにメッセージを転送します。

4 Universal Broker プラグインは、エンド ユーザーの要求を満たすために使用できる最善のデスクトップを識別します。

5 Universal Broker サービスは、ポッド 1 の一意の FQDN（通常はポッド 1 ロード バランサの FQDN）を含む応答を Horizon Client に返します。Horizon Client は、ロード バランサとの接続を確立してデスクトップとのプロトコル セッションを要求します。

6 ローカルのロード バランサを通過した後、要求はポッド 1 の Unified Access Gateway に送信されます。Unified Access Gateway は、要求が信頼されていることを検証し、Blast Secure Gateway、PCoIP Secure Gateway、およびトンネル サーバを準備します。

7 Horizon Client ユーザーは指定のデスクトップを受信し、構成されたセカンダリ プロトコル（Blast Extreme、PCoIP、または RDP）に基づいてセッションを確立します。

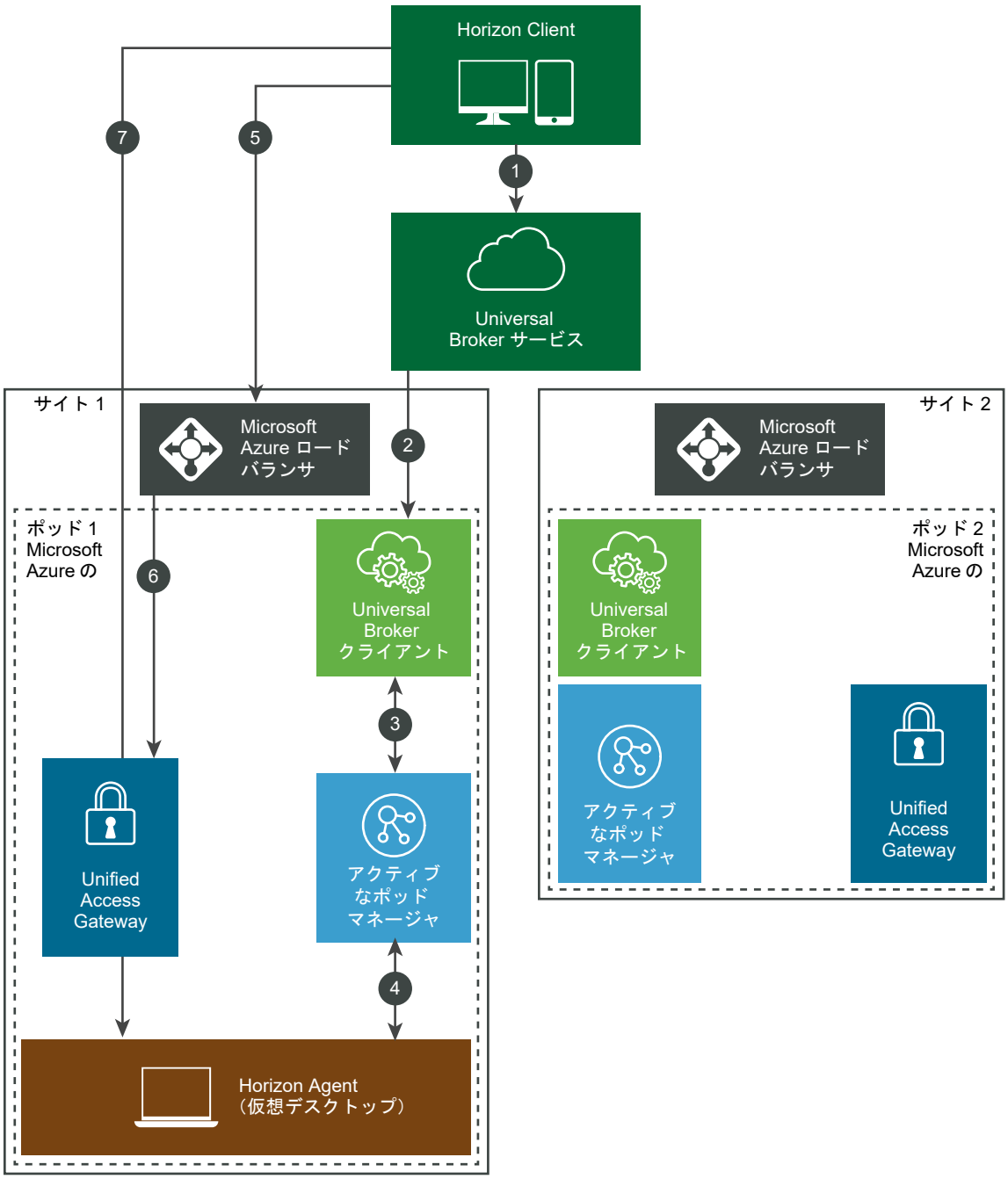
Universal Broker 通信に使用されるポートの詳細については、Horizon ポッド - Universal Broker の DNS、ポートおよびプロトコルの要件を参照してください。

Microsoft Azure の Horizon Cloud ポッドの Universal Broker のシステム アーキテクチャ

次のコンポーネントは、Microsoft Azure の Horizon Cloud ポッドからの VDI 割り当てと RDSH 割り当てのクラウドベースの仲介のための Universal Broker ソリューションを構成しています。

- Universal Broker サービスは、Horizon Cloud に接続された Universal Broker クラウド内で実行されるマルチテナント クラウド サービスです。各ユーザーは、Universal Broker の設定で説明するように、構成された一意の専用 FQDN を使用して、Universal Broker サービスに接続します。
- Universal Broker クライアントは、Microsoft Azure に参加している各 Horizon Cloud ポッド内で実行されます。

注： 次に示すシナリオには、企業ネットワーク外の外部ネットワークに配置され、ポッドに外部 Unified Access Gateway が構成されている Horizon Client が含まれます。



1 Horizon Client から、エンド ユーザーは仲介の FQDN を介して Universal Broker サービスに接続することにより仮想リソースを要求します。このサービスは、XML-API プロトコルを使用して Horizon Client ユーザーを認証し、接続セッションを管理します。

2 ユーザーの要求に最適なリソースがサイト 1 のポッド 1 にあると判断した Universal Broker サービスは、ポッド 1 内で実行されている Universal Broker クライアントにメッセージを送信します。

3 Universal Broker クライアントは、そのメッセージをポッド 1 内のアクティブなポッド マネージャに転送します。

4 アクティブなポッド マネージャは、エンド ユーザーの要求を満たすために使用できる最善のリソースを識別します。

5 Universal Broker サービスは、ポッド 1 の一意の FQDN（通常はポッド 1 の Microsoft Azure ロード バランサの FQDN）を含む応答を Horizon Client に返します。Horizon Client はロード バランサとの接続を確立し、リソースとのプロトコル セッションを要求します。

6 Microsoft Azure ロード バランサを通過した要求は、ポッド 1 の Unified Access Gateway に送信されます。Unified Access Gateway は、要求が信頼されていることを検証し、Blast Secure Gateway、PCoIP Secure Gateway、およびトンネル サーバを準備します。

7 Horizon Client ユーザーは指定のリソースを受信し、構成されたセカンダリ プロトコル（Blast Extreme、PCoIP、または RDP）に基づいてセッションを確立します。

Universal Broker 通信に使用されるポートの詳細については、2019 年 9 月リリースのマニフェスト以降の Horizon Cloud ポッドのポートとプロトコルの要件の「Universal Broker で必要なポートとプロトコル」セクションを参照してください。

Universal Broker - 機能に関する注意事項と既知の制限

このドキュメント ページでは、Universal Broker に関連するいくつかの機能の注意事項と、サポートが制限されている、またはサポートされていない Horizon 機能のリストを提供します。

機能に関する注意事項

- Horizon ポッドと Horizon Cloud ポッドの両方を含むポッド フリートでは、作成する各エンド ユーザー割り当ては、1 つのポッド タイプからの VDI デスクトップのみで構成する必要があります。たとえば、複数の Horizon ポッドにわたるデスクトップで構成される割り当てと、複数の Horizon Cloud ポッドにわたるデスクトップで構成される割り当てのいずれかを作成できます。しかし、Horizon ポッドと Horizon Cloud ポッドの両方にわたるデスクトップで構成される割り当てを作成することはできません。
- テナントをシングルポッド ブローカ構成から Universal Broker に移行した場合は、追加の注意事項が適用されます。Universal Broker への移行後のテナント環境の最新情報を参照してください。

VDI マルチクラウド割り当てあたりのポッドの最大数制限

1 つの VDI マルチクラウド割り当てでサポートされるポッドの最大数は 5 です。この制限は、Horizon Connection Server タイプのポッドと Horizon Cloud on Microsoft Azure タイプのポッドの両方に適用されます。5 つ以上使用すると、Universal Broker の同時負荷が増加します。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。

仮想リソース

仮想リソースの仲介の場合、このリリースの Universal Broker は Windows オペレーティング システムのみをサポートします。Linux ベースのデスクトップはサポートされません。

このリリースでは、管理者が作成したデスクトップおよびアプリケーションへのショートカットをサポートしていません。

注： 特定のユーザーは、1 つの割り当てに複数のポッドのデスクトップが含まれていても、Universal Broker によって仲介された専用割り当てから最大で 1 つの割り当てられたデスクトップを受信できます。

Horizon HTML Access と Horizon Client for Chrome

エンド ユーザーは、サポートされている Web ブラウザで Horizon HTML Access を実行するか、Horizon Client for Chrome 5.4 以降を実行することにより、Universal Broker サービスにリソースを要求できます。Universal Broker サービスが自己署名証明書を使用する Unified Access Gateway インスタンスに要求をリダイレクトすると、クライアント アプリケーションは認証局が無効であることを示すエラー メッセージを表示します。

これは設計によるものです。要求されたリソースに接続するために、ユーザーは証明書エラー メッセージのプロンプトに従って自己署名証明書を受け入れることができます。

認証方法

このリリースの Universal Broker は、UPN および NETBIOS 形式の Windows ユーザー名とパスワードによるクライアント ユーザー認証をサポートします。

次のリストに示すように、RADIUS または RSA を介した 2 要素認証も、テナントのポッド フリートの現在の状態に応じてサポートされます。

また、クライアントで Universal Broker を使用し、2 要素認証が構成されている場合のエンドユーザー エクスペリエンスについて説明している次のセクションも確認してください。現在の動作は、ポッドのゲートウェイ FQDN を直接使用する場合の動作とは異なります。

Horizon ポッドのみ

RADIUS と RSA SecurID の両方の認証がサポートされます。

Horizon Cloud on Microsoft Azure デプロイのみ

すべてのポッドがマニフェスト 3139.x 以降で、ポッドで [ポッドの編集] ウィザードを実行するときに RSA SecurID と RADIUS の両方のオプションが選択可能に表示されている場合、RSA SecurID と RADIUS の両方の認証がサポートされます。それ以外の場合は、RADIUS タイプのみがサポートされます。

Horizon ポッドと Horizon Cloud on Microsoft Azure デプロイの混在

混合フリートでサポートされる認証タイプは、Horizon Cloud on Microsoft Azure デプロイが RSA SecurID オプションを構成するための条件を満たしているかによって異なります。

- Horizon Cloud on Microsoft Azure デプロイがこれらの条件を満たしていない場合は、RADIUS 認証のみがサポートされます。
- Horizon Cloud on Microsoft Azure デプロイがこれらの条件を満たす場合、RADIUS と RSA SecurID の両方の認証がサポートされます。

満たすべき条件とは、ポッドがマニフェスト 3139.x 以降を実行しており、ポッドで [ポッドを編集] ウィザードを開いたときに、RSA SecurID オプションと RADIUS オプションの両方が表示され、選択可能であることです。

2 要素認証が構成されている場合

2 要素認証が含まれている場合、ポッドのゲートウェイ FQDN を直接使用する場合のフローとは少し異なる Universal Broker FQDN を使用すると、エンド ユーザーは 1 つの認証フローを経験します。

- Universal Broker 認証フローでは、エンド ユーザーは Windows Active Directory (AD) 認証情報を 2 回入力するように求められます。Universal Broker FQDN に最初に接続するときに 1 回入力し、構成された RADIUS または RSA SecurID システムで 2 要素認証を正常に完了した後にもう 1 回入力します。
- ポッドのゲートウェイ認証フローを使用する場合、エンド ユーザーは最初にポッドのゲートウェイ FQDN に接続するときに、Windows Active Directory (AD) 認証情報を 1 回入力するように求められます。

注： Universal Broker を使用するときに 2 つの Active Directory プロンプトが表示されないようにするには、VMware Workspace ONE Access と統合し、VMware Workspace ONE Access で 2 要素認証を構成することを検討してください。

現在サポートされていないユーザー認証およびアクセス方法

次のユーザー認証およびアクセス方法は、現在サポートされていません。

- スマート カード
- 証明書
- SAML 認証（VMware Workspace ONE との統合外）
- 現在のユーザーとしてログイン
- 匿名アクセス

サポート対象外のアイテムの 1 つがサポート対象になる場合、そのエントリは前のリストから削除され、サポートの発表は既存のクラウド接続ポッドを使用する現在のユーザー向け - Horizon Cloud Service リリースについてというタイトルのページに記載されます。このページでは、サポートが追加されたリリースに対応するセクションにステートメントが表示されます。

リモート デスクトップ機能

以下の機能は今回のリリースの Universal Broker ではサポートされていません。

- URL コンテンツ リダイレクト
- セッション共同作業

その他の機能

このリリースの Universal Broker では、次の機能もサポートされていません。

- キオスク モード
- タイミング プロファイル（ユーザー セッションのトラブルシューティングに使用）
- OPSWAT ベースのエンドポイント コンプライアンス チェック

Universal Broker のシステム要件

この記事では、Universal Broker の使用をサポートするために Horizon Cloud テナント環境が満たす必要のある詳細なシステム要件について説明しま要件は、Universal Broker を Horizon ポッド（Horizon Connection Server テクノロジー ベース）用に構成するか、Microsoft Azure の Horizon Cloud ポッド用に構成するかによってわずかに異なります。

注： Universal Broker のサポートの制限事項に関する最新情報については、Horizon Cloud - 既知の制限事項を参照してください。

Horizon Cloud Connector によって Horizon Cloud に接続されている Horizon ポッドの要件

Horizon Cloud Connector によってクラウド サービスに接続されている Universal Broker の使用をサポートするには、システム環境が次の要件を満たしている必要があります。

主要コンポーネントのソフトウェア バージョン：

- Horizon ポッド - Connection Server への Universal Broker プラグインのインストールで説明するように、各ポッドは、バージョン 7.11 以降の Horizon Connection Server を実行し、有効なライセンスを持ち、Connection Server に適切な Universal Broker プラグイン バージョンがインストールされている必要があります。

  各ポッドと Connection Server は、特定の Connection Server バージョンの製品ドキュメント（VMware Horizon ドキュメントまたは VMware Horizon 7 のドキュメント）に従って有効なインストールを行う必要があります。

- 各ポッドは、バージョン 1.6 以降の Horizon Cloud Connector を使用して Horizon Cloud にクラウド接続されている必要があります。1.6 は非常に古いバージョンの Horizon Cloud Connector であり、新しいポッドのオンボーディングではサポートされていないことに注意してください。このバージョンは、Universal Broker が利用可能になった最初のバージョンであるため、完全を期すためにここに記載されています。新しいオンボーディングは、Horizon Cloud Connector 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、本書の執筆時点で利用可能な最新の Horizon Cloud Connector バージョンです。

- コネクタのバージョン 1.8 または 1.9 に関する特記：Universal Broker は、コネクタで実行されているクラウド ブローカ クライアント サービス (CBCS) を使用してポッドと通信します。Horizon ポッドが Horizon Cloud Connector 1.8 または 1.9 を使用している場合、フル機能プロファイルを使用して Horizon Cloud Connector をデプロイした場合、または基本機能プロファイルを使用してデプロイし、コネクタ用にクラウド ブローカ クライアント サービス (CBCS) を手動で有効にした場合、Universal Broker がサポートされます。このセットアップで CBCS を手動で有効にする手順については、バージョン 1.8 または 1.9 のサービスを手動で有効にするを参照してください。

- ネイティブの Amazon EC2 デプロイで Horizon Cloud Connector を使用してクラウド接続された Horizon ポッドに関する特記：そのポッドに Universal Broker を使用するには、そのアプライアンスで

クラウド ブローカ クライアント サービス (CBCS) の使用を手動で有効にする必要があります。これは、そのサービスがネイティブの Amazon EC2 デプロイでデフォルトで無効になるためです。このセットアップで CBCS の使用を手動で有効にする方法については、ネイティブの Amazon EC2 の Horizon Cloud Connector のサービスを手動で有効にするを参照してください。

特定のエンドユーザー シナリオごとの要件：

Universal Broker で 2 要素認証を使用する場合

- Universal Broker でいずれかのエンド ユーザーに 2 要素認証を使用する場合は、Horizon ポッド上のセキュリティ サーバを外部 Unified Access Gateway アプライアンス（バージョン 3.8 以降）に置き換える必要があります。
- また、Universal Broker がサポートする適切な 2 要素認証サービスを使用して、外部 Unified Access Gateway を構成する必要があります。Universal Broker 環境で 2 要素認証を実装する際のベスト プラクティスに記載されているガイダンスと基準に従ってください。

ユーザーがすべて内部ユーザーで、直接接続を使用する必要がある場合

すべてのユーザーが常に内部ネットワークからアクセスする場合は、直接接続で Universal Broker を使用できます。直接接続では、このようなエンド ユーザーのセッションは、ユーザーの Horizon Client または Web クライアントと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）の間で直接確立されます。この場合、コンソールの [ブローカ] - [ネットワーク範囲] 機能を使用して IP アドレスも指定し、Universal Broker がエンドユーザー トラフィックが内部ネットワークから来ていることを認識している限り、Unified Access Gateway インスタンスは必要ありません。これらの IP アドレスを指定せず、エンド ユーザーがすべて内部ユーザーの場合、セッションに接続するには、ポッドに内部 Unified Access Gateway アプライアンス（バージョン 3.8 以降）が必要です。どちらの場合でも、セキュリティ サーバは必要ありません。ポッドに含まれるセキュリティ サーバを削除することもできます。

内部ユーザーと外部ユーザーの両方があり、Universal Broker で 2 要素認証を構成したい場合

[ブローカ] - [ネットワーク範囲] 機能を使用して IP アドレスを指定する場合、Universal Broker は接続中のユーザーがいつ内部ネットワーク上に存在するかを判断でき、それをそのユーザーの直接接続と見なします。逆に、[ブローカ] - [ネットワーク範囲] で IP アドレスを指定しない場合、Universal Broker はすべてのエンド ユーザー接続を外部として扱い、外部 Unified Access Gateway アプライアンスに接続を送信します。

前述のシナリオに従って、Unified Access Gateway が関係している場合：

- 各 Unified Access Gateway インスタンスを、ペアリングされた Connection Server への接続要求に対するプロキシ サーバとして構成します。各 Unified Access Gateway インスタンスが 1 つのポッドのみとペアリングされていることを確認します。
- ポッドに内部 Unified Access Gateway インスタンスのみが含まれている場合（外部インスタンスなし）、Universal Broker は [ブローカ] - [ネットワーク範囲] で指定された IP アドレス範囲をオーバーライドし、IP アドレスに関係なく、すべてのユーザーをその内部 Unified Access Gateway インスタンスにルーティングします。[ブローカ] - [ネットワーク範囲] で IP アドレス範囲が指定されていない場合、仮想デスクトップとリモート アプリケーションの起動はその内部 Unified Access Gateway によって異なります。

Unified Access Gateway 製品のドキュメントは、https://docs.vmware.com/jp/Unified-Access-Gateway/index.html にあります。

DNS 名、ポート、プロトコル：

- Horizon ポッド - Universal Broker の DNS、ポートおよびプロトコルの要件で説明するように、各ポッドが必要なポートとプロトコルで構成されている必要があります。
- Unified Access Gateway が必要なシナリオで Universal Broker がエンドユーザー トラフィックを適切にルーティングすることをサポートするには、ポッドが Unified Access Gateway で構成されている場合、すべての DNS 名が内部および外部 DNS サーバに適切にマッピングされていることを確認する必要があります。ポッドが内部と外部の両方の Unified Access Gateway を構成している場合は、内部と外部の構成で異なる FQDN を指定することも、同じ FQDN とスプリット DNS ゾーンで構成されたポッドのロード バランサを使用して構成することもできます。

デスクトップ プール：

エンドユーザー セッションを起動するには、デスクトップ プールは、参加しているポッド上に、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に基づいて構成する必要があります。さらに、Horizon ポッド - マルチクラウド割り当てに使用する既存のデスクトップ プールを準備するで説明するように、プールの構成は Universal Broker の要件を満たす必要があります。

Microsoft Azure Horizon Cloud ポッドの要件

Universal Broker で使用するには、Microsoft Azure に参加している各 Horizon Cloud ポッドが次の要件を満たしている必要があります。

- 2020 年 7 月リリースのマニフェスト (2298.0) 以降で Microsoft Azure に新規でデプロイされている必要があります

  注： Universal Broker は、[すべて] の Horizon Cloud ポッドがマニフェスト 2298.0 以降でデプロイされている場合にのみ使用できます。いずれの Horizon Cloud ポッドがマニフェスト 2298.0 より前でデプロイされている場合、Universal Broker は Horizon Cloud ポッドで使用可能な仲介オプションではありません。

- インターネットからのエンドユーザー接続を許可する場合、または 2 要素認証を使用する場合は、ポッドで外部 Unified Access Gateway 構成が必要です。

  注： 各 Unified Access Gateway インスタンスが 1 つのポッドのみとペアリングされていることを確認します。

  注： ポッドに内部 Unified Access Gateway インスタンスだけが含まれる場合、Universal Broker は [ブローカ] ページの [ネットワーク範囲] タブで定義されたネットワーク ポリシーを上書きし、IP アドレスに関係なく、すべてのユーザーをその Unified Access Gateway インスタンスにルーティングします。

特定のユースケースをサポートするには、ポッドが次の追加要件を満たしている必要があります。

- 内部および外部のネットワーク トラフィックを Universal Broker からそれぞれの内部および外部の DNS サーバにルーティングするには、各ポッドで内部と外部の両方の Unified Access Gateway インスタンスが構成されている必要があります。内部および外部の Unified Access Gateway インスタンスは、別の FQDN を使用して構成することも、同じ FQDN およびスプリット DNS ゾーンで構成されたポッドのロード バランサを使用して構成することもできます。
- Universal Broker で 2 要素認証を使用するには、適切な 2 要素認証サービスを使用して、ポッドに少なくとも 1 つの外部 Unified Access Gateway インスタンスが構成されている必要があります。同じ 2 要素認証サービスを使用するには、参加しているすべてのポッドにまたがるすべての外部 Unified Access Gateway インスタンスを構成する必要があります。Universal Broker 環境で 2 要素認証を実装する際のベスト プラクティスに記載されているガイダンスと基準に従ってください。

既存の Horizon Cloud ポッドへのゲートウェイ構成の追加については、デプロイ済みの Horizon Cloud ポッドへのゲートウェイ構成の追加を参照してください。

- 地域の Universal Broker インスタンスに必要な DNS 名が解決可能であり、アクセス可能であるように構成されている。Microsoft Azure での Horizon Cloud ポッドの DNS の要件の「ポッドのデプロイと操作に関する DNS の要件」の表を参照してください。
- 必要なポートとプロトコルが構成されている (2019 年 9 月リリースのマニフェスト以降の Horizon Cloud ポッドのポートとプロトコルの要件の「Universal Broker で必要なポートとプロトコル」セクションを参照)
- 健全な状態。[キャパシティ] ページで、健全な状態のポッドの場合は [ステータス] 列に緑色のドットが表示され、ポッドがオンラインで、準備ができていることを示します。

クライアント要件

Universal Broker に関連するクライアントの要件については、Horizon Cloud - 利用可能な環境、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、および互換性情報のトピック内に記載されている Horizon Client の情報を参照してください。

Horizon ポッド - Universal Broker の DNS、ポートおよびプロトコルの要件

参加している Horizon ポッド（Horizon Connection Server テクノロジー ベース）の仲介コンポーネントとシステム コンポーネントとの間の継続的な通信を確立するために、Universal Broker には特定のポートとプロトコルの要件があります。また、Universal Broker で構成された環境では、一部の特定の DNS 名に Horizon Cloud Connector がアクセスできる必要があります。

DNS の要件については、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 上の Universal Broker クライアントは、ポート 443 を介して Universal Broker サービスとの永続的な WebSocket 接続を確立します。Universal Broker クライアントは、ランダムに選択されたポートを介してサービスから接続要求を受信します。

次に、Universal Broker クライアントは、ランダムに選択された別のポートを介して、Connection Server 上の Universal Broker プラグインにリクエストを転送します。Universal Broker プラグインは、プラグインのインストール中に指定されたポートを介してこれらの着信要求を待機します。

Universal Broker のシステム アーキテクチャとトラフィック フローの詳細については、Universal Broker のシステム アーキテクチャとコンポーネントを参照してください。

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
Horizon Cloud Connector の Universal Broker クライアント	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、その後の継続的な接続には WebSocket	Universal Broker サービスとの永続的な WebSocket 接続を確立するために使用されます。
Horizon Cloud Connector の Universal Broker クライアント	使用可能なポートからランダムに選択されます。	Connection Server 上の Universal Broker プラグイン	Universal Broker プラグインのインストール時に指定されます。ポートが指定されていない場合は、デフォルトでポート 33443 が使用されます。	HTTPS	Universal Broker クライアントによって Universal Broker サービスから転送された着信接続要求を待機するために Universal Broker プラグインによって使用されます。

Horizon 制御プレーン テナントの Universal Broker サービスのセットアップ

この記事では、テナントの Universal Broker を設定するために必要なフローの概要について説明します。実際の手順は、テナントのポッド デプロイのタイプによって異なります。

Microsoft Azure の Horizon Cloud ポッドの場合

注： テナントのすべての Horizon Cloud ポッドがポッド マニフェスト 2298.0 以降である場合、テナントでの Universal Broker のセットアップがサポートされます。Universal Broker の正常な設定をサポートするには、すべての Horizon Cloud ポッドがオンラインで、健全な状態で準備が整っている必要があります。

1 Horizon Universal Console を使用した Universal Broker の有効化の開始で説明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 Horizon Universal Console にログインし、[ブローカ] ページに移動して、[開始] をクリックします。

3 Universal Broker の設定に記載されている手順に従って設定を完了します。

Horizon ポッドの場合

Horizon ポッド（Horizon Connection Server テクノロジー ベース）の構成にはいくつかの手順が含まれ、以降のトピックで詳しく説明します。

1 Horizon ポッド - Connection Server への Universal Broker プラグインのインストール

2 Horizon ポッド - Universal Broker で使用する Unified Access Gateway を構成する

3 Horizon Universal Console を使用した Universal Broker の有効化の開始

4 Universal Broker の設定

Horizon ポッド - Universal Broker で使用する Unified Access Gateway を構成する

このトピックでは、Universal Broker で使用するために、Horizon ポッド内の Unified Access Gateway インスタンスを構成する方法について説明します。Universal Broker に必要なトンネル サーバとプロトコルのリダイレクトをサポートするために、各 Unified Access Gateway インスタンスで必要な JSON Web トークンの設定を構成する手順を実行します。

注： 次の手順は、Horizon Connection Server テクノロジー ベースの Horizon ポッド内の Unified Access Gateway インスタンスにのみ必要です。Microsoft Azure の Horizon Cloud ポッドの場合、JSON Web トークンの設定は、ポッドのデプロイ時に自動的に構成されます。（Horizon Connection Server テクノロジー ベースではない）Horizon Cloud ポッド内の Unified Access Gateway インスタンスに対する JSON Web トークンの構成を追加で行う必要はありません。

デフォルトの設計では、Universal Broker は、テナントのポッド フリートの各ポッドでまったく同じ 2 要素認証設定を使用することを想定しています。また、設計上、Universal Broker は、2 要素認証設定で構成されている場合、認証要求を形成し、それを外部 Unified Access Gateway インスタンスに送信します。次にそのインスタンスは、設定で構成されている認証サーバと通信して、特定の認証アクションを処理します。Unified Access Gateway は、次に認証サービスの応答を Universal Broker にリレーします。

そのため、Universal Broker に加えて 2 要素認証が必要な場合は、テナントのポッド フリート内のすべてのポッドで、すべての外部 Unified Access Gateway インスタンスにまったく同じ認証サービスを構成する必要があります。Horizon ポッドのみで構成されているフリートの場合、Universal Broker はすべての Unified Access Gateway インスタンスで RADIUS サービスまたは RSA SecurID サービスの使用をサポートできます。

ただし、テナントに Horizon ポッドと Horizon Cloud ポッドの両方で構成される混合ポッド フリートがある場合は、使用できるオプションは Horizon Cloud on Microsoft Azure デプロイが RSA SecurID オプションを使用する条件を満たしているかどうかによって異なることに注意してください。すべての Horizon Cloud ポッドがマニフェスト 3139.x 以降で、[ポッドを編集] ウィザードに RSA SecurID オプションが表示されている場合は、すべてのポッドが RSA SecurID タイプを使用するように構成できます。それ以外の場合は、すべてのポッド フリートで同一の認証サービスを使用する要件を満たすために RADIUS を使用する必要があります。

前提条件

- サポートするエンドユーザーのユースケースに応じて、テナントのポッド フリートの各 Horizon ポッドで、適切な Unified Access Gateway アプライアンスを構成していることを確認します。ユースケースの簡単な説明については、Horizon Cloud Connector によって Horizon Cloud に接続されている Horizon ポッドの要件を参照してください。
- これらの Unified Access Gateway アプライアンスがバージョン 3.8 以降を実行しており、Horizon Cloud Connector によって Horizon Cloud に接続されている Horizon ポッドの要件に記載されているその他の関連するすべての Unified Access Gateway 要件を満たしていることを確認します。
- 各 Unified Access Gateway インスタンスとそれに対応するポッドとのペアリングを検証するには、Unified Access Gateway インスタンスに直接接続して、仮想デスクトップにアクセスできることを確認します。

手順

1. Unified Access Gateway 管理コンソールにログインします。
2. [手動構成] セクションで、[選択] をクリックします。
3. [詳細設定] で、[JWT 設定] のギアボックスをクリックします。
4. ギアボックスをクリックした後：
   - Unified Access Gateway ソフトウェアが 2209 より前のバージョンの場合は、[追加] をクリックします。
   - Unified Access Gateway ソフトウェアが 2209 以降の場合は、[JWT コンシューマの追加] をクリックします。Unified Access Gateway 管理ユーザー インターフェイスは、バージョン 2209 で初めて変更されました。

5 表示されるユーザー インターフェイス ボックスで、次の設定を指定します。

設定	説明
Name	構成セットのわかりやすい名前を入力します。
Issuer	Horizon Console に表示される Horizon ポッドのクラスタ名を入力します。 **注意：** このフィールドは、Unified Access Gateway 管理ユーザー インターフェイスでは大文字と小文字が区別されます。 クラスタ名は、Horizon Console から取得したとおりに正確に入力する必要があります。 Unified Access Gateway ユーザー インターフェイスは、フィールドで大文字と小文字が区別されることについて警告を表示せず、大文字と小文字が正しいかどうかを検証しません。 この大文字と小文字の区別は、Horizon Console に表示される [Cluster] という単語にも適用されます。 Horizon Console に大文字の [C] と小文字の [luster] を含む単語が表示されている場合は、この [発行者] フィールドで正確に一致させ、この [発行者] フィールドに **`Cluster`** と入力する必要があります。 この [発行者] フィールドに、Horizon Console に表示される名前と大文字と小文字が正確に一致する名前を入力しないと、Universal Broker のダウンストリームで問題が発生し、エンド ユーザーは Universal Broker FQDN を使用してデスクトップやアプリケーションを起動できなくなります。 Horizon Console でポッドのクラスタ名を見つけるには、Horizon Console の [ダッシュボード] 領域に移動し、ユーザー インターフェイスの上部の縦の領域を確認します。 Horizon Console 内のポッドのクラスタ名の場所を次に示します。 表示される名前の [Cluster] 部分が、先頭の大文字とそれに続く小文字の組み合わせになっていることがわかります。 表示されている名前を Unified Access Gateway 管理ユーザー インターフェイスのこの [発行者] フィールドに正確に入力する必要があります。[発行者] フィールドでは、名前が正しく入力されているかどうかは検証されません。 
Dynamic Public key URL	ここで入力する値は、ポッドの Connection Server ホスト名、または Connection Server FQDN、またはローカルのロード バランサ（ポッドに複数のゲートウェイ インスタンスがある場合）から取得します。 **`https://<Horizon pod FQDN>/broker/publicKey/protocolredirection`** と入力します。ここで、*<Horizon pod FQDN>* はポッドの一意の FQDN（完全修飾ドメイン名）に置き換えます。通常、FQDN は次のように定義されます。 ■ ポッドに Unified Access Gateway インスタンスが 1 つしかない場合は、そのインスタンスのペアリングされた Connection Server のアドレスを FQDN として指定します。 ■ ポッドに複数の Unified Access Gateway インスタンスがある場合は、ローカル ロード バランサのアドレスを FQDN として指定します。

設定	説明
Public key URL thumbprints	このフィールドは認証にパブリック キー URL を使用することを指定します。 ポッドの Connection Server 証明書を認証に使用するには、前述の [動的パブリック キー URL] に使用した Connection Server に対する Horizon ポッドの Connection Server 証明書の SHA1 サムプリントを入力します。 **注：** 認証には、[パブリック キー URL のサムプリント] または [信頼されている証明書] のいずれかを設定できます。両方のオプションを設定する必要はありません。
Trusted Certificates	認証に Horizon ポッドの証明書以外の証明書を使用するには、(+) アイコンをクリックして、信頼されている証明書を追加します。 **注：** 認証には、[信頼されている証明書] または [パブリックキー URL のサムプリント] のいずれかを設定できます。両方のオプションを設定する必要はありません。
Public key refresh interval	最良の結果を得るには **900** と入力します。この値は、更新間隔を 900 秒つまり 15 分に設定します。
Static public keys	このオプションは、デフォルト値のままにします。

6 [保存] をクリックして、[閉じる] をクリックします。

7 Universal Broker に 2 要素認証を使用する場合は、[認証設定] の [表示] 設定を有効にします。次に、Universal Broker でサポートされている 2 要素認証サービスの 1 つの設定を有効にして構成します。現在サポートされているサービスは、RADIUS と RSA SecurID の 2 つです。

注： 参加しているすべてのポッドの外部 Unified Access Gateway インスタンスで適切な 2 要素認証サービスを構成する必要があります。参加しているポッド内のすべての外部 Unified Access Gateway インスタンスの構成は互いに一致する必要があり、他のすべての参加しているポッドの外部 Unified Access Gateway インスタンスの構成と同じである必要があります。そうでないと、Universal Broker サービスへの認証が失敗します。

たとえば、Universal Broker で構成された Horizon ポッドに RADIUS 認証を使用する場合は、参加しているすべての Horizon ポッドにわたって、すべての外部 Unified Access Gateway インスタンスで同じ RADIUS サービスを構成する必要があります。参加している一部のポッドで RADIUS を構成し、他のポッドで RSA SecurID を構成することはできません。

Horizon ポッド - Connection Server への Universal Broker プラグインのインストール

Horizon ポッドが Universal Broker によって仲介されたマルチクラウド割り当てに参加できるようにするには、そのポッドの各 Connection Server インスタンスに必要な Universal Broker プラグインをインストールする必要があります。Universal Broker プラグインは、仲介サービスとポッド内の Connection Server インスタンス間の通信をサポートします。

注： Universal Broker プラグインのインストールは、Horizon Connection Server テクノロジー ベースの Horizon ポッドの場合にのみ必要です。Microsoft Azure の Horizon Cloud ポッドは Universal Broker プラグインを必要としません。

Universal Broker プラグインをインストールするときは、次の考慮事項を確認します。

- インストーラの EXE ファイル内のコードには、Connection Server の特定のバージョンでインストーラの EXE ファイルを実行できるかどうかを決定するフラグが含まれているため、Connection Server のバージョンと互換性のあるバージョンの Universal Broker プラグイン インストーラの EXE ファイルを実行する必要があります。

  Horizon YYMM のバージョン管理と数値スタイルのバージョン管理の関係については、KB2143853 を参照してください。

Connection Server バージョン用の Universal Broker プラグイン インストーラのバージョンと VMware Customer Connect でのダウンロード場所

Universal Broker プラグイン インストーラは、VMware Customer Connect からダウンロードされます。次の表の各 URL からダウンロード ページに移動できます。Universal Broker プラグインがそのページの下部にあります。

ブラウザでこれらの URL のいずれかを読み込んだら、一番下までスクロールして、Universal Broker プラグイン エントリとそのバージョン番号を確認します。[今すぐダウンロード] ボタンをクリックして、そのバージョンをダウンロードします。[今すぐダウンロード] をクリックするときに、VMware Customer Connect 認証情報を使用してログインしていない場合は、ログイン ユーザー インターフェイスが最初に表示されます。

Connection Server の実行バージョン：	Connection Server で実行される Universal Broker プラグイン インストーラ EXE：	VMware Customer Connect 内の場所 - ダウンロード ページの一番下までスクロールして Universal Broker プラグインを表示
2309 (8.11)	22.01 - 2206 (8.6) と同じ	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-240&productId=716&rPId=112315
2306 (8.10)	22.01 - 2206 (8.6) と同じ	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-240&productId=716&rPId=112315
2303 (8.9)	22.01 - 2206 (8.6) と同じ	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-230&productId=716&rPId=112315
2212 (8.8)	22.01 - 2206 (8.6) と同じ	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-230&productId=716&rPId=112315

Connection Server の実行バージョン：	Connection Server で実行される Universal Broker プラグイン インストーラ EXE：	VMware Customer Connect 内の場所 - ダウンロード ページの一番下までスクロールして Universal Broker プラグインを表示
2209 (8.7)	22.01 - 2206 (8.6) と同じ	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-230&productId=716&rPId=112315
2206 (8.6)	22.01	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-220&productId=716&rPId=112315
2111 (8.4)	21.06	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-210&productId=716&rPId=112315
2106 (8.3)	21.06 - 2111 (8.4) と同じ	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-210&productId=716&rPId=112315
2103 (8.2)	21.03	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-110&productId=716&rPId=112315
2012 (8.1)	21.01	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-190&productId=716&rPId=112315
7.13	20.10	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-180&productId=716&rPId=112315

Connection Server の実行バージョン：	Connection Server で実行される Universal Broker プラグイン インストーラ EXE：	VMware Customer Connect 内の場所 - ダウンロード ページの一番下までスクロールして Universal Broker プラグインを表示
7.12 または 2006 (8.0)	20.3	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-170&productId=716&rPId=112315
7.11	19.4	https://customerconnect.vmware.com/downloads/details?downloadGroup=HCS-CC-150&productId=716&rPId=112315

- ポッドに複数の Connection Server インスタンスがある場合は、各 Connection Server インスタンスに Universal Broker プラグインをインストールする必要があります。
- 参加するポッド内のすべての Connection Server インスタンスに同じバージョンのプラグインをインストールする必要があります。たとえば、1 つの Connection Server インスタンスでプラグインを新しいバージョンにアップグレードする場合、ポッド内の他のすべての Connection Server インスタンスでプラグインを同じバージョンにアップグレードする必要があります。
- 参加しているポッドに新しい Connection Server インスタンスを追加する場合、新しい Connection Server インスタンスにプラグインをインストールする必要があります。
- Connection Server のアップグレード中に、既存のプラグインのインストールがすべて失われます。Horizon デプロイをアップグレードする場合は、各 Connection Server インスタンスを新しいバージョンにアップグレードした直後にプラグインを再インストールする必要があります。

  たとえば、Connection Server インスタンスをバージョン 8.2 (2103) にアップグレードする場合は、それらの Connection Server インスタンスにバージョン 21.03 のプラグインをインストールする必要があります。
- プラグインのインストール中に、インストーラは Connection Server サービスを再起動します。その時点で、システムは Connection Server 上のすべての管理コンソール セッションをログアウトします。
- 現在、Universal Broker プラグインは IPv4 のみに対応しています。
- Universal Broker プラグインがインストールされている Connection Server インスタンスで LDAP 構成を使用する場合は、次のガイドラインに従ってください。
  - LDAP 構成のバックアップ コピーを作成することに加え、現在の Connection Server インスタンスの仮想マシン スナップショットを作成します。バックアップを使用して LDAP 構成を以前の状態にリストアする場合、スナップショットを使用して、リストアする LDAP 構成に Universal Broker プラグインが機能するために必要な情報を入力できます。
  - LDAP 構成を以前の状態にリストアする場合は、プラグインが Connection Server にインストールされた後に作成された LDAP バックアップのみを使用してください。

- LDAP 構成を Universal Broker ラグインのインストール前の状態にリストアすると、リストアされた LDAP 構成にプラグインに必要な特定の情報が失われます。そのため、プラグインは機能しません。

Connection Server のバージョンに適したバージョンの Universal Broker プラグインをダウンロードしたら、次の手順を使用して、ポッド内の Connection Server インスタンスにプラグインをインストールします。

- Connection Server インスタンスの一括デプロイで Universal Broker プラグインをサイレント インストールするには、次のコマンドを使用します。*X.X.X* をバージョン番号に置き換え、*yyyyyyyy* をダウンロードしたインストーラのビルド番号に置き換えます。*<portNumber>* には、プラグインが Universal Broker クライアントからの着信要求をリッスンして受け入れるために使用する TCP ポートを入力します。

  ```
  horizon-universal-broker-plugin-X.X.X-yyyyyyyy-x64.exe /s /v"LISTENPORT=<portNumber> /qn"
  ```

- 個々の Connection Server インスタンスに Universal Broker プラグインをインストールするには、このトピックの後半で説明されている番号付きの手順を実行します。

前提条件

Connection Server インスタンスで Universal Broker プラグイン インストーラを実行する前に、次の点を確認します。

- Connection Server インスタンスがバージョン 7.11 以降を実行している。
- Connection Server に対して Horizon 管理者とローカル管理者の両方の権限を持っている。インストーラは、これらの両方の権限を持つ管理者によって開始された場合にのみ実行されます。
- このページですでに説明したように、Universal Broker プラグインを実行して、特定のバージョンの Connection Server にインストールするための互換性のあるバージョンの Universal Broker プラグイン がある。

手順

1. 必要に応じて、ダウンロードしたプラグイン インストーラ ファイルを Connection Server に配置します。
2. `.exe` インストーラ ファイルを実行します。
3. インストーラのウィザードのようこそ画面で、[次へ] をクリックします。
4. エンド ユーザー使用許諾契約を承諾し [次へ] をクリックします。

5 [構成] 画面で、必要なポート情報を指定します。

a Universal Broker プラグインが Universal Broker クライアントからの着信要求をリッスンして受け入れるために使用する TCP ポート番号を入力します。

注： インストーラは、指定されたポートが使用可能であることを検証します。ポートですでにプロセスが実行されている場合は、警告メッセージが表示され、インストールが停止します。インストールを再開するには、使用可能な TCP ポートを指定する必要があります。

b 指定したポートを介した着信接続を許可するために必要なファイアウォール例外をインストーラで構成する場合は、[Windows ファイアウォール例外を自動的に設定する] を選択します。ファイアウォール例外を手動で構成する場合は、このオプションを選択解除します。

注： Windows ファイアウォールの例外は、インストーラで構成するか、自分で構成するかに関わらず Universal Broker では必須です。

c [次へ] をクリックします。

6 ウィザードの残りの画面に表示されるプロンプトに従って、Connection Server への Universal Broker プラグインのインストールを完了します。

次のステップ

重要： 後で Universal Broker プラグインまたは Connection Server インスタンスをアンインストールする場合は、アンインストールを次の順序で実行します。

1 まず、Universal Broker プラグイン をアンインストールします。

2 次に、Connection Server ソフトウェアをアンインストールします。

最初に Connection Server をアンインストールすると、システム エラーが発生し、Universal Broker プラグインをアンインストールできなくなります。

注： Universal Broker プラグインが Universal Broker クライアントからの着信要求をリッスンするために使用するポートを変更する場合は、次の手順を実行します。

1 Connection Server の LDAP 構成で、`pae-RCXServerPort` プロパティの値を新しいポート番号に変更します。

2 Connection Server を再起動します。

3 必要に応じて、対応する Windows ファイアウォールの例外を更新して、新しいポートを介した着信トラフィックを許可します。

新しいポート構成は、Connection Server と Universal Broker プラグインが再起動シーケンスを完了した後に有効になります。

Horizon Universal Console を使用した Universal Broker の有効化の開始

Horizon Cloud テナントの Universal Broker を構成するために必要な手順は、コンソールの [ブローカ] ページを使用して Universal Broker を明示的に有効にし、セットアップ ウィザードを開始することです。

テナントのポッド フリートに次の 1 つ以上がある場合は、コンソールの [ブローカ] ページから Universal Broker のセットアップを開始できます。

- Horizon ポッド（Horizon Connection Server テクノロジー ベース）
- すべて 2298.0 以降のマニフェストを実行している、Microsoft Azure の Horizon Cloud ポッド（ポッド マネージャ テクノロジーに基づく）。

注： Universal Broker 構成はテナント全体の設定です。ポッド タイプの [ブローカ] ページで [開始] をクリックすると、テナントのポッド フリート内の指定されたタイプのすべてのポッドに Universal Broker 構成が適用されます。

前提条件

以下を検証します:

- テナントのポッド フリートが上記の特性を満たしていること。Horizon Cloud ポッドの場合は、すべてのポッドがオンラインで、健全な状態で準備が整っていることを確認します。それによって、セットアップ プロセスを成功させることができます。
- Horizon Cloud 環境に Active Directory ドメインを登録し、Horizon Cloud スーパー管理者ロールを Active Directory ドメイン グループに割り当てていること。第 1 世代のテナント - Horizon Cloud 制御プレーン テナントで最初に必要な Active Directory ドメイン登録の実行を参照してください。

  コンソールでは、これらの手順を完了するまで [ブローカ] ページにアクセスできなくなります。
- [ブローカ] ページには、Universal Broker を有効にしてセットアップ ウィザードを開始するための青いボタンがあります。セットアップ ウィザードを開始するためのボタンが表示されない場合、テナントの Universal Broker はすでに有効になっています。

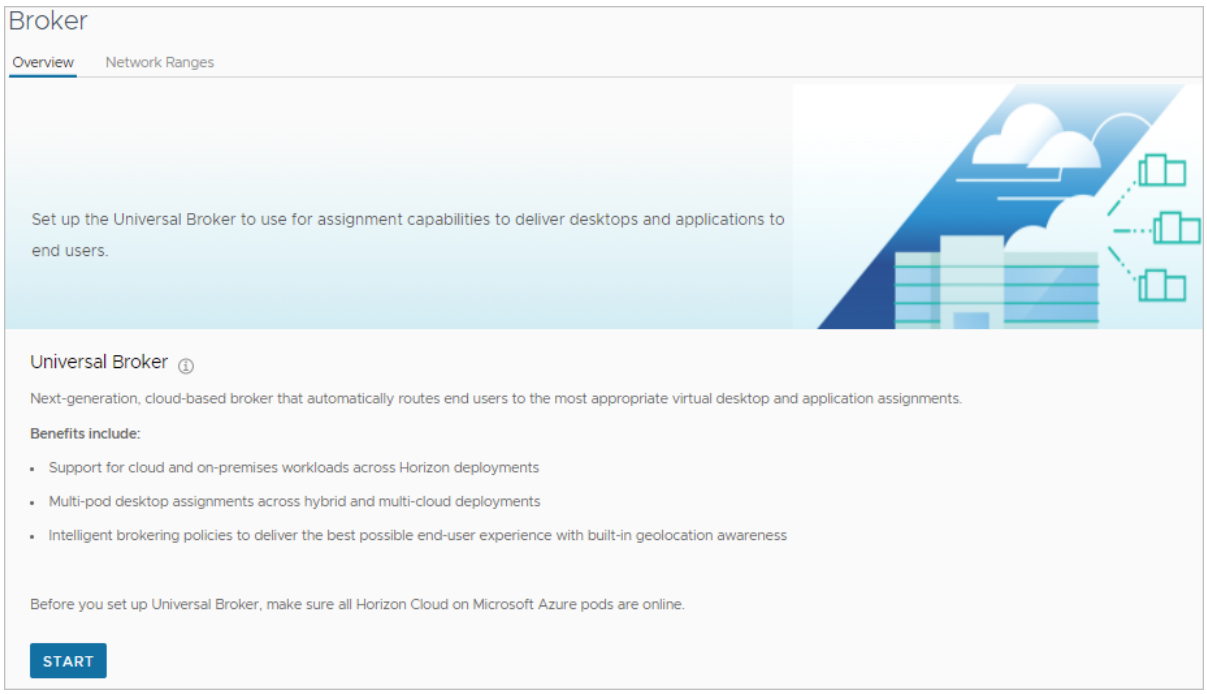
重要： Horizon Cloud ポッドの場合、Universal Broker の正常なセットアップをサポートするには、[ブローカ] ページの [開始] ボタンをクリックする前に、すべての Horizon Cloud ポッドがオンラインで、健全な状態で準備が整っていることを確認します。Universal Broker サービスは、ポッドとの通信を行い、セットアップ プロセスを完了するためにポッドでいくつかの構成手順を実行する必要があります。いずれかの Horizon Cloud ポッドがオフラインまたは使用できない場合、Universal Broker のセットアップは失敗します。

手順

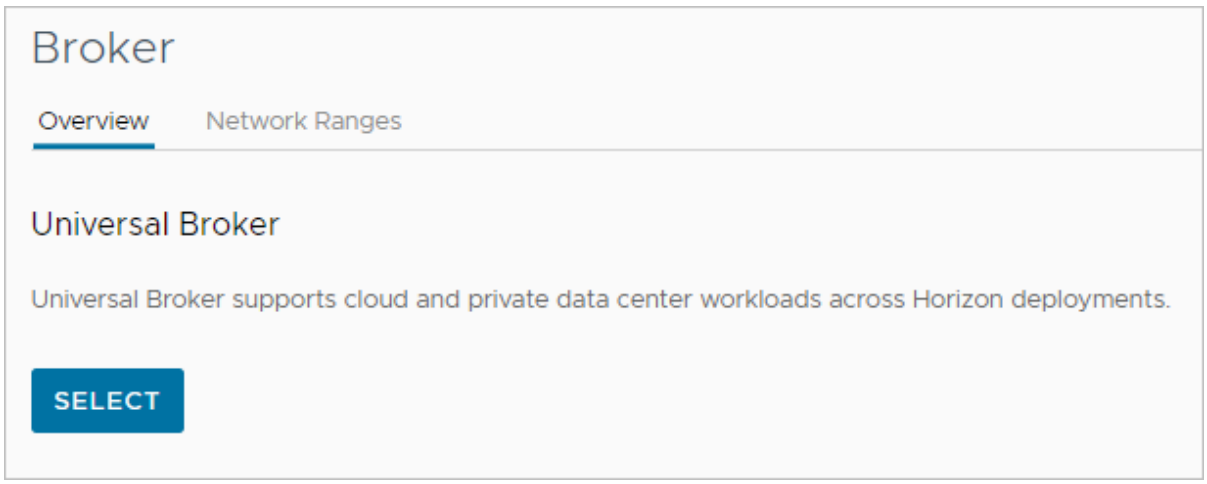
1 コンソールで、[設定] - [ブローカ] に移動します。

  [ブローカ] ページが表示されます。このページの実際の表示は、Universal Broker をセットアップするポッドのタイプや、すでに別のポッド タイプにブローカを選択しているかどうかなど、さまざまな要因によって異なります。

  たとえば、次のスクリーンショットは、ポッド フリートにポッド マニフェスト 2298.0 以降の Horizon Cloud ポッドのみがあり、他のポッドがない場合の [ブローカ] ページを示しています。



次のスクリーンショットは、ポッド フリートに Horizon ポッドのデプロイしかない場合のブローカ選択ページを示しています。



重要： Horizon Cloud ポッドの場合、Universal Broker の正常なセットアップをサポートするには、[ブローカ] ページの [開始] ボタンをクリックする前に、すべての Horizon Cloud ポッドがオンラインで、健全な状態で準備が整っていることを確認します。Universal Broker サービスは、ポッドとの通信を行い、セットアップ プロセスを完了するためにポッドでいくつかの構成手順を実行する必要があります。いずれかの Horizon Cloud ポッドがオフラインまたは使用できない場合、Universal Broker のセットアップは失敗します。

2 [開始] をクリックして、セットアップを開始します。

結果

[開始] をクリックすると、システムのバックエンドでクラウド プレーンのテナント レコードが更新され、このテナント環境で Universal Broker が有効になったことが反映されます。

この時点で、コンソールには Universal Broker 構成ウィザードがすぐに表示され、完了することができます。ウィザードの指示に従って構成設定を完了します。

次のステップ

- Universal Broker の設定の説明に従って、ブローカ構成ウィザードの手順を完了します。

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

このトピックでは、Universal Broker サービスに対して 2 要素認証を構成するために使用できる概要の手順とベスト プラクティスについて説明します。

Universal Broker での 2 要素認証の仕組み

デフォルトでは、Universal Broker は Active Directory のユーザー名とパスワードのみを使用してユーザーを認証します。追加の認証サービスを指定することで、オプションの 2 要素認証を実装できます。

サービス リリース バージョン 2203 の時点で、Universal Broker は Horizon デプロイと Horizon Cloud on Microsoft Azure デプロイの両方で次の 2 要素認証サービスをサポートしています。

- RADIUS
- RSA SecurID

注： Horizon Cloud on Microsoft Azure デプロイで RSA SecurID をサポートするには、それらのポッドでマニフェスト 3139.x 以降が実行されている必要があります。また、それらのポッドで [ポッドを編集] を実行すると、[ゲートウェイ設定] で選択する RSA SecurID オプションが表示されます。

Universal Broker は、ネットワーク ユーザーの 2 要素認証を実行するときに、参加している各ポッド内の外部 Unified Access Gateway インスタンスの構成に依存します。内部 Unified Access Gateway インスタンスを構成して内部ネットワーク ユーザーの認証とルーティングを処理することもできますが、Universal Broker では、その 2 要素認証は、外部 Unified Access Gateway インスタンスで構成されている認証サービスに基づきます。

注： 参加しているすべてのポッドの外部 Unified Access Gateway インスタンスで適切な 2 要素認証サービスを構成する必要があります。参加しているポッド内のすべての外部 Unified Access Gateway インスタンスの構成は互いに一致する必要があり、他のすべての参加しているポッドの外部 Unified Access Gateway インスタンスの構成と同じである必要があります。そうでないと、Universal Broker サービスへの認証が失敗します。

たとえば、Universal Broker で構成された Horizon ポッドに RADIUS 認証を使用する場合は、参加しているすべての Horizon ポッドにわたって、すべての外部 Unified Access Gateway インスタンスで同じ RADIUS サービスを構成する必要があります。参加している一部のポッドで RADIUS を構成し、他のポッドで RSA SecurID を構成することはできません。

外部ネットワークと内部ネットワークの両方でユーザーの 2 要素認証を有効にする場合

1 Universal Broker 環境内の各ポッドに対して、少なくとも 1 つの外部 Unified Access Gateway インスタンスを構成します。すべてのポッドにわたって、すべての外部 Unified Access Gateway インスタンスで同じ 2 要素認証サービスを構成します。

次のような、特定のユースケースの構成ガイドラインに従います。テナントのフリートが以下の場合：

Horizon ポッドのみ

すべてのポッドにわたって、すべての外部 Unified Access Gateway インスタンスで RADIUS または RSA SecurID サービスのいずれかを構成します。

Horizon Cloud on Microsoft Azure デプロイのみ

すべてのポッドにわたって、すべての外部 Unified Access Gateway インスタンスで同じ 2 要素認証サービスを構成します。すべてのポッドがマニフェスト 3139.x 以降であり、ポッドで [ポッドの編集] ウィザードを実行するときに 2 要素認証設定で RSA SecurID オプションが使用可能な場合、すべてのポッドが RSA SecurID タイプを使用するように構成するオプションがあります。それ以外の場合は、RADIUS タイプを使用できます。

Horizon ポッドと Horizon Cloud on Microsoft Azure デプロイの混在

混合フリートで使用できるオプションは、Horizon Cloud on Microsoft Azure デプロイが RSA SecurID オプションを使用するための条件を満たしているかによって異なります。

- Horizon Cloud on Microsoft Azure デプロイが RSA SecurID タイプを構成する条件を満たしていない場合は、フリート内のすべてのポッドにまたがるすべての外部 Unified Access Gateway インスタンスで RADIUS サービスを構成できます。
- Horizon Cloud on Microsoft Azure デプロイが RSA SecurID タイプを構成する条件を満たしている場合は、フリート内のすべてのポッドにまたがるすべての外部 Unified Access Gateway インスタンスで RSA SecurID または RADIUS を構成できます。

Horizon ポッドについては、Unified Access Gateway ドキュメント、VMware Horizon ドキュメント、および VMware Horizon 7 ドキュメントを参照してください。

Microsoft Azure の Horizon Cloud ポッドについては、デプロイ済みの Horizon Cloud ポッドへのゲートウェイ構成の追加および Horizon Cloud ポッドのゲートウェイでの 2 要素認証の有効化を参照してください。

2 オプションで、各ポッドで内部 Unified Access Gateway インスタンスを構成します。ユーザー トラフィックを内部および外部の DNS サーバそれぞれにルーティングするには、次のいずれかの操作を実行します。

- ポッドの内部および外部の Unified Access Gateway インスタンスに個別の FQDN を構成します。
- ポッドの内部および外部の Unified Access Gateway インスタンスに同一の FQDN を構成します。次に、ポッドのロード バランサの FQDN にスプリット DNS ゾーンを構成します。

3 (Horizon ポッドのみ) Universal Broker に必要なトンネル サーバとプロトコルのリダイレクトをサポートするために、各 Unified Access Gateway インスタンスで必要な JSON Web Token 設定を構成します。Horizon ポッド - Universal Broker で使用する Unified Access Gateway を構成するを参照してください。

4 Universal Broker 構成ウィザードの [認証] ページで、次の設定を指定します。

a [2 要素認証] トグルを有効にします。

b [タイプ] で、ポッド全体にわたるすべての外部 Unified Access Gateway インスタンスで構成した認証サービスを選択します。

c [2 要素認証をスキップ] トグルをオフの位置に設定します。

Universal Broker の設定を参照してください。

外部ネットワークでのみユーザーの 2 要素認証を有効にする場合

1 前のユースケース「外部ネットワークと内部ネットワークの両方でユーザーの 2 要素認証を有効にする場合」の記載どおりに手順 1 から 3 までを実行します。

2 [ブローカ] ページの [ネットワーク範囲] タブで、内部ネットワークを表すパブリック IP アドレス範囲を定義します。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。

3 Universal Broker 構成ウィザードの [認証] ページで、次の設定を指定します。

a [2 要素認証] トグルを有効にします。

b [タイプ] で、ポッド全体にわたるすべての外部 Unified Access Gateway インスタンスで構成した認証サービスを選択します。

c [2 要素認証をスキップ] トグルを有効にします。

Universal Broker の設定を参照してください。

Universal Broker の内部ネットワーク範囲の定義

このトピックでは、Edge ファイアウォールまたはルーターで出力方向 NAT アドレスを指定して内部ネットワークの範囲を定義する方法について説明します。この方法で内部ネットワークを定義することにより、Universal Broker サービスは、内部ユーザーの 2 要素認証をバイパスするなどのネットワーク固有のポリシーを適用できます。

Universal Broker の内部ネットワークを定義するには、[ブローカ] ページの [ネットワーク範囲] タブを使用して、内部エンド ユーザー トラフィックに属している出力方向 NAT のすべての範囲を指定します。

Universal Broker サービスは、Edge ルーターまたはファイアウォール上の出力方向 NAT アドレスの指定された範囲を内部ネットワークからの発信元として認識します。これらの範囲内のオリジンから接続するユーザーは、内部ユーザーとみなされます。これらの範囲外のオリジンから接続するユーザーは、外部ユーザーとみなされます。

重要： ネットワーク構成が変更され、指定したアドレス範囲のいずれかが使用されなくなった場合は、[ネットワーク範囲] リストから使用されていない範囲を手動で削除する必要があります。Universal Broker サービスでは、アドレス範囲が使用中であるかどうかが検出されず、リストから範囲が自動的に削除されることはありません。

前提条件

内部エンド ユーザー トラフィックに対応する Edge ルーターまたはファイアウォールの出力方向ネットワーク アドレス変換 (NAT) アドレスを特定します。

手順

1 [設定] - [ブローカ] の順に選択します。

2 [ブローカ] ページで、[ネットワーク範囲] タブをクリックします。

内部エンドユーザー トラフィックに対応するアドレス範囲のリストが表示されます。

注： [ネットワーク範囲] タブがパブリック IP アドレス範囲を参照している場合でも、これらのエントリは技術的にはパブリック IP アドレスではありません。Edge ルーターまたはファイアウォールの出力方向 NAT アドレスです。

3 出力方向 NAT アドレス範囲をリストに追加するには、[追加] をクリックします。範囲を CIDR 形式で入力します。/1 から /32 までの範囲が使用可能です。次に、[保存] をクリックします。

4 内部ネットワーク トラフィックの全範囲を定義するまで、出力方向 NAT アドレス範囲をリストに追加し続けます。

次のステップ

[ネットワーク範囲] タブのコントロールを使用して、リスト内の範囲を [編集] または [削除] することができます。

注： リストから範囲を削除する前に、次の点を考慮してください。

- 出力方向 NAT アドレス範囲を削除すると、Universal Broker は、その範囲が外部ネットワークの一部であると見なします。
- リストからすべての範囲を削除すると、Universal Broker はすべてのユーザーを外部ユーザーとして扱います。ポッドの内部 Unified Access Gateway インスタンスが構成済みであっても、内部ユーザーに対してポリシーを適用すること（2 要素認証をバイパスするなど）はできなくなります。

Universal Broker セッションに対するグローバル クライアント制限の構成

この記事では、特定の Horizon Client バージョンのみが、Universal Broker によって仲介される仮想デスクトップ、公開デスクトップ、公開アプリケーションを起動できるように指定するクライアント制限を構成する方法について説明します。また、今後制限する予定のクライアント バージョンのユーザーに警告メッセージを表示することもできます。

クライアント制限機能は、Horizon Client バージョン 4.5.0 以降でサポートされます。ただし、Horizon Client for Chrome の場合はバージョン 4.8.0 以降である必要があります。この機能を構成すると、クライアント タイプの Horizon Client の特定のバージョンまたは以前のバージョンはリモート デスクトップや公開アプリケーションに接続できなくなります。特定のクライアント バージョンに警告メッセージを表示する機能は、Horizon Client 5.5 および Horizon Client 2006 以降で使用できます。

手順

1 [設定] - [ブローカ] の順に選択します。

2 [ブローカ] ページで、[クライアントの制限] タブをクリックします。

このタブには、ユーザーが Universal Broker サービスを介してデスクトップおよびアプリケーションに接続しようとするときに現在有効なすべてのクライアント制限設定が表示されます。

3 クライアント制限設定を変更するには、[追加] または [編集] をクリックします。次に、以下の表の説明どおりに設定します。

編集ウィンドウでは、クライアント制限を有効化および構成するための制御機能が提供されています。

4 トグルを使用して、特定のプラットフォーム上の Horizon Client に対する制限をオンまたはオフにします。制限がオンになっているクライアント プラットフォームの場合は、以下の表の説明どおりに設定します。

注： 設定するときは次の指針を使用してください。

- クライアント バージョンを指定する場合、バージョンを内部バージョン番号に対応する *x.x.x* の形式で入力する必要があります。Horizon Client 2006 以降の内部バージョン番号を見つけるには、その Horizon Client のアプリケーション情報を表示するクライアント メニューからコマンドを選択します。
- [クライアント バージョンから接続しているユーザーに警告する] に指定するクライアント バージョンは、[クライアント バージョンからの接続をブロック] に指定するものと異なっている必要があります。特定のクライアント バージョンを構成して、警告メッセージを表示するか、セッションへの接続をブロックすることができます。両方を実行するように同じクライアント バージョンを構成することはできません。

表 5-1. Horizon Client に対するグローバル クライアント制限の設定

クライアント プラットフォーム	説明
[Windows]	[クライアント バージョンからの接続をブロック] 設定には、次のいずれかのオプションを選択します。 ■ [次のバージョンより前]: クライアント バージョンを指定します。このバージョンより前のクライアントはすべてブロックされます。 ■ [次のバージョンと等しい] : 接続時にユーザーをブロックするクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。 [クライアント バージョンから接続しているユーザーに警告する] 設定に、接続時にユーザーに警告を表示するクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。
[Linux]	[クライアント バージョンからの接続をブロック] 設定には、次のいずれかのオプションを選択します。 ■ [次のバージョンより前]: クライアント バージョンを指定します。このバージョンより前のクライアントはすべてブロックされます。 ■ [次のバージョンと等しい] : 接続時にユーザーをブロックするクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。 [クライアント バージョンから接続しているユーザーに警告する] 設定に、接続時にユーザーに警告を表示するクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。

表 5-1. Horizon Client に対するグローバル クライアント制限の設定 （続き）

クライアント プラットフォーム	説明
[Mac]	[クライアント バージョンからの接続をブロック] 設定には、次のいずれかのオプションを選択します。 ■ [次のバージョンより前]: クライアント バージョンを指定します。このバージョンより前のクライアントはすべてブロックされます。 ■ [次のバージョンと等しい] : 接続時にユーザーをブロックするクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。 [クライアント バージョンから接続しているユーザーに警告する] 設定に、接続時にユーザーに警告を表示するクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。
[iOS]	[クライアント バージョンからの接続をブロック] 設定には、次のいずれかのオプションを選択します。 ■ [次のバージョンより前]: クライアント バージョンを指定します。このバージョンより前のクライアントはすべてブロックされます。 ■ [次のバージョンと等しい] : 接続時にユーザーをブロックするクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。 [クライアント バージョンから接続しているユーザーに警告する] 設定に、接続時にユーザーに警告を表示するクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。
[Android]	[クライアント バージョンからの接続をブロック] 設定には、次のいずれかのオプションを選択します。 ■ [次のバージョンより前]: クライアント バージョンを指定します。このバージョンより前のクライアントはすべてブロックされます。 ■ [次のバージョンと等しい] : 接続時にユーザーをブロックするクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。 [クライアント バージョンから接続しているユーザーに警告する] 設定に、接続時にユーザーに警告を表示するクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。
[UWP]	[クライアント バージョンからの接続をブロック] 設定には、次のいずれかのオプションを選択します。 ■ [次のバージョンより前]: クライアント バージョンを指定します。このバージョンより前のクライアントはすべてブロックされます。 ■ [次のバージョンと等しい] : 接続時にユーザーをブロックするクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。
[Chrome]	[クライアント バージョンからの接続をブロック] 設定には、次のいずれかのオプションを選択します。 ■ [次のバージョンより前]: クライアント バージョンを指定します。このバージョンより前のクライアントはすべてブロックされます。 ■ [次のバージョンと等しい] : 接続時にユーザーをブロックするクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。 [クライアント バージョンから接続しているユーザーに警告する] 設定に、接続時にユーザーに警告を表示するクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。

表 5-1. Horizon Client に対するグローバル クライアント制限の設定 （続き）

クライアント プラットフォーム	説明
[HTML Access]	[クライアント バージョンからの接続をブロック] 設定には、次のいずれかのオプションを選択します。 ■ [次のバージョンより前]: クライアント バージョンを指定します。このバージョンより前のクライアントはすべてブロックされます。 ■ [次のバージョンと等しい] : 接続時にユーザーをブロックするクライアント バージョンを入力します。複数のバージョンを指定する場合は、カンマで区切ります。
[追加のクライアントをブロック]	このオプションを選択すると、制限されていない Horizon Client プラットフォーム以外のすべてのクライアント タイプでデスクトップまたは公開アプリケーションの起動がブロックされます。
[ブロックされたメッセージ]	ブロックされた Horizon Client バージョンで接続を試みたユーザーに表示するメッセージを入力します。メッセージは 1,024 文字以下にする必要があります。
[警告メッセージ]	指定された Horizon Client バージョンを使用して接続したユーザーに表示する警告メッセージを入力します。メッセージは 1,024 文字以下にする必要があります。 たとえば、この警告メッセージを使用して、指定した Horizon Client バージョンが今後制限されることをユーザーに通知し、新しいクライアント バージョンへのアップグレードを推奨できます。

5 [保存] をクリックして、変更を保存します。

Universal Broker の設定

この記事では、接続 FQDN または URL、2 要素認証、セッション タイムアウト、Horizon 機能ポリシーなど、Universal Broker 設定を構成するための詳細な手順を説明します。

エンド ユーザーの割り当てからのリソースの仲介に Universal Broker を使用するには、最初に特定の設定を構成する必要があります。

Universal Broker の初回セットアップに、Horizon Universal Console を使用した Universal Broker の有効化の開始で説明されているように構成ウィザードが自動的に開きます。

サービスの使用中に設定を修正する必要がある場合は、コンソールの [ブローカ] ページまたは [はじめに] ページから構成ウィザードを再度開くことができます。

この構成ウィザードの 2 要素認証設定に関するいくつかの重要なポイント

- 設計上、Universal Broker は、2 要素認証設定を使用して構成されている場合、認証要求を形成し、それを外部の Unified Access Gateway インスタンスに送信します。次にそのインスタンスは、設定で構成されている実際の認証サーバと通信します。Unified Access Gateway は、次に認証サービスの応答を Universal Broker にリレーします。

- デフォルトの設計では、テナントのポッド フリート内の各ポッドに使用される同じ Universal Broker 2 要素認証設定がテナント全体に適用されます。Universal Broker に 2 要素認証を使用するには、まず、ポッド フリート内で参加しているすべてのポッドの各外部 Unified Access Gateway インスタンスで適切な認証サービスを構成する必要があります。外部 Unified Access Gateway インスタンスの構成は、参加しているポッド内およびポッド間で同一でなければなりません。
- たとえば、ポッド フリートが Horizon ポッドと Horizon Cloud ポッドの両方で構成されている場合、RADIUS 認証を使用するには、これらすべての Horizon ポッドと Horizon Cloud ポッドにわたって、各外部 Unified Access Gateway インスタンスに RADIUS サービスを構成します。

前提条件

重要： エンド ユーザーがインターネットから接続する場合、または 2 要素認証を使用する場合は、ポッドにある外部 Unified Access Gateway インスタンスを削除しないでください。外部エンド ユーザーの場合、クライアントが Universal Broker で認証された後、エンドユーザー クライアントから仮想デスクトップまたはリモート アプリケーションを正常に起動するには、外部 Unified Access Gateway が必要です。2 要素認証の場合、Universal Broker は、2 要素認証設定を外部 Unified Access Gateway と一致させ、そのために外部 Unified Access Gateway 構成が必要です。

ポッドのタイプに応じて必要なシステム コンポーネントを準備します。これらの前提条件の確認は、テナントが初めて Universal Broker をセットアップするためのウィザードを完了するときに特に重要です。

Horizon ポッド（Horizon Connection Server テクノロジー ベース）の場合：

- 必要なポートを構成します（Horizon ポッド - Universal Broker の DNS、ポートおよびプロトコルの要件を参照）。
- Horizon ポッド - Connection Server への Universal Broker プラグインのインストール。
- Horizon ポッド - Universal Broker で使用する Unified Access Gateway を構成する。Universal Broker で Horizon ポッドに 2 要素認証を使用する場合は、参加しているすべてのポッド内の各 Unified Access Gateway インスタンスで適切な 2 要素認証サービスを構成します。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。
- 2 要素認証を外部ユーザーに対してのみ有効にして、内部ユーザーに対してはバイパスさせる場合は、Universal Broker の内部ネットワーク範囲の定義を行います。
- Horizon Universal Console を使用した Universal Broker の有効化の開始の説明に従って、Horizon ポッドのテナント全体のコネクション ブローカとして Universal Broker を選択します。

Horizon Cloud ポッドの場合（Horizon Cloud ポッドマネージャ テクノロジー ベース）：

- 地域の Universal Broker インスタンスに必要な DNS 名が解決可能であり、アクセス可能であることを確認します。Microsoft Azure での Horizon Cloud ポッドの DNS の要件の「ポッドのデプロイと操作に関する DNS の要件」の表を参照してください。
- 必要なポートとプロトコルを構成します（Horizon Cloud ポッド - ポートおよびプロトコルの要件の「Universal Broker で必要なポートとプロトコル」セクションを参照）。

- Universal Broker で Horizon Cloud ポッドに 2 要素認証を使用する場合は、参加しているすべてのポッド内の各外部 Unified Access Gateway インスタンスで同じタイプの認証サービスを構成します。Horizon Cloud ポッドのゲートウェイでの 2 要素認証の有効化および 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。
- 2 要素認証を外部ユーザーに対してのみ有効にして、内部ユーザーに対してはバイパスさせる場合は、Universal Broker の内部ネットワーク範囲の定義を行います。
- Horizon Cloud ポッドのテナント全体のコネクション ブローカとして Universal Broker を選択します (Horizon Universal Console を使用した Universal Broker の有効化の開始を参照)。

重要： ウィザードの最後の手順を送信する前に、すべての Horizon Cloud ポッドがオンラインで、健全な状態で準備が整っている必要があります。設定の適用中、セットアップ プロセスを完了するために、Universal Broker サービスはポッドとの通信を行い、ポッドでいくつかの構成手順を実行する必要があります。いずれかのポッドがオフラインまたは使用できない場合、Universal Broker のセットアップは失敗します。

手順

1 Universal Broker をセットアップするための構成ウィザードを開きます。

または、[設定] - [ブローカ] の順にクリックし、鉛筆アイコンをクリックして構成を編集して、ウィザードを直接開くことができます。

Horizon Universal Console を使用した Universal Broker の有効化の開始の手順の直後にこのウィザードを完了する場合

この場合、ウィザードを終了する前にキャンセルしない限り、コンソールには通常ウィザードがすでに表示されています。ウィザードを終了する前にキャンセルした場合は、[設定] - [ブローカ] の順に移動して、[セットアップ] をクリックし、ウィザードを直接開きます。

保存した構成を修正する場合

[設定] - [ブローカ] の順に移動し、その構成の横にある鉛筆アイコンをクリックして、ウィザードを直接開きます。

Universal Broker の構成ウィザードが表示されます。現在のリリースでは、ウィザード セクションは FQDN、認証、およびクライアント セッションに適用可能な一部のデフォルト設定に対応しています。

2 ウィザードの [FQDN] ページで、Universal Broker サービスの完全修飾ドメイン名 (FQDN) の設定を構成します。これらの設定は、エンド ユーザーが Universal Broker によって仲介されるリソースにアクセスするために使用する専用接続アドレスまたは URL を定義します。

注： サブドメインまたは FQDN 設定を変更すると、すべての DNS サーバで変更が有効になるまでに時間がかかる場合があります。

a [タイプ] には、[VMware が提供] または [お客様が提供] の完全修飾ドメイン名 (FQDN) を選択します。

b 選択した FQDN タイプの追加設定を指定します。

[VMware が提供]

設定	説明
[サブドメイン]	会社または組織を表すネットワーク構成内の有効なサブドメインの一意の DNS 名を入力します。このサブドメインは、仲介の FQDN を形成するために、VMware が提供するドメインの先頭に付けられます。 **注：** 一部の文字列は、システムによって禁止または予約されています。そのような文字列のカテゴリには、`book` のような一般的な語句、`gmail` のような有名企業が所有している既知の用語、プロトコル、コーディング、オープンソースの用語（たとえば `php` や `sql`）などがあります。またシステムは、`mail0`、`mail1`、`mail2` など、これらの文字列のパターンのカテゴリを禁止します。 ただし、このフィールドに禁止されている名前を入力すると、システムはその時点での入力を検証しません。ウィザードの最終サマリ ステップに到達した時点で初めて、システムはここで入力した名前を検証し、入力が禁止された名前のいずれかに一致した場合はエラーが表示されます。その場合は、より一意の名前をここで入力します。
[ブローカ URL]	この読み取り専用フィールドには、構成された FQDN が表示されます。FQDN は `https://<your sub-domain>vmwarehorizon.com` の形式を使用します。 この FQDN をエンド ユーザーに提供し、Horizon Client を使用して Universal Broker サービスに接続できるようにします。 Universal Broker は、この FQDN の DNS および SSL 検証を管理します。

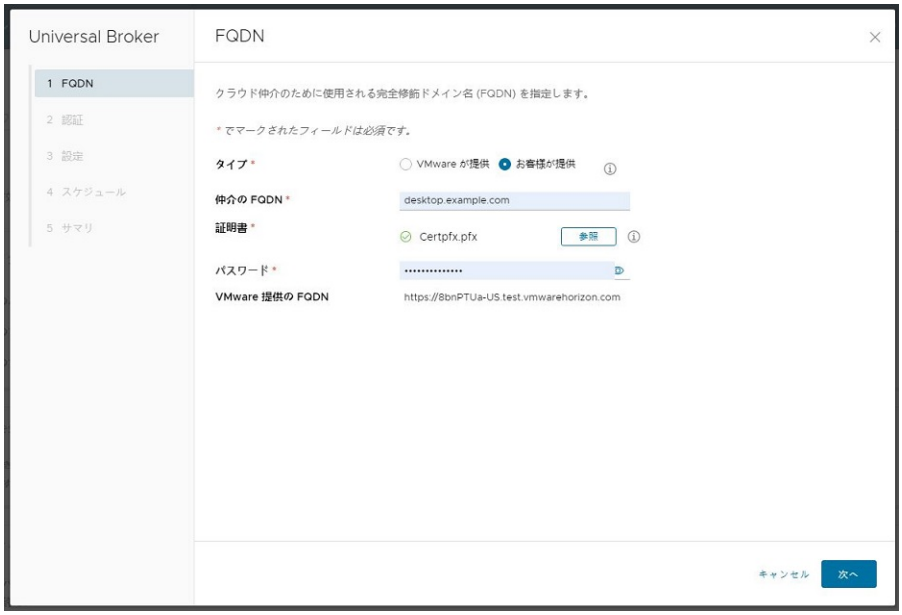
次のスクリーンショットは、VMware 提供の FQDN の設定が入力された構成ウィザードの例を示しています。

[お客様が提供]

設定	説明
[仲介の FQDN]	エンド ユーザーが Universal Broker サービスへのアクセスに使用するカスタムの FQDN を入力します。カスタム FQDN は、サービスへの接続を完了する自動生成された VMware 提供の FQDN のエイリアスとして機能します。 カスタム FQDN 内で指定されたドメイン名の所有者であること、またそのドメインを検証できる証明書を指定することが必要です。 **注：** カスタム FQDN は、接続 URL とも呼ばれ、会社または組織を表します。このカスタム FQDN を使用するための適切な権限があることを確認します。 **注：** カスタム FQDN は、ポッド内のすべての Unified Access Gateway インスタンスの FQDN とは異なる一意の値でなければなりません。 **重要：** カスタム FQDN を Universal Broker サービスの内部接続アドレスを表す VMware 提供の FQDN にマッピングする CNAME レコードを DNS サーバに作成する必要があります。たとえば、レコードは `vdi.examplecompany.com` を *<自動生成文字列>*`.vmwarehorizon.com` にマッピングすることがあります。
[証明書]	[参照] をクリックして、仲介の FQDN を検証する証明書（パスワード保護された PFX 形式）をアップロードします。証明書は以下の条件をすべて満たす必要があります。 ■ 90 日以上有効である ■ 信頼されている認証局 (CA) によって署名されている ■ 証明書の共通名 (CN) またはそのサブジェクト代替名 (SAN) のいずれかが FQDN と一致している ■ 証明書の内容が標準の X.509 形式に準拠している PFX ファイルに、ドメイン証明書、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。 Universal Broker サービスは、この証明書を使用して、クライアントとの信頼された接続セッションを確立します。

設定	説明
	注： 証明書の CN または SAN フィールドにワイルドカード FQDN を含めることができます。ワイルドカード文字が参照識別子の左端のサブドメインの唯一の文字である場合、左端のサブドメインに一致する FQDN のみが証明書によって検証されます。たとえば、証明書にワイルドカード FQDN `*.mycompany.com` が含まれている場合、一致ルールにより、`vdi.mycompany.com` が有効な仲介 FQDN として許可されます。ただし、`test.vdi.mycompany.com` は参照識別子と一致しないため、許可されません。
[パスワード]	PFX 証明書ファイルのパスワードを入力します。
[VMware 提供の FQDN]	この読み取り専用フィールドには、仲介サービス用に自動的に作成される VMware 提供の FQDN が表示されます。FQDN は `https://<auto-generated string>.vmwarehorizon.com` の形式を使用します。 VMware 提供の FQDN はエンド ユーザーには表示されず、Universal Broker サービスの内部接続アドレスを表します。カスタム FQDN は、VMware 提供の FQDN のエイリアスとして機能します。 **重要：** カスタム FQDN を VMware 提供の FQDN にマッピングする CNAME レコードを DNS サーバに作成して、エイリアスの関連付けを設定する必要があります。たとえば、レコードは `vdi.examplecompany.com` を `<自動生成文字列>.vmwarehorizon.com` にマッピングすることがあります。

次のスクリーンショットは、カスタム FQDN の設定が入力された構成ウィザードの例を示しています。



c FQDN 設定の構成が完了したら、[次へ] をクリックしてウィザードの次のページに進みます。

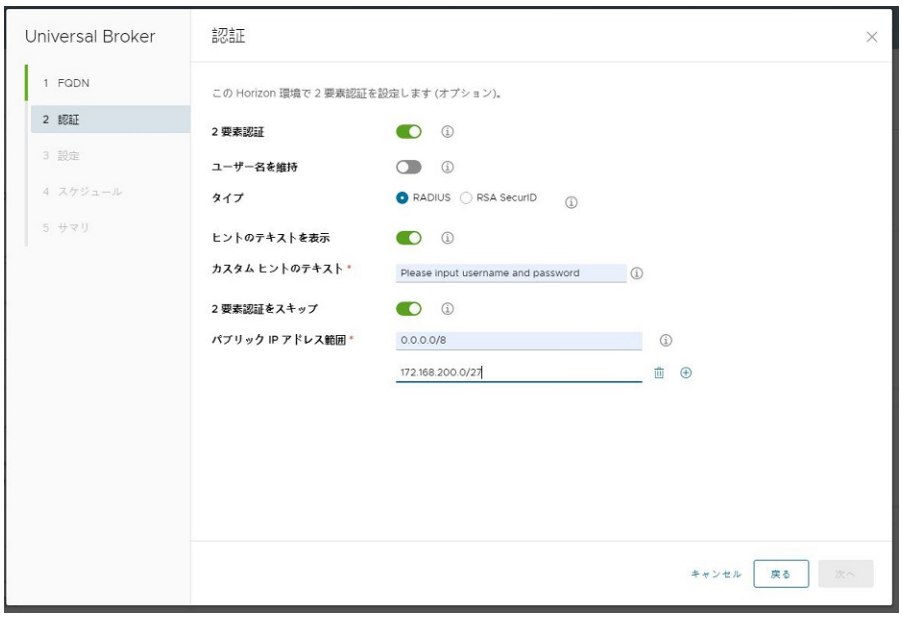
3 （オプション）ウィザードの [認証] ページで、2 要素認証を構成します。

デフォルトでは、Universal Broker は Active Directory のユーザー名とパスワードのみを使用してユーザーを認証します。追加の認証方法を指定することで、2 要素認証を実装できます。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。

設定	説明
[2 要素認証]	2 要素認証を使用するには、このトグルを有効にします。 トグルを有効にすると、2 要素認証を構成するための追加オプションが表示されます。
[ユーザー名を維持]	Universal Broker への認証中にユーザーの Active Directory ユーザー名を維持する場合はこのトグルを有効にします。有効になっている場合： ■ ユーザーは、Universal Broker に対する Active Directory 認証の場合と同じユーザー名認証情報を追加の認証方法でも利用できる必要があります。 ■ ユーザーは、クライアント 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。 このトグルがオフになると、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。
[タイプ]	Active Directory のユーザー名とパスワードに加えて、Universal Broker がエンド ユーザーで使用する認証方法を指定します。ユーザー インターフェイスには、[RADIUS] と [RSA SecurID] の 2 つの選択肢が表示されます。 この設定は、テナント全体に適用されます。エンド ユーザー クライアントの動作は、以下のように、テナントのポッド フリートの構成と、ポッドのゲートウェイで構成されている 2 要素認証タイプによって異なります。 **Horizon ポッドのみ** ここで選択するタイプは、クライアントで使用されるタイプです。 **Horizon Cloud ポッドのみ** ■ ポッドの外部ゲートウェイで構成されているタイプと一致するタイプを選択します。 **Horizon ポッドと Horizon Cloud on Microsoft Azure デプロイの混在** 混合フリートでは、ここで [RADIUS] を選択すると、両方のポッド タイプの Unified Access Gateway インスタンスを介してユーザーの RADIUS 認証要求が試行されます。 混合フリートでは、ここで [RSA SecurID] を選択すると、クライアントの動作は、Horizon Cloud on Microsoft Azure デプロイが外部ゲートウェイで RSA SecurID を使用して構成されているかどうかによって異なります。 ■ Horizon Cloud on Microsoft Azure デプロイのゲートウェイで RSA SecurID タイプが構成されていない場合、ここで [RSA SecurID] を選択すると、Horizon ポッドの Unified Access Gateway インスタンスのみを介してユーザーの RSA 認証要求が試行されます。Active Directory のユーザー名とパスワードの認証要求は、Horizon ポッドまたは Horizon Cloud ポッドの Unified Access Gateway インスタンスを通じて試行されます。 ■ Horizon Cloud on Microsoft Azure デプロイで RSA SecurID タイプが構成されている場合、ユーザーの RSA 認証要求は両方のポッド タイプの Unified Access Gateway インスタンスを介して試行されます。
[ヒントのテキストを表示]	RADIUS タイプに適用されます。このトグルを有効にすると、クライアントのログイン画面に表示されるテキスト文字列を構成して、ユーザーに追加の認証方法に対する認証情報の入力を求めることができます。

設定	説明
[カスタム ヒントのテキスト]	このフィールドは、ヒント テキストの表示を選択した場合に使用できます。RADIUS タイプに適用されます。 クライアントのログイン画面に表示す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 DisplayHint user name and password` としてエンド ユーザーに表示されます。ここで、*DisplayHint* はこのテキスト ボックスで指定するテキスト文字列です。 **注：** Universal Broker のヒント テキストに、**& < > ' "** の文字を含めることはできません。 これらの許可されていない文字のいずれかをヒント テキストに含めると、ユーザーは Universal Broker FQDN への接続に失敗します。 このヒントを参考にして、ユーザーは正しい認証情報を入力することができます。たとえば、**`Company user name and domain password below for`** のようなフレーズを入力すると、`Enter your Company user name and domain password below for user name and password` というプロンプトがエンド ユーザーに表示されます。
[2 要素認証をスキップ]	Universal Broker サービスに接続している内部ネットワーク ユーザーの 2 要素認証をバイパスするには、このトグルを有効にします。Universal Broker の内部ネットワーク範囲の定義の説明に従って、内部ネットワークに属しているパブリック IP アドレス範囲を指定していることを確認します。 ■ このトグルが有効になると、内部ユーザーは、Universal Broker サービスに対して認証するために、Active Directory の認証情報のみを入力する必要があります。外部ユーザーは、Active Directory の認証情報と、追加の認証サービスの認証情報の両方を入力する必要があります。 ■ このトグルがオフになると、内部および外部の両方のユーザーは、Active Directory の認証情報と、追加の認証サービスの認証情報を入力する必要があります。
[パブリック IP アドレス範囲]	このフィールドは、[2 要素認証をスキップ] が有効になっている場合に表示されます。 [ブローカ] ページの [ネットワーク範囲] タブで 1 つ以上のパブリック IP アドレス範囲がすでに指定されている場合、このフィールドは読み取り専用で、これらの IP アドレス範囲が一覧表示されます。 [ブローカ] ページの [ネットワーク範囲] タブにパブリック IP アドレス範囲がまだ指定されていない場合は、このフィールドを使用して、内部ネットワークを表すパブリック IP アドレス範囲を指定し、それらの範囲からのトラフィックの 2 要素認証プロンプトをスキップすることができます。Universal Broker は、これらのいずれかの範囲内の IP アドレスから接続しているユーザーを、内部ユーザーと見なします。 これらの範囲を指定する目的の詳細については、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。

次のスクリーンショットは、RADIUS タイプでの 2 要素認証設定が入力された構成ウィザードの例を示しています。



選択が完了したら、[次へ] をクリックしてウィザードの次のページに進みます。

4 構成ウィザードの [設定] ページで、Horizon Client の [期間] 設定を構成します。

これらのタイムアウト設定は、Horizon Client と Universal Broker によって割り当てられた割り当て済みのデスクトップ間の接続セッションに適用されます。これらの設定は、割り当てられたデスクトップのゲスト OS へのユーザーのログイン セッションには適用されません。Universal Broker がこれらの設定で指定されたタイムアウト状態を検出すると、ユーザーの Horizon Client 接続セッションを閉じます。

設定	説明
[Client ハートビートの間隔]	Horizon Client ハートビートの間隔（分）と、ユーザーの Universal Broker への接続状態を制御します。これらのハートビートは、Horizon Client 接続セッション中に経過したアイドル時間を Universal Broker にレポートします。 Horizon Client を実行しているエンドポイント デバイスとの相互作用が発生しない場合、アイドル時間が測定されます。このアイドル時間は、ユーザーに割り当てられたデスクトップの基盤となるゲスト OS へのログイン セッションがアクティブでない状態であることの影響を受けません。 大規模なデスクトップ デプロイでは、[クライアントのハートビート間隔] を増やすとネットワーク トラフィックが減少し、パフォーマンスが向上する場合があります。
[Client アイドル ユーザー]	Horizon Client と Universal Broker 間の接続セッションで許可される最大アイドル時間（分）。 最大時間に達すると、ユーザーの認証期間が期限切れになり、Universal Broker はすべてのアクティブな Horizon Client セッションを閉じます。接続セッションを再度開くには、ユーザーは Universal Broker ログイン画面で認証情報を再入力する必要があります。 **注：** 割り当てられたデスクトップからユーザーが予期せず切断されないようにするには、[クライアントのアイドル ユーザー] タイムアウトを [クライアントのハートビート間隔] の少なくとも 2 倍の値に設定します。

設定	説明
[Client ブローカ セッション]	ユーザーの認証の有効期限が切れるまでの Horizon Client 接続セッションの最大許容時間（分）。この時間はユーザーが Universal Broker に対して認証されると開始します。セッションのタイムアウトが発生すると、ユーザーは割り当てられたデスクトップで作業を続行できます。ただし、Universal Broker との通信を必要とする設定の変更などのアクションを実行すると、Horizon Client によって Universal Broker の認証情報を再入力するように求められます。 **注：** [Client ブローカ セッション] のタイムアウトは、少なくとも [Client ハートビート間隔] 値と [Client アイドル ユーザー] のタイムアウトの合計値以上にする必要があります。
[クライアント認証情報のキャッシュ タイムアウト]	この設定は、Universal Broker の、Horizon Connection Server 設定（[その他のクライアント。SSO 認証情報の破棄] とラベル付けされた設定）に相当する設定として意図しています。 したがって、この設定に関するここでの説明は、Horizon Connection Server の設定およびコンソールのこの設定のツールチップの説明と一致するように記述されています。 この設定は、アプリケーションのリモート処理をサポートしていないクライアント用です。指定した時間（分）が経過すると、SSO 認証情報は破棄されます。クライアント デバイスでのユーザー アクティビティに関係なく、指定した時間（分）が経過した後にデスクトップに接続するには、ユーザーは再度ログインする必要があります。デフォルトは 15 分です。

5 構成ウィザードの [設定] ページで、[ポリシーの詳細] を構成します。

[ポリシーの詳細] は、エンド ユーザーが特定の Horizon 機能（デスクトップとクライアントで使用可能である場合）にアクセスできるかどうかを制御します。

設定	説明
[マルチメディア リダイレクト (MMR)]	この設定を有効にすると、エンド ユーザーがマルチメディア リダイレクト機能（デスクトップとクライアントで使用可能な場合）にアクセスできるようになります。
[USB アクセス]	この設定を有効にすると、エンド ユーザーが USB リダイレクト機能（デスクトップとクライアントで使用可能な場合）にアクセスできるようになります。
[タブを閉じるときに HTML Access 認証情報をクリーンアップする]	この設定を有効にすると、リモート デスクトップに接続するタブや、Horizon HTML Access クライアントのデスクトップの選択ページに接続するタブをユーザーが閉じるときに、キャッシュからユーザーの認証情報を削除します。 この設定が有効である場合、次の HTML Access クライアントのシナリオにおいても認証情報はキャッシュから削除されます。 ■ ユーザーが、デスクトップの選択ページやリモート セッション ページを更新する。 ■ サーバから自己署名証明書が提示されており、ユーザーがリモート デスクトップを起動し、セキュリティの警告が表示されるときにユーザーがその証明書を受け入れる。 ■ リモート セッションが含まれるタブで URI コマンドをユーザーが実行する。 この設定がオフに切り替わると、認証情報はキャッシュに残ります。
[クライアントがパワーオフ状態の仮想マシンを待機することを許可する]	この設定を有効にすると、Horizon Client は現在使用できないリモート デスクトップへの接続要求を再試行することができます。 たとえば、クライアント ユーザーは、現在パワーオフ状態のデスクトップを要求する場合があります。この設定を有効にすると、Horizon Client はその接続要求を再送信して、デスクトップがパワーオンされ、使用可能になったときに接続セッションを確立できます。

[ポリシーの詳細] の構成が完了したら、[次へ] をクリックしてウィザードの次の手順に進みます。

6 [サマリ] ページで設定を確認し、[終了] をクリックして構成を保存して適用します。

システムとネットワークの状態にもよりますが、DNS レコードはすべてのグローバル リージョンの DNS サーバに伝達されるため、構成の設定が Universal Broker サービスで完全に有効になるまで、通常は少なくとも数分から最大で 30 分かかります。この期間中は Universal Broker サービスを利用できません。セットアップが正常に完了すると、[はじめに] ページの [ブローカ] セクションに [完了] ステータスが表示され、[設定] - [ブローカ] ページに緑のドットで [有効] ステータスが表示されます。

重要： Universal Broker のセットアップが失敗した場合、[設定] - [ブローカ] 画面には赤のアラート アイコンで [エラー] ステータスが表示されます。構成エラーを修正し、Universal Broker サービスをセットアップするには、VMware ナレッジベースの記事 KB2006985 の説明に従って、VMware サポートにお問い合わせください。

次のステップ

- Horizon ポッドに対して Universal Broker を構成している場合は、ポッドを管理対象状態に変更する手順に進みます。Horizon Universal Console を使用して、クラウド接続された Horizon ポッドを管理対象状態に変更するを参照してください。
- Microsoft Azure の Horizon Cloud ポッド用に Universal Broker を構成している場合は、これ以上の構成は必要ありません。コンソールを使用してマルチポッド イメージを作成してから、それらのイメージに基づいてエンド ユーザー割り当てを作成できます。

Universal Broker 環境でのサイトの操作

サイトは、Universal Broker サービスがリモート リソースをエンド ユーザーに仲介する最善の方法を決定するのに役立ちます。[サイト] とは、同一の物理的場所（通常は単一データセンター内）にあるクラウド接続されたポッドの集合のことです。

サイトとホーム サイトの構成

デフォルトでは、Horizon ポッド（Horizon Connection Server テクノロジー ベース）は監視対象状態になります。割り当ての作成をサポートするために、ポッドを監視対象状態から管理対象状態に変更すると、ポッドを新規または既存のサイトに関連付けるように求められます。

Microsoft Azure の Horizon Cloud ポッドの仲介方法として Universal Broker を選択すると、Default-Site という名前のデフォルト サイトが作成されます。参加している Horizon Cloud ポッドは、自動的に Default-Site に追加されます。後で新しいサイトを構成し、Default-Site から構成済みのサイトにポッドを移動することができます。

また、ユーザーまたはユーザーのグループを、[ホーム サイト] と呼ばれる特定のサイトに関連付けることもできます。

サイトは、ディザスタ リカバリ ソリューションの有用な部分として機能します。たとえば、さまざまなデータセンター内のポッドをさまざまなサイトに追加して、それらのサイト全体にわたる割り当ての使用資格をユーザーやグループに割り当てることができます。あるサイトのデータセンターが使用不可になった場合、Universal Broker は使用可能なサイトからデスクトップを識別して、ユーザーの要求を満たすことができます。

Horizon Universal Console を使用してサイトとホーム サイトを構成します。Universal Broker のサイトの構成および Universal Broker のホーム サイトの構成を参照してください。

サイトを使用したデスクトップ検索の動作の定義

ユーザーが割り当てにアクセスすると、Universal Broker はその割り当てに参加しているプールから利用可能なデスクトップを検索します。デフォルトでは、Universal Broker はユーザーのホーム サイト、ユーザーに物理的に最も近いサイト、および他のサイトの順に優先順位を設定します。

専用デスクトップ プールを含む割り当ての場合、Universal Broker は、ユーザーが初めてデスクトップを要求したときのみデフォルトの検索動作を使用します。Universal Broker は、この最初のセッションでユーザーの要求を専用デスクトップにルーティングした後、後続のセッションでユーザーを同じデスクトップに直接返します。

個々の割り当てのデフォルトの検索および要求のルーティング動作を変更するには、サイト ポリシーとホーム サイトの上書きを構成します。たとえば、Universal Broker は、ユーザーのホーム サイトではなく、ユーザーに物理的に最も近いサイトを優先することができます。Universal Broker は、検索の範囲を特定のサイトのデスクトップに制限することもできます。

割り当てのホーム サイト上書きを指定することもできます。この場合、Universal Broker は、ユーザーのホーム サイトではなく、上書きサイトで使用可能なデスクトップの検索を開始します。

Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成や Microsoft Azure の Horizon Cloud ポッド - 第 1 世代環境での VDI マルチクラウド割り当ての作成と表示で説明するように、割り当てを作成するときに、サイト ポリシーとホーム サイト上書きを設定できます。また、Horizon Cloud テナント環境でのマルチクラウド割り当ての編集で説明するように、割り当てを編集して既存のサイト ポリシーとホーム サイト上書き設定を変更することもできます。

注： ユーザーの物理的な場所を解決するために、Universal Broker は MaxMind で作成された GeoLite2 データを使用します。これは https://www.maxmind.com から入手可能です。

Universal Broker のサイトの構成

[キャパシティ] ページの [サイト] タブを使用して、Universal Broker のサイトを構成できます。ポッドは、Universal Broker によって仲介されるマルチクラウド割り当てに参加する前にサイトに関連付ける必要があります。

Horizon ポッド（Horizon Connection Server テクノロジー ベース）を監視対象状態から管理対象状態に変更すると、ポッドを新規または既存のサイトに関連付けるように求められます。

Microsoft Azure の Horizon Cloud ポッドは、Default-Site と呼ばれるデフォルト サイトに自動的に追加されます。後で新しいサイトを構成し、Default-Site から構成済みのサイトにポッドを移動することができます。

[設定] - [キャパシティ] ページの [サイト] タブには、Universal Broker 環境で構成されたサイトのリストが表示され、各サイトに関連付けられているポッドの数がレポートされます。

[サイト] タブで使用可能なサイトレベルのアクション

[サイト] タブから次のアクションを実行できます。

アクション	説明
[新規]	Universal Broker 環境にサイトを作成するには [新規] をクリックします。[名前] と [説明] に値を入力し、[保存] をクリックします。 たとえば、サンフランシスコにあるデータセンターに対応するサイトの名前には、**San Francisco** と入力します。新規作成されたサイトが [サイト] リストに追加されます。
[編集]	リストからサイトを選択し、[編集] をクリックして、サイトの名前と説明を変更します。
[削除]	[削除] アクションを使用すると、Universal Broker 環境からサイトを永久に削除できます。サイトを削除する前に、特定のポッド、ユーザー、または割り当てとの関連付けのサイトをクリアします。 ■ ポッドのサイトの関連付けを変更して、サイト内の各ポッドを別のサイトに移動します。ポッドのサイトの関連付けの構成を参照してください。 ■ 以下を検証します: ■ サイトがユーザーまたはグループのホーム サイトとして構成されていないこと。Universal Broker のホーム サイトの構成を参照してください。 ■ サイトがマルチクラウド割り当てのホーム サイト上書きとして構成されていないこと。Horizon Cloud テナント環境でのマルチクラウド割り当ての編集を参照してください。 **注:** 削除されたサイトをホーム サイトまたはホーム サイト上書きとして使用するマルチクラウド割り当てがある場合、Universal Broker はこれらの割り当てからリソースに接続要求をルーティングすることはできません。 サイトを永久に削除するには、リストでサイトを選択し、[削除] をクリックします。

ポッドのサイトの関連付けの構成

ポッドのサイトの関連付けを構成するには、次のいずれかを実行します。

- Horizon ポッドを [監視対象] から [管理対象] に変更する場合は、ポッドに関連付ける新規または既存のサイトを指定します。Horizon Universal Console を使用して、クラウド接続された Horizon ポッドを管理対象状態に変更するを参照してください。

- ポッドのプロパティを編集して、Horizon ポッドまたは Microsoft Azure の Horizon Cloud ポッドのサイトの関連付けを変更します。[キャパシティ] ページの [ポッド] タブをクリックし、リスト内のポッドを選択して、[編集] をクリックします。ポッド： 使用可能なポッドレベルのアクションを参照してください。

Universal Broker のホーム サイトの構成

ユーザーまたはユーザーのグループを、ホーム サイトと呼ばれる Universal Broker 環境内の特定のサイトに関連付けることができます。ホーム サイトは、エンド ユーザーの接続要求を満たすために Universal Broker が割り当てからリソースを検索する方法を定義するのに役立ちます。

ホーム サイトのユースケースの 1 つには、ローミング ユーザーおよびグループの接続要求の管理が含まれます。たとえば、ホーム サイトがサンフランシスコにあるユーザーがロンドンを訪れている場合、Universal Broker はユーザーに近いデスクトップに要求をルーティングするのではなく、サンフランシスコのサイトで検索してユーザーのデスクトップ要求を満たすようにします。

[ユーザーとグループ] ページの概要

[ユーザーとグループ] ページには、Universal Broker 環境内でのマルチクラウド割り当ての使用資格が付与されているユーザーとグループが一覧表示されます。このページでは、ホーム サイトをユーザーまたはグループに割り当てることもできます。

[ユーザーとグループ] ページを開くには、[設定] - [ユーザーとグループ] の順に選択します。

[ユーザーとグループ] ページには次の情報が報告されます。

列	詳細
[ユーザー名]	ユーザーまたはグループの名前が表示されます。
[ドメイン]	ユーザーまたはグループが存在する Active Directory ドメインが表示されます。
[タイプ]	ユーザー アカウントのタイプが表示されます。
[ホーム サイト]	ユーザーまたはグループに関連付けられているホーム サイトの名前が表示されます。

[ユーザーとグループ] ページで使用可能なアクション

[ユーザーとグループ] ページから次のアクションを実行できます。

アクション	説明
[新規]	[新規] アクションを使用すると、ホーム サイトを選択したユーザーまたはグループに関連付けるホーム サイト割り当てを作成できます。ホーム サイトの割り当ての構成を参照してください。
[編集]	選択したユーザーまたはグループに関連付けられているホーム サイトを変更するには、[編集] をクリックします。
[削除]	選択したユーザーまたはグループから既存のホーム サイト割り当てを削除するには、[削除] をクリックします。

ホーム サイトの割り当ての構成

ホーム サイトをユーザーまたはグループに関連付けるには、次の手順を実行します。

1 [ユーザーとグループ] ページで、[新規] をクリックします。[新しいホーム サイトの割り当て] ウィザードが表示されます。

2 ウィザードの [ユーザー] ページで、ホーム サイトの割り当てを受け取るユーザーまたはグループを指定します。

a [ドメイン] には、ユーザーまたはグループが存在する Active Directory ドメインを指定します。

注： 選択できるのは、クラウド構成のドメインのみです。

b [ユーザーを検索] では、ユーザー名またはグループ名の最初の数文字を入力し、表示されるリストからユーザーまたはユーザー グループを選択します。選択した項目が [選択されたユーザー/ユーザー グループ] リストに追加されます。

注： リストからユーザーまたはグループを削除するには、ユーザーまたはグループの左側にあるチェックボックスをオンにして、[削除] をクリックします。

3 ホーム サイトの割り当ての詳細を指定します。

a ホーム サイトの割り当てを受け取るユーザーまたはグループの横にあるチェック ボックスをオンにします。

b [ホーム サイトの割り当て] をクリックして、メニューからサイトを選択します。

c [次へ] をクリックします。

4 [サマリ] ページの設定を確認して、[終了] をクリックします。

構成されたユーザーまたはグループが [ユーザーとグループ] リストに表示され、関連付けられたホーム サイトが [ホーム サイト] 列に示されます。

View ポッド - マルチクラウド割り当てのためのクラウド接続されたポッドの有効化

Horizon Universal Console の [キャパシティ] 画面には、クラウド接続された Horizon ポッド（Horizon Connection Server テクノロジー ベース）の現在の状態が表示されます。このリリースでは、Horizon ポッドは監視対象または管理対象のいずれかの状態になります。ポッドが管理対象状態にある場合にのみ、そのポッドのリソースをマルチクラウド割り当て (MCA) で使用できます。

監視対象状態

監視対象状態は、最初に Horizon ポッドを Horizon Cloud 環境に接続した後のポッドのデフォルト状態です。次のリストは監視対象状態のポッドで使用可能な機能について説明しています。

- [ダッシュボード] ページには、監視対象ポッドのコンポーネントに関する全体的な健全性レポートが表示されます。このページには、リソース使用状況、現在のユーザー セッション、およびポッドの接続統計に関する情報も表示されます。第 1 世代のテナント - 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を参照してください。
- [キャパシティ] ページには、ステータス、場所、状態など、ポッドに関する詳細が表示されます。3 章 第 1 世代テナント - 第 1 世代 Horizon Cloud がサポートするすべてのポッド タイプのクラウド接続ポッドの管理を参照してください。
- 管理コンソールでは、ユーザーをサポートするためのヘルプデスク操作を実行できるユーザーベースの検索機能を使用できます。2 章 第 1 世代のテナント - 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 デスク機能の紹介を参照してください。

管理対象状態

監視対象のポッドが特定の要件を満たしている場合は、その Horizon ポッドの状態を管理対象状態に変更できます。Horizon Universal Console を使用して、クラウド接続された Horizon ポッドを管理対象状態に変更するを参照してください。

管理対象ポッドは、監視対象ポッドで利用可能なすべての機能を提供します。また、管理対象ポッドのリソースを使用するマルチクラウド割り当てを作成し、それらのマルチクラウド割り当てを Horizon Universal Console を使用して管理することもできます。詳細については、Horizon Cloud テナント環境でのマルチクラウド割り当ての管理を参照してください。

Horizon Universal Console を使用して、クラウド接続された Horizon ポッドを管理対象状態に変更する

テナントのフリート内にある Horizon ポッドの場合、Universal Broker 設定を保存した後、それらのポッドを監視対象から管理対象に変更できます。ポッドを管理対象状態に変更すると、そのポッドから Universal Broker 環境に割り当てを追加できます。また、Horizon Cloud によって提供される追加のサービスである イメージ管理サービス (IMS) の機能を使用することもできます。

Horizon Universal Console の [キャパシティ] ページから状態変更ワークフローを実行します。[キャパシティ] ページから状態変更ワークフローを実行する前に、まずコンソールの [ブローカ] ページを使用して Universal Broker 設定を保存する必要があります。

前提条件

- Universal Broker のシステム要件で説明するように、Horizon ポッドが Universal Broker の要件を満たしていることを確認します。
- ポッド内のすべての Connection Server インスタンスに Universal Broker プラグインをインストールします。Horizon ポッド - Connection Server への Universal Broker プラグインのインストールを参照してください。
- 外部ネットワーク上のエンド ユーザーによるこのポッドの使用をサポートする場合、または 2 要素認証を使用する場合は、ポッドの外部 Unified Access Gateway インスタンスを構成する必要があります。Horizon ポッド - Universal Broker で使用する Unified Access Gateway を構成するを参照してください。
- Universal Broker に 2 要素認証を使用する場合は、ポッド内のすべての外部 Unified Access Gateway インスタンスが同じ 2 要素認証設定で構成されていることを確認します。また、これらの設定が、マルチクラウド割り当てに参加している他のすべてのポッドのすべての Unified Access Gateway インスタンスの 2 要素認証設定と一致していることを確認します。
- Universal Broker を Horizon ポッドのテナント全体のコネクション ブローカとして有効にして構成します。Horizon Universal Console を使用した Universal Broker の有効化の開始および Universal Broker の設定を参照してください。
- テナントの Universal Broker 設定で 2 要素認証がすでに構成されている場合、コンソールはこのワークフローで外部 Unified Access Gateway と外部 FQDN を強制的に指定します。

手順

1. [設定] - [キャパシティ] をクリックします。[ポッド] タブをまだ選択していない場合は、選択します。
2. リスト内のポッドを選択し、[詳細] - [状態の変更] をクリックします。

   コンソールに、状態変更ワークフローのウィンドウが表示されます。
3. 状態変更ワークフローのウィンドウで、ポッドとサイトの関連付けを設定します。
   - ポッドを新しいサイトに関連付けるには [新規] を選択し、新しいサイトの名前を入力します。
   - ポッドを既存のサイトに関連付けるには [既存] を選択し、ドロップダウン メニューからサイトを選択します。

4 （オプション）外部ネットワーク上のエンド ユーザーによるこのポッドの使用をサポートする場合、または 2 要素認証を使用する場合は、トグルを有効にして、外部 FQDN（完全修飾ドメイン名）を指定します。通常、FQDN は次のように定義されます。

- ポッドに複数の外部 Unified Access Gateway インスタンスがある場合は、ローカル ロード バランサのアドレスをポッドの FQDN として指定します。
- ポッドに外部 Unified Access Gateway インスタンスが 1 つしかない場合は、その Unified Access Gateway インスタンスのアドレスをポッドの FQDN として指定します。

5 （オプション） ポッドに内部 Unified Access Gateway インスタンスも含まれている場合は、内部エンド ユーザーが内部ネットワーク上のデスクトップにアクセスできるようにするかどうかを指定し、内部 FQDN を指定します。

このトグルを有効にすると、ポッドの内部 FQDN を指定するためのフィールドが表示されます。

- ポッドに複数の内部 Unified Access Gateway インスタンスがある場合は、これらのインスタンスによって使用されるローカル ロード バランサのアドレスを、ポッドの内部 FQDN として指定します。
- ポッドに内部 Unified Access Gateway インスタンスが 1 つしかない場合は、その Unified Access Gateway インスタンスのアドレスをポッドの内部 FQDN として指定します。

6 [保存] をクリックします。

結果

ポッドは検証プロセスを実行し、Universal Broker のシステム要件で説明されている必要な構成をすべて満たしていることを確認します。ポッドの検証プロセスが成功すると、ポッドの Universal Broker 環境への参加が有効になり、[キャパシティ] ページにはポッドの状態が [管理対象] として表示されます。

注： ポッドの検証プロセスが失敗すると、不足しているシステム構成の詳細を示すメッセージが表示されます（たとえば Universal Broker プラグインがインストールされていない、など）。ポッドの管理対象状態への変更を再試行する前に、必要なアクションを実行してポッドの構成を修正します。

次のステップ

ポッドに内部 Unified Access Gateway インスタンスがあり、2 要素認証を使用するように Universal Broker を構成済みで、内部エンド ユーザーに対して 2 要素認証をバイパスしたい場合は、内部ネットワーク範囲を定義し、それらのユーザーの 2 要素認証をスキップするための内部接続として Universal Broker が識別できるようにします。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。

Horizon ポッド - ポッドを監視対象状態に変更する

Horizon ポッド（Horizon Connection Server テクノロジー ベース）を管理対象状態から監視対象状態に変更するには、最初にポッドを切断してから、Horizon Cloud に再デプロイする必要があります。ポッドを再デプロイすると、[キャパシティ] ページに監視対象状態として表示されます。

手順

1 そのポッドを含むデスクトップ割り当てからポッドを削除します。詳しい手順については、Horizon Cloud テナント環境でのマルチクラウド割り当ての編集を参照してください。

2 ポッドを Horizon Cloud から切断します。詳しい手順については、クラウド接続された Horizon ポッドを Horizon Cloud での使用から削除するを参照してください。

ポッドが Horizon Cloud から切断され、ポッドの名前は [キャパシティ] ページから消えます。

注： プロセス中にオフラインだった Horizon ポッドからクラウド管理プロパティをクリアして Horizon Cloud から切断するで説明されている手順を実行する必要はありません。

3 この手順を繰り返して、ポッドを Horizon Cloud にオンボーディングします。詳細については、第 1 世代テナント - 第 1 世代 Horizon Universal Console の [キャパシティ] の概要と、Horizon Cloud のポッド フリートへのポッドの追加を参照してください。

結果

オンボーディングされたポッドが、[キャパシティ] ページに監視対象状態として表示されます。

Universal Broker 環境での割り当ての作成および管理

割り当ては、エンド ユーザーの仮想デスクトップとリモート アプリケーションのプールを定義し、それらの使用資格をエンド ユーザーに付与できる Horizon Universal Console の概念的なエンティティです。Universal Broker 環境で割り当てを作成するには、Horizon Universal Console を使用します。ポッドのタイプによっては、割り当てに含める前に特定の設定でプールを構成する必要がある場合があります。

必要なプールの準備手順

Universal Broker 環境の割り当てに参加するには、Horizon ポッドの VDI デスクトップ プールまたは RDSH プールを、Universal Broker に必要な特定の設定で準備する必要があります。これらの必須設定を使用して新しいプールを作成するか、既存のプールを変更して、Universal Broker によって仲介される割り当てで使用できるようにすることができます。次のページの情報を参照してください。

Horizon ポッド - マルチクラウド割り当てに適したデスクトップ プールの作成

Horizon ポッドでデスクトップ プールを作成し、Universal Broker およびマルチクラウド割り当てでの使用に適したものにする場合は、プールで特定の必須設定を構成する必要があります。このドキュメント ページでは、これらの必須の要素について説明します。

このページでは、デスクトップ プールを Universal Broker およびマルチクラウド割り当てでの使用に適したものにする要素のみを説明します。Horizon ポッドでのデスクトップ プールの作成に関する全体的な情報が必要な場合は、ポッドのソフトウェア バージョンに応じて、『Horizon での仮想デスクトップのセットアップ』（Horizon 7 7.13 バージョンの場合）または『Horizon の Windows デスクトップとアプリケーション』（VMware Horizon 8 バージョン 2006 以降の場合）のいずれかのガイドを参照してください。

注： 手動デスクトップ プールは、マルチクラウド割り当てに参加する資格がありません。

手順

1 ターゲット ポッド内の Connection Server インスタンスの Horizon Console ユーザー インターフェイスにログインします。

2 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。

3 [追加] をクリックします。

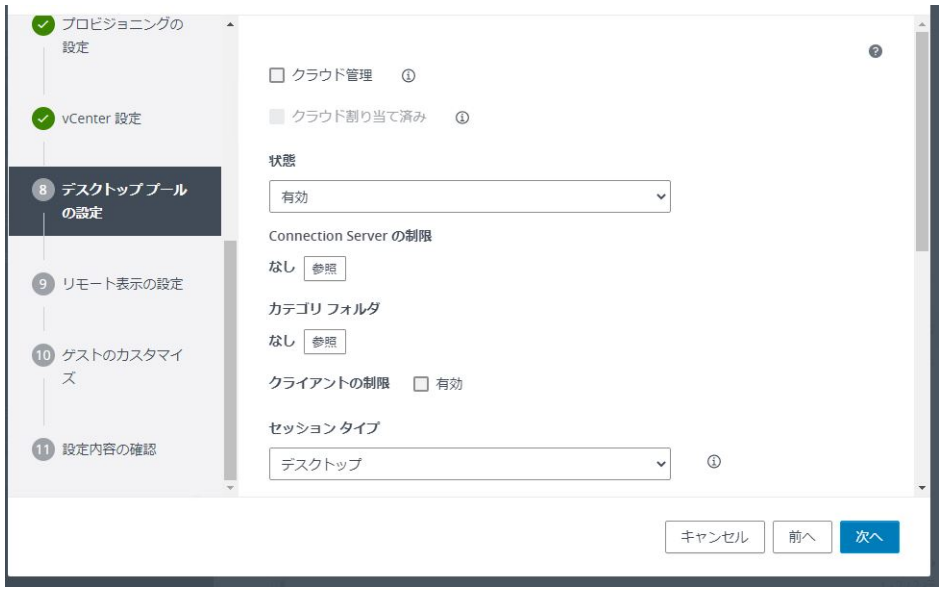
[プールの追加] ウィザードが開きます。

4 ウィザードの指示に従って、マルチクラウド割り当てに適したプールを設定する次の必須構成を行います。

- [タイプ] ページ：[自動化されたデスクトップ プール] を選択します。
- [vCenter Server] ページ：[インスタント クローン] または [フル仮想マシン] を選択します。
- [ユーザー割り当て] ページ: [フローティング] または [専用] を選択します。

  [専用] を選択した場合は、[自動割り当てを有効化] も選択します。

  ユーザーへのマシンの手動割り当てを構成しないでください。
- [デスクトップ プールの設定] ページ: [クラウド管理] を選択します。Universal Broker は [クラウド管理] としてマークされたデスクトップ プールのみを認識します。



注： Horizon Console を使用して、[クラウド管理] として構成されたデスクトップ プールを削除または無効化することはできません。

- [リモート表示設定] ページ：デスクトップ プールのデフォルトの表示プロトコルを選択します。

5 プールの追加設定を行うには、ウィザードのプロンプトに従って操作を続行します。

6 [送信] をクリックして、プールを作成します。

次のステップ

Universal Broker およびマルチクラウド割り当てで使用するために専用プールを構成した場合、プールに含まれる仮想マシンからユーザー割り当てを削除します。ユーザー割り当ての削除については、ポッドのソフトウェア バージョンに応じて、『Horizon での仮想デスクトップのセットアップ』（Horizon 7 7.13 バージョンの場合）または『Horizon の Windows デスクトップとアプリケーション』（VMware Horizon 8 バージョン 2006 以降の場合）のいずれかのガイドを参照してください。

デスクトップ プールがマルチクラウド割り当てでの使用に適した構成になったので、Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成に進みます。

Horizon ポッド - マルチクラウド割り当てに使用する既存のデスクトップ プールを準備する

Horizon ポッドの既存のデスクトップ プールを Universal Broker で使用する場合は、プールを Universal Broker およびマルチクラウド割り当てでの使用に適したものにする必要があります。このドキュメント ページでは、プールがその使用に適した条件について説明します。

Universal Broker は、特定の条件を満たす場合にのみデスクトップ プールをサポートします。

- Universal Broker によって仲介されるマルチクラウド割り当てで既存のデスクトップ プールを使用するには、以下の手順で説明する必須の設定を使用してプールを構成する必要があります。
- また、プールからすべてのローカル資格を削除し、プールに含まれる仮想マシンからユーザー割り当てを削除する必要があります。

注： 手動デスクトップ プールは、マルチクラウド割り当てに参加する資格がありません。

手順

1. デスクトップ プールを含むポッド内の Connection Server インスタンスの Horizon Console ユーザー インターフェイスにログインします。
2. Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。リストで、マルチクラウド割り当てで使用するデスクトップ プールを選択し、[編集] をクリックします。

   [プールの編集] ウィザードが開きます。
3. [全般] タブをクリックします。[ユーザー割り当て] で、[自動割り当てを有効化] を選択します（プール タイプでこのオプションが使用可能な場合）。
4. [デスクトップ プールの設定] のタブをクリックして、次の設定を指定します。
   - [状態] には [有効] を選択します。
   - [Connection Server の制限] では、[参照] をクリックし、[制限なし] を選択してから [送信] をクリックします。
   - [全般] で、[クラウド管理] を選択します。Universal Broker は [クラウド管理] としてマークされたデスクトップ プールのみを認識します。

5 構成を保存し、[プールの編集] ウィザードを閉じるには、[OK] をクリックします。

6 デスクトップ プールからローカル資格をすべて削除するには、[デスクトップ プール] ページでプールを選択し、[資格] - [資格を削除] を選択します。

7 このプールが専用デスクトップ プールの場合は、プールに含まれる仮想マシンからユーザー割り当てを削除します。

手順については、ポッドのソフトウェア バージョンに応じて、『Horizon での仮想デスクトップのセットアップ』（Horizon 7 7.13 バージョンの場合）または『Horizon の Windows デスクトップとアプリケーション』（VMware Horizon 8 バージョン 2006 以降の場合）のいずれかのガイドを参照してください。

次のステップ

デスクトップ プールがマルチクラウド割り当てでの使用に適した構成になったので、Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成に進みます。

Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成

クラウド接続された Horizon ポッドによってプロビジョニングされた仮想デスクトップをエンド ユーザーに提供するには、マルチクラウド割り当てを作成します。割り当て内のデスクトップ プールは、管理対象状態にある 1 つ以上のクラウド接続 Horizon ポッドに配置できます。

VDI マルチクラウド割り当てあたりの Horizon 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 Connection Server タイプのポッドの最大数は 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。

前提条件

- クラウド接続された Horizon ポッドを管理状態に変更します。View ポッド - マルチクラウド割り当てのためのクラウド接続されたポッドの有効化を参照してください。
- Universal Broker のサイトの構成および Universal Broker のホーム サイトの構成の説明に従って、仲介環境にサイトとホーム サイトの関連付けを構成します。
- Horizon Console を使用して、割り当てに含めるクラウド接続ポッド上でデスクトップ プールを構成します。

  Horizon ポッド - マルチクラウド割り当てに適したデスクトップ プールの作成および Horizon ポッド - マルチクラウド割り当てに使用する既存のデスクトップ プールを準備するを参照してください。これらのトピックで説明するように、デスクトップ プールが Universal Broker の構成要件を満たしていることを確認します。

手順

1. コンソールの左ペインで、[割り当て] をクリックします。サブメニューが表示された場合は、VDI デスクトップのオプションを選択します。
2. [割り当て] ページで [新規] を選択し、VMware SDDC プラットフォーム上の Horizon ポッドのサブメニュー オプションを選択します。

   [新しいデスクトップの割り当て] ウィザードが表示されます。
3. [定義] ページで、必要な設定を構成します。

設定	説明
[デスクトップ タイプ]	次のいずれかのオプションを選択します。 ■ [フローティング]：フローティング割り当てでは、ユーザーはログインするたびにマシン名が異なる別の仮想マシンを受け取ります。フローティング割り当てでは、ユーザーのシフトに合わせてデスクトップを作成できます。この場合、同時実行ユーザーの最大数を基準としてサイジングされます。たとえば、ユーザーがシフトして作業しており、1 度に 100 ユーザーが作業している場合は、300 ユーザーが 100 台のデスクトップ割り当てを使用できます。フローティング割り当てでは、ユーザーに各デスクトップ セッションで異なるホスト名が表示される場合があります。 ■ [専用]：専用の割り当てでは、各仮想デスクトップが特定のユーザーにマッピングされます。マッピングされた各ユーザーは、ログインするたびに同じデスクトップに戻ります。専用のデスクトップが特定のユーザーにマッピングされると、そのデスクトップはそのユーザーに割り当てられたということになります。 **注：** 特定のユーザーは、1 つの割り当てに複数のポッドのデスクトップが含まれていても、Universal Broker によって仲介された専用割り当てから最大で 1 つの割り当てられたデスクトップを受信できます。 この設定は、既存の割り当てを編集するときに読み取り専用になります。
[デスクトップ名]	割り当てにはわかりやすい名前を入力します。 資格のあるエンド ユーザーが、クライアントでデスクトップにアクセスする際に、この形式の割り当ての名前が表示されます。名前には文字、ハイフン、数字のみを含める必要があります。スペースは使用できません。名前を英字以外の文字で始めることはできません。
[説明]	割り当てのオプションの説明を入力します。

設定	説明
[ポッドの選択]	割り当てに追加するデスクトップ プールを含む各ポッドの横にあるチェック ボックスをオンにします。複数のポッドを選択して、異なるポッドのデスクトップ プールからなる割り当てを作成できます。 **注：** 1 つの VDI マルチクラウド割り当てでサポートされる Horizon Connection Server タイプのポッドの最大数は 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。
[範囲]	ユーザーのデスクトップ要求に応答してブローカがデスクトップを検索できる場所を指定するには、次のいずれかのオプションを選択します。 ■ [任意のサイト] を選択すると、ブローカは構成された任意の地理的な場所にある利用可能なデスクトップを検索できます。 ■ [1 つのサイトに制限] は、ブローカに対して、[サイト接続のアフィニティ] で指定したユーザーのデフォルト サイトにある利用可能なデスクトップのみを検索するよう指示します。 サイトおよびデスクトップ割り当ての概要については、Universal Broker 環境でのサイトの操作を参照してください。
[サイト接続のアフィニティ]	この設定は、特定の地理的サイトをユーザーのデフォルト サイトとして指定します。ユーザーがデスクトップを要求すると、ブローカはデフォルト サイトで利用可能なデスクトップの検索を開始します。デフォルト サイトに使用可能なデスクトップが見つからず、サイトの制限が有効になっていない場合、ブローカはデフォルト サイト以外でデスクトップの検索を続けます。 以下のいずれかのオプションを選択します。 ■ [最も近いサイト] は、最も近い地理的サイトをユーザーのデフォルト サイトとして指定します。 ■ [ホーム サイト] は、ユーザーのホーム サイト（またはユーザーを含むグループのホーム サイト）をそのユーザーのデフォルト サイトとして指定します。 ■ ユーザーが構成済みのホーム サイトの外部でもデスクトップにアクセスできるようにするには、[ホーム サイト制限] を有効にしないでください。 ■ デスクトップにアクセスする場合にユーザーを構成済みのホーム サイトに制限するには、[ホーム サイト制限] を有効にします。 **重要：** [ホーム サイト制限] を有効にすると、ユーザー（またはユーザーを含むグループ）は、デスクトップにアクセスする前にホーム サイトを構成する必要があります。

[定義] 設定を構成した後、[次へ] をクリックしてウィザードの次のページに進みます。

4 [デスクトップ] ページで、マルチクラウド割り当てに追加できるデスクトップ プールをフィルタするために使用される構成プロパティとポリシーを指定します。

たとえば、[オペレーティング システム] に [Windows 10 (64 ビット)] を指定し、[ユーザーによる仮想マシンの再起動を許可] ポリシーを有効にした場合、[ユーザーによる仮想マシンの再起動を許可] ポリシーを有効にした Windows 10（64 ビット）に基づくデスクトップ プールのみを割り当てに含めることができます。

オプション	説明
[オペレーティング システム]	割り当てに含めるデスクトップ プールのオペレーティング システムを指定します。 メニューには、Windows Server 2016 を参照する [Windows Server 2016] と [Windows Server 2016 以降] という 2 つの選択肢が表示されることがあります。[Windows Server 2016 以降] を選択すると、Windows Server 2016 以降の Windows Server バージョン（Windows Server 2019 など）で構成されたプールと一致します。 **注：** この設定は、既存の割り当てを編集するときに読み取り専用になります。
[デフォルト表示プロトコル]	割り当てに含めるデスクトップ プールのデフォルト表示プロトコルを選択します。

オプション	説明
[ユーザーによるプロトコル選択を許可]	このポリシーは、ユーザーがデフォルト以外の表示プロトコルを選択できるかどうかに基づいて、デスクトップ プールをフィルタリングします。 **注：** この設定は、既存の割り当てを編集するときに読み取り専用になります。
[HTML Access]	このポリシーは、ユーザーが HMTL Access クライアントを使用して Web ブラウザから仮想デスクトップに接続できるかどうかに基づいて、デスクトップ プールをフィルタリングします。この機能の詳細については、『VMware Horizon HTML Access のドキュメント』を参照してください。
[ユーザーによる仮想マシンの再起動を許可]	このポリシーは、ユーザーがオペレーティング システムを正常に再起動して仮想マシンを再起動できるかどうかに基づいて、デスクトップ プールをフィルタリングします。このポリシーは、vCenter Server 仮想マシンが含まれる自動プールまたは手動プールにのみ適用されます。 **注：** この設定は、既存の割り当てを編集するときに読み取り専用になります。
[冗長セッションをクリーンアップ]	このポリシーは、重複したユーザー セッションを自動的に閉じるかどうかを指定します。 セッションの重複は、セッションを含むポッドがオフラインになり、ユーザーが再度ログインして別のセッションを開始し、問題のポッドが元のセッションでオンラインに戻るときに発生する可能性があります。セッションの重複が発生すると、Horizon Client がユーザーにセッションを選択するように求めます。 このポリシーは、ユーザーが選択しないセッションに何が発生するかを決定します。このポリシーを無効にすると、ユーザーは Horizon Client クライアントでログオフするか、セッションを起動してからログオフして、独自の余剰セッションを手動で終了する必要があります。
[デスクトップ プールの選択]	割り当てに追加する各デスクトップ プールの横にあるチェック ボックスをオンにします。1 つの割り当てに複数のプールを追加できます。 必要なデスクトップ プールがリストに見つからない場合は、次のことを確認します。 ■ デスクトップ プールが手動プールではない。手動デスクトップ プールは、マルチクラウド割り当てに参加する資格がありません。 ■ デスクトップ プールのプロパティとポリシーは、このマルチクラウド割り当てに指定したプロパティとポリシーと一致します。たとえば、[オペレーティング システム] に [Windows 10 (64 ビット)] を指定し、[ユーザーによる仮想マシンの再起動を許可] ポリシーを有効にした場合、デスクトップ プールは Windows 10（64 ビット）をベースにし、[ユーザーによる仮想マシンの再起動を許可] ポリシーを有効にする必要があります。 ■ Horizon ポッド - マルチクラウド割り当てに使用する既存のデスクトップ プールを準備するで説明するように、デスクトップ プールが Universal Broker をサポートするための構成要件を満たしている。

[デスクトップ] 設定を指定した後、[次へ] をクリックしてウィザードの次のページに進みます。

5 [ユーザー] ページで、割り当ての使用資格を付与するユーザーとユーザー グループを指定します。

オプション	説明
[ドメイン]	ユーザーとグループが常駐する Active Directory ドメインを指定します。 **注：** 選択できるのは、クラウド構成のドメインのみです。
[ユーザーを検索]	ユーザー名またはグループ名の最初の数文字を入力し、表示されるリストからユーザーまたはユーザー グループを選択します。 選択した項目が [選択されたユーザー/ユーザー グループ] リストに追加されます。[削除] ボタンを使用して、リストから選択したユーザーまたはグループを削除できます。
[ホーム サイトの割り当て]	このオプションの設定を使用して、この割り当てにアクセスしている選択したユーザーまたはグループのホーム サイトの上書きを構成します。この場合、Universal Broker は、ユーザーまたはグループの構成済みホーム サイトではなく、上書きサイトで使用可能なデスクトップの検索を開始します。 たとえば、あるユーザーがサンフランシスコにホーム サイトを持っていて、その上書きサイトとしてニューヨークを指定したとします。ユーザーが割り当てにアクセスすると、Universal Broker は最初にサンフランシスコではなく、ニューヨークで利用可能なデスクトップを検索します。 **注：** [ホーム サイトの割り当て] メニューは、ウィザードの [定義] ページで [サイト接続のアフィニティ] に [ホーム サイト] を選択した場合にのみ使用できます。 ホーム サイトの上書きを指定するには、ユーザーまたはグループを選択し、[ホーム サイトの割り当て] をクリックします。[ホーム サイトの割り当て] メニューには、この割り当てに参加しているポッドで利用可能なすべてのサイトが表示されます。 ■ ユーザーまたはグループの構成済みホーム サイトではなく、デフォルトとして上書きサイトを指定するには、メニューで上書きサイトを選択します。 ■ 上書きサイトを削除して、代わりにユーザーまたはグループの構成済みホーム サイトを使用するには、[ホーム サイトのクリア] を選択します。

[ユーザー] 設定を指定した後、[次へ] をクリックしてウィザードの次のページに進みます。

6 [サマリ] ページの設定を確認して、[終了] をクリックします。

結果

[割り当て] ページのリストに、新しく作成された割り当てが表示されます。

割り当てに含まれている各デスクトップ プールは、Horizon Console の [プールの編集] ウィザードで、[クラウド割り当て] としてマークされるようになりました。Horizon Console を使用して、[クラウド割り当て] としてマークされたデスクトップ プールを削除または無効にすることはできません。

注： Horizon Client ユーザーがマルチクラウド割り当てからフローティング デスクトップにログインすると、[冗長セッションをクリーンアップ] ポリシーが有効になっていても、重複した接続セッションが発生する場合があります。ユーザーが重複するセッションから手動でログアウトしようとすると、「ログオフする現在のセッションがありません。」というエラー メッセージが表示されます。このエラーは、割り当てのポリシーによって重複するセッションがすでに終了している一方で、Horizon Client がセッションの終了状態をまだ反映していないために発生します。ユーザーがエラー メッセージを閉じると、Horizon Client は表示を更新し、重複するセッションは表示されなくなります。

Horizon ポッド - Universal Broker 環境用の RDSH デスクトップとアプリケーションの構成

この記事では、セッション デスクトップ プールとリモート アプリケーション プールをクラウド管理の Horizon ポッドから Universal Broker 環境に追加する方法について説明します。これらのプールは RDSH プールとも呼ばれ、単一の Horizon ポッド内の Microsoft リモート デスクトップ サービス (RDS) ホストによってプロビジョニングされたリソースで構成されます。エンド ユーザーは、Universal Broker FQDN に接続することでセッションを開くことができ、Universal Broker はこれらのセッションのコネクション ブローカとして機能します。

RDSH プールは、単一の Horizon ポッド内の Microsoft リモート デスクトップ サービス (RDS) ホストによってプロビジョニングされたデスクトップまたはアプリケーションで構成されます。Universal Broker 環境に RDSH プールを追加すると、プールは Horizon Universal Console で読み取り専用の割り当てになります。詳細については、Horizon ポッド - Horizon Universal Console での RDSH 割り当ての操作を参照してください。

前提条件

次の前提条件の手順を完了していることを確認します。

- Universal Broker を Horizon ポッドのコネクション ブローカとして有効にして構成します。Horizon Universal Console を使用した Universal Broker の有効化の開始および Universal Broker の設定を参照してください。

- RDSH デスクトップまたはアプリケーション プールのソースである Horizon ポッドの場合：
  - ポッド内のすべての Connection Server インスタンスが VMware Horizon 8 バージョン 2103 (8.2) 以降を実行していることを確認します。
  - ポッドがバージョン 1.10 以降の Horizon Cloud Connector アプライアンスとペアリングされていることを確認します。バージョン 1.10 で初登場した RDSH デスクトップまたはアプリケーション プールのサポート。ただし、最新のセキュリティおよびバグ修正と改善を取得するには、最新バージョンの Horizon Cloud Connector を使用することを強くお勧めします。
  - ポッドを管理対象状態に変更します。Horizon Universal Console を使用して、クラウド接続された Horizon ポッドを管理対象状態に変更するを参照してください。

手順

1 構成する RDSH デスクトップまたはアプリケーション プールを含むポッドの Horizon Console（Horizon ポッドの管理者コンソール）を開きます。

Horizon Console の使用方法の詳細については、VMware Horizon のドキュメントを参照してください。

2 Horizon Console で、RDSH デスクトップまたはアプリケーション プールを構成するためのウィザードを開きます。

3 構成ウィザードで、プールの [クラウド仲介] オプションを有効にします。

Universal Broker は、[クラウド仲介] としてマークされた RDSH デスクトップおよびアプリケーション プールのみを認識します。

- RDSH デスクトップ プールの場合、プール設定を構成できるウィザードのセクションに [クラウド ブローカ] オプションが表示されます。
- アプリケーション プールの場合、アプリケーションを追加できるウィザードのセクションに [クラウド ブローカ] オプションが表示されます。

4 変更をプールに保存するには、構成ウィザードのプロンプトに従います。

プールの構成情報が Universal Broker サービスと同期されるまで最大で 10 分かかることがあります。

5 Horizon Universal Console で、VMware SDDC のポッドから RDSH デスクトップおよびアプリケーションの割り当てページに移動します。[クラウド仲介] として構成したプールがページにリストされた割り当てとして表示されることを確認します。

結果

資格のあるユーザーは、Universal Broker FQDN に接続することで、プールのデスクトップまたはアプリケーションにアクセスできるようになりました。

プールの構成情報は、次のタイミングで Universal Broker サービスに自動的に同期されます。

- プールが Horizon Console に作成されたとき。
- プールの構成が Horizon Console で変更されたとき。
- プールが Horizon Console で削除されたとき。

詳細については、Horizon ポッド - Horizon Universal Console での RDSH 割り当ての操作を参照してください。

Horizon ポッド - Horizon Universal Console での RDSH 割り当ての操作

クラウド管理の Horizon ポッドで適切な構成で RDSH デスクトップまたはアプリケーション プールを準備すると、プールはテナント環境で RDSH 割り当てとして使用できるようになり、Horizon Universal Console を使用してこれらの割り当てを表示および監視できます。

RDSH 割り当てをテナントに追加する方法については、Horizon ポッド - Universal Broker 環境用の RDSH デスクトップとアプリケーションの構成を参照してください。

注： 次の機能制限と考慮事項は、Horizon ポッド（Horizon Connection Server テクノロジー ベース）のクラウド仲介された RDSH デスクトップおよびアプリケーション プールに適用されます。

- RDSH プールは、Horizon Universal Console では読み取り専用の RDSH 割り当てとして表示されます。Horizon Universal Console を使用してこれらの割り当ての構成を変更することはできません。
- RDSH 割り当ての構成を変更するには、Horizon Console（Horizon ポッドの管理者コンソール）を使用する必要があります。
- RDSH 割り当ては、Horizon Universal Console の検索機能をサポートしていません。この機能を使用してユーザーまたは仮想マシン (VM) を検索する場合、Horizon ポッドからの RDSH 割り当ては検索の範囲に含まれません。

Horizon Universal Console でクラウド仲介された RDSH 割り当ての詳細を表示するには、VMware SDDC のポッドから RDSH デスクトップとアプリケーションの割り当てページに移動します。環境にクラウド仲介された RDSH が割り当てられた複数のポッドがある場合は、ページ上部のメニューを使用して特定のポッドを選択します。

ページにリストされている割り当ての名前をクリックすると、[サマリ]、[セッション]、[資格] の 3 つのタブで構成される割り当ての詳細ページが開きます。各タブでさまざまな種類の情報を表示できます。タブに表示される情報は、Horizon Console で定義されている RDSH プールの現在の構成を反映しています。

[サマリ] タブ

割り当ての詳細ページの [サマリ] タブでは、基盤となるファームに関する情報など、RDSH プールのステータスと構成に関する一般的な情報を確認できます。次のアクションを実行することもできます。

アクション	説明
[今すぐ同期]	プールの構成情報を Universal Broker サービスに手動で同期します。手動同期を実行して、自動同期が失敗した場合や遅延した場合に発生する問題を解決できます。 たとえば、次のような場合に手動同期を実行します。 ■ Horizon Universal Console に自動同期の失敗に関する通知が表示されたとき。 ■ 資格のあるユーザーが、Universal Broker FQDN に接続した後でプール リソースを表示できない、またはアクセスできないとき。 ■ ポッドを Horizon Cloud Connector とペアリングして管理対象状態に変更する前に、Horizon ポッドの Horizon Console で既存の RDSH デスクトップまたはアプリケーション プールが構成されていた場合。既存の RDSH プールは Universal Broker サービスと自動的に同期されないため、個々のプールを手動で同期する必要があります。 自動同期が通常発生するタイミングの詳細については、Horizon ポッド - Universal Broker 環境用の RDSH デスクトップとアプリケーションの構成を参照してください。
[Horizon Console の起動]	プールのソースであるポッドの Horizon Console を開きます。 **注：** Horizon Console でプールの [クラウド仲介] オプションを無効にすると、プールは Horizon Universal Console に割り当てとしてリストされなくなり、ユーザーは Universal Broker FQDN を介して RDSH 割り当てにアクセスできなくなります。 場合によっては、[クラウド仲介] オプションを無効にしたり、Horizon Console でプールを削除したりした後も、Universal Broker FQDN を介して RDSH プールにアクセスできる場合があります。このような状況が発生した場合は、VMware サポートに連絡して、Universal Broker サービスからの RDSH プールの削除を要求してください。

[セッション] タブ

割り当ての詳細ページの [セッション] タブには、プールで現在開いているユーザー セッションが一覧表示されます。

[資格] タブ

割り当ての詳細ページの [資格] タブには、Horizon Console で構成されているように、プールのリソースにアクセスする資格のあるユーザーが一覧表示されます。

[ユーザー アクティビティ] タブ

割り当ての詳細ページの [ユーザー アクティビティ] タブには、割り当てによって提供されるセッションのログインやログオフなど、ユーザー アクションによって発生する割り当て内のアクティビティが表示されます。

表示された情報をレポート ファイルとしてエクスポートするには、[エクスポート] 機能をクリックし、画面上の指示に従います。

Horizon ポッド - マルチクラウド割り当てからのデスクトップ プールの削除

Horizon ポッドで構成されたマルチクラウド割り当てからデスクトップ プールを削除するには、一連の適切な手順を適切な順序で実行する必要があります。最初にプールを含む割り当てを変更してから、プールの [クラウド管理] 設定をクリアする必要があります。

このシーケンスを完了すると、デスクトップ プールは Horizon Console で構成されたローカル資格で使用可能になります。

重要： マルチクラウド割り当てからデスクトップ プールを削除するには、常に一連の適切な手順を使用します。Horizon Console の [クラウド割り当て] 設定を手動でクリアしてプールを削除しないでください。[クラウド割り当て] を手動でクリアしても、プールはマルチクラウド割り当てとの関連付けを保持し、Universal Broker は割り当てを要求しているユーザーにプールからデスクトップを仲介できます。

手順

1 Horizon Universal Console で、デスクトップ プールを含むマルチクラウド割り当てを編集します。

   a コンソールの左ペインで、[割り当て] をクリックします。[割り当て] メニューから [オンプレミスおよび VMware Cloud] を選択します。

   b [割り当て] ページで、デスクトップ プールを含む割り当ての横にあるチェック ボックスをオンにして、[編集] をクリックします。

   c [デスクトップ割り当ての編集] ウィザードで、[デスクトップ] ページに移動し、削除するデスクトップ プールを選択解除します。

   d [終了] をクリックします。

2 デスクトップ プールを含むポッド内の Connection Server インスタンスの Horizon Console ユーザー インターフェイスにログインします。次に、プールの構成設定を変更します。

   a Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。

   [プールの編集] ウィザードが開きます。

   b リストからデスクトップ プールを選択し、[編集] をクリックします。

   c [デスクトップ プールの設定] タブをクリックします。[全般] で、[クラウド割り当て] 設定がクリアされていることを確認します。

   Horizon Universal Console でマルチクラウド割り当てからプールを削除すると、[クラウド割り当て] 設定は自動的にクリアされます。

d [全般] で、[クラウド管理] 設定をクリアします。

これで、Horizon Console のローカル資格でプールが使用できるようになります。

次のスクリーンショットは、ローカル資格で使用可能で、マルチクラウド割り当てに参加しなくなったデスクトップ プールの構成を示しています。

e [OK] をクリックして [プールの編集] ウィザードを閉じます。

Microsoft Azure の Horizon Cloud ポッド - 第 1 世代環境での VDI マルチクラウド割り当ての作成と表示

このドキュメント ページでは、Horizon Cloud ポッドから VDI マルチクラウド割り当てを作成し、その詳細を表示する方法について説明します。これらのポッドは、Horizon Cloud ポッド マネージャ テクノロジーに基づいて構築されたポッドです。

割り当て構成ウィザードを使用して、Microsoft Azure の複数の Horizon Cloud ポッドによってプロビジョニングされるデスクトップの VDI マルチクラウド割り当てを作成します。

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。

エンド ユーザーがこれらの VDI マルチクラウド割り当てのいずれかからプロビジョニングされたデスクトップに適切にアクセスするためにクライアントで使用する URL について

環境が Horizon Cloud ポッドで Universal Broker を使用するように構成されている場合にのみ、それらの Horizon Cloud ポッドを使用して VDI マルチクラウド割り当てを作成できます。これらのポッドで Universal Broker を使用するように環境が構成されている場合、エンド ユーザーはクライアントで環境の構成済みの Universal Broker URL を使用して、これらのマルチクラウド割り当てによってプロビジョニングされた、使用資格のある VDI デスクトップにアクセスすることを期待されています。環境が Universal Broker を使用するように構成されている場合は、エンド ユーザーがクライアントで Unified Access Gateway FQDN を使用するという旧式の方法を使用しないようにします。エンド ユーザーが Universal Broker をバイパスして Unified Access Gateway FQDN に直接移動した場合、予期しない結果が発生する可能性があります。

エンド ユーザーがクライアントで確認できるデスクトップ タイルに表示されるラベルについて

エンド ユーザーがクライアントで Universal Broker URL を使用すると、次の割り当て作成手順で説明するように、クライアントのデスクトップ タイルのラベルに、マルチクラウド割り当てフォームの [割り当ての名前] で指定した名前が表示されることに注意してください。

ただし、以前に使用した、Unified Access Gateway FQDN を使用するシングルポッド仲介方法を使用するようにエンド ユーザーに指示すると、デスクトップ タイルには、[割り当ての名前] で指定された正確な名前ではなく、[割り当ての名前] で指定された名前のバリエーションが表示されます。タイルには、[割り当ての名前] フィールドに表示される割り当ての名前に加えて、一意の 8 文字のサフィックスが付加されます。

たとえば、マルチクラウド割り当ての定義で [割り当ての名前] が **`Dedicated-Sales`** として指定されている場合、次のようになります。

- Universal Broker URL を使用しているクライアント - エンド ユーザーには、**`Dedicated-Sales`** というラベルの付いたデスクトップ タイルが表示されます。
- 代わりに Unified Access Gateway FQDN を使用しているクライアント - エンド ユーザーには、**`Dedicated-Sales`**-*nnnnnnnn* というラベルの付いたデスクトップ タイルが表示されます。ここでの *nnnnnnnn* は一意のランダムな英数字の文字列です。この例で、2 人のエンド ユーザーがデスクトップの Universal Broker URL の代わりに Unified Access Gateway FQDN を使用している場合、一方のエンド ユーザーのデスクトップ タイルには **`Dedicated-Sales-d1f466f1`** というラベルが付けられ、もう一方のエンド ユーザーのタイルには **`Dedicated-Sales-6bdbb611`** というラベルが付けられます。

重要： これらのポッドで Universal Broker を使用するように構成されている場合、エンド ユーザーはクライアントで Universal Broker URL を使用して、これらの割り当てからプロビジョニングされた VDI デスクトップにアクセスすることが期待されます。

前提条件

- VDI マルチクラウド割り当ては、ポッド マネージャ タイプのポッドで Universal Broker を使用するように構成されているテナント環境で使用できます。このようなポッドは、自動ポッド デプロイ ウィザードを使用して Microsoft Azure にデプロイされるポッドです。テナントが、それらのポッドで使用する仲介方法として Universal Broker を使用するように構成されていることを確認します。Horizon Universal Console を使用した Universal Broker の有効化の開始および Universal Broker の設定を参照してください。
- Universal Broker のサイトの構成および Universal Broker のホーム サイトの構成の説明に従って、仲介環境にサイトとホーム サイトの関連付けを構成します。
- 割り当てへの参加を選択する予定の各ポッドに、Microsoft Windows クライアント オペレーティング システムを備えた少なくとも 1 つの公開イメージがあることを確認します。参加している各ポッドにそのようなイメージがないと、VDI マルチクラウド割り当てを作成できません。たとえば、割り当てに単一のポッドを選択する場合、そのポッドには公開イメージが必要です。この割り当てに複数のポッドを選択する場合は、それらの各ポッドに少なくとも 1 つの公開イメージが必要です。確認するには、[イメージ] ページに移動し、該当するイメージが一覧表示されているかを確認します。公開イメージの作成手順については、構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の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。
- デスクトップに暗号化されたディスクを使用するかどうかを決定します。VDI マルチクラウド割り当てを作成する際は、ディスクの暗号化を指定する必要があります。割り当ての作成後にディスクの暗号化を追加することはできません。ディスクの機能の詳細については、Horizon Cloud 環境のファームと VDI デスクトップでの Microsoft Azure Disk Encryption の使用を参照してください。

  重要： このリリースでは、データ ディスクが接続されたイメージ仮想マシンを使用するフローティング VDI 割り当てのディスク暗号化をサポートしていません。割り当てで使用する予定のイメージにデータ ディスクがないことを確認してください。

- デスクトップ仮想マシンで NSX Cloud 機能を使用できるようにするかどうかを決定します。VDI マルチクラウド割り当てを作成する際は、NSX Cloud 管理を有効にする必要があります。NSX Cloud 管理の割り当ては、作成後に有効にすることはできません。この割り当て用に選択する公開済みイメージには、NSX エージェントがインストールされていることが必要です。イメージの公開前に NSX エージェントをインストールする必要があります。Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッド とそのサブトピックを参照してください。

  重要： NSX Cloud の機能とディスク暗号化の両方を使用するには、イメージにインストールされている NSX エージェントが最新のエージェント バージョンであることを確認します。以前のバージョンの NSX エージェントでディスク暗号化を使用することはサポートされていません。

- ポッドが複数の仮想マシン サブネットを持つように構成されている場合、そのポッドのサブスクリプションにデプロイされているデスクトップ仮想マシンをそれらの仮想マシン サブネットのいずれかに接続するか、そのポッドの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）に接続するかを決定できます。マニフェスト 2298 以降を実行しているポッドを編集して仮想マシン サブネットを追加した場合、それらのサブネットの使用を、その特定のポッドに対してインスタンス化される割り当てのデスクトップ仮想マシンに対して

指定できます。このユースケースでは、使用する仮想マシン サブネットが Ready の状態でポッドの詳細ページの [ネットワーク] セクションに表示されていることを確認する必要があります。これにより、そのサブネットがワークフローの手順で選択できるようになります。詳細については、ファーム用および VDI 割り当て用 Horizon Cloud ポッドでの複数のテナント サブネットの使用の概要 を参照してください。

重要： 割り当てに仮想マシン サブネットの使用を指定すると、選択した仮想マシン サブネットは引き続き有効になり、割り当ての作成後に変更することはできません。また、選択したサブネットによって提供される IP アドレスの総数は、指定された [仮想マシンの最大数] の設定以上である必要があります。たとえば、割り当てにプライマリ サブネットを使用するか、複数の仮想マシン サブネットを使用して割り当てに対し 100 の IP アドレスを使用可能にするかを選択する場合、[仮想マシンの最大数] は 100 を超えることはできません。

手順

1 コンソールの左ペインで [割り当て] をクリックし、VDI デスクトップのサブメニュー オプションを選択します。

2 [割り当て] ページで [新規] をクリックし、Microsoft Azure のデスクトップのサブメニュー オプションを選択します。

[新しいデスクトップ割り当て] ウィンドウが開き、最初のウィザードの手順が表示されます。

3 ウィザードで、必要な設定を構成します。

注： 必要に応じてスクロール バーを使用して、すべての設定内容を表示します。

設定	説明
デスクトップ タイプ	次のいずれかのオプションを選択します。 ■ [フローティング]：フローティング割り当てでは、ユーザーはログインするたびにマシン名が異なる別の仮想マシンを受け取ります。フローティング割り当てでは、ユーザーのシフトに合わせてデスクトップを作成できます。この場合、同時実行ユーザーの最大数を基準としてサイジングされます。たとえば、ユーザーがシフトして作業しており、1 度に 100 ユーザーが作業している場合は、300 ユーザーが 100 台のデスクトップ割り当てを使用できます。フローティング割り当てでは、ユーザーに各デスクトップ セッションで異なるホスト名が表示される場合があります。 ■ [専用]：専用の割り当てでは、各仮想デスクトップが特定のユーザーにマッピングされます。マッピングされた各ユーザーは、ログインするたびに同じデスクトップに戻ります。専用のデスクトップが特定のユーザーにマッピングされると、そのデスクトップはそのユーザーに割り当てられたということになります。 **注：** 特定のユーザーは、1 つの割り当てに複数のポッドのデスクトップが含まれていても、Universal Broker によって仲介された専用割り当てから最大で 1 つの割り当てられたデスクトップを受信できます。 この設定は、既存の割り当てを編集するときに読み取り専用になります。
割り当ての名前	割り当てにはわかりやすい名前を入力します。 このドキュメントのトピックで前述したとおり、資格のあるエンド ユーザーが、クライアントでデスクトップにアクセスする際に、この形式の割り当ての名前がデスクトップ タイルに表示されます。名前には文字、ハイフン、数字のみを含める必要があります。スペースは使用できません。名前を英字以外の文字で始めることはできません。
説明	割り当てのオプションの説明を入力します。

設定	説明
ポッドの選択	この割り当てに参加させたい各ポッドの横にあるチェック ボックスをオンにします。割り当てのデスクトップ仮想マシンは、Microsoft Azure で選択したポッドのサブスクリプションでインスタンス化されます。 **注：** 前提条件のセクションで説明したように、選択した各ポッドには、Microsoft Windows クライアント オペレーティング システムを備えた、少なくとも 1 つの公開イメージが必要です。選択したポッドがこの要件を満たしていない場合、システムは、参加している各ポッドからのイメージを指定するウィザードの次のステップが完了するのを妨げます。
範囲	ユーザーのデスクトップ要求に応答してブローカがデスクトップを検索できる場所を指定するには、次のいずれかのオプションを選択します。 ■ [任意のサイト] を選択すると、ブローカは構成された任意の地理的な場所にある利用可能なデスクトップを検索できます。 ■ [1 つのサイトに制限] は、ブローカに対して、[接続のアフィニティ] 設定で指定したとおりに、ユーザーのデフォルト サイトにある利用可能なデスクトップのみを検索するよう指示します。 サイトおよびデスクトップ割り当ての概要については、Universal Broker 環境でのサイトの操作を参照してください。
接続のアフィニティ	この設定は、特定の地理的サイトをユーザーのデフォルト サイトとして指定します。ユーザーがデスクトップを要求すると、ブローカはデフォルト サイトで利用可能なデスクトップの検索を開始します。デフォルト サイトに使用可能なデスクトップが見つからず、サイトの制限が有効になっていない場合、ブローカはデフォルト サイト以外でデスクトップの検索を続けます。 以下のいずれかのオプションを選択します。 ■ [最も近いサイト] は、最も近い地理的サイトをユーザーのデフォルト サイトとして指定します。 ■ [ホーム サイト] は、ユーザーのホーム サイト（またはユーザーを含むグループのホーム サイト）をそのユーザーのデフォルト サイトとして指定します。 **注：** [ホーム サイト] を選択した場合は、ウィザードの後続の手順で、[ユーザー] ページでの [ホーム サイトの割り当て] 設定が利用可能になります。 ■ ユーザーが構成済みのホーム サイトの外部でもデスクトップにアクセスできるようにするには、[ホーム サイト制限] を有効にしないでください。 ■ デスクトップにアクセスする場合にユーザーを構成済みのホーム サイトに制限するには、[ホーム サイト制限] を有効にします。 **重要：** [ホーム サイト制限] を有効にすると、ユーザー（またはユーザーを含むグループ）は、デスクトップにアクセスする前にホーム サイトを構成する必要があります。

[定義] 設定を構成した後、[次へ] をクリックしてウィザードの次のページに進みます。

4 ウィザードの [デスクトップ] ページで、必要な設定を構成します。

注： 必要に応じてスクロール バーを使用して、すべての設定内容を表示します。

設定	説明
フィルタ	1 つ以上のフィルタを設定して、[モデル] ドロップダウン メニューで使用できるモデルを制御します。モデルは、タイプ、シリーズ、CPU の数、メモリ、およびタグでフィルタできます。モデルの選択の詳細については、Horizon Universal Console でのファームと割り当ての仮想マシン タイプとサイズの管理を参照してください。ここでは、[仮想マシンのタイプとサイズ] ページ（[設定] - [仮想マシンのタイプとサイズ]）のオプションについて説明しています。  フィルタを設定するには、まずドロップダウン メニューで条件を選択し、次に 1 つ以上の目的の値を入力します。デフォルトでは、条件が「タグ」、値が「VMware 推奨」の単一のフィルタがあります。この最初のフィルタを編集し、And および Or 演算子によって接続されたフィルタをさらに追加できます。 次に、フィルタに使用できる基準と、それぞれに入力できる値の説明を示します。 ■ タイプ  このオプションを選択すると、2 番目のドロップダウン メニューには次の使用可能な値のみが表示されます。 ■ GPU と高パフォーマンス - GPU を使用するモデル。 **注：** GPU モデルを選択した場合、表示されるイメージのリストには「GPU を含める」フラグを選択して作成されたイメージのみが含まれるため、GPU モデルを使用してファームまたはプールを作成するにはそのようなイメージが少なくとも 1 つ必要です。GPU 以外のモデルを選択した場合、表示されるイメージのリストには、「GPU を含める」フラグなしで作成されたイメージのみが含まれます。 ■ シリーズ  このオプションを選択すると、2 番目のドロップダウン メニューから一連のモデルを選択できます。リストの一番上にある [フィルタ] テキスト ボックスにテキストを入力してこのリストをフィルタリングすることもできます。 ■ CPU  このオプションを選択すると、CPU 範囲を入力できます。 **重要：** 本番環境では、予期しないエンドユーザー接続の問題を回避するために、2 個以上の CPU を持つ仮想マシン モデルを使用します。 ■ メモリ

設定	説明
	 このオプションを選択すると、メモリ範囲（GB 単位）を入力できます。 ■ タグ  このオプションを選択すると、2 番目のドロップダウン メニューからタグを選択できます。リストの一番上にある [フィルタ] テキスト ボックスにテキストを入力してこのリストをフィルタリングすることもできます。ドロップダウン メニューで使用可能なタグは、ハードコードされたシステム タグと、[仮想マシンのタイプとサイズ] ページ（[設定] - [仮想マシンのタイプとサイズ]）で作成したカスタム タグの両方です。 フィルタごとに次の手順を実行して、追加フィルタを設定できます。 a [+] リンクをクリックします。 b 前のフィルタと作成中の新しいフィルタの間の演算子として And または Or を選択します。 c 新しいフィルタを設定するには、条件を選択して値を入力します。
モデル	デスクトップ インスタンスに使用するモデルを選択します。メニューには、割り当てに参加している選択済みポッドすべてで選択可能なモデルのみが表示されます。 この選択では、デスクトップ インスタンスが作成されるときに使用される基盤となるリソースのセットを、キャパシティ（コンピューティング、ストレージなど）の観点から定義します。 **重要：** 本番環境の場合は、2 個以上の CPU が搭載された仮想マシン モデルを選択します。第 1 世代の Horizon Cloud スケール テストでは、2 個以上の CPU を使用すると、予期しないエンド ユーザー接続の問題を回避す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、このようなモデルはテスト用または事前検証用にのみ使用する必要があります。
ディスク タイプ	利用可能なオプションからサポートされているディスク タイプを選択します。メニューには、割り当てに参加している選択済みポッドすべてで選択可能なディスク タイプ オプションのみが表示されます。 ディスク タイプのオプションは、選択したモデル、および Azure サブスクリプションとリージョンに基づいています。一般的に使用可能なディスク タイプは次のとおりです。 ■ 標準 HDD - デフォルトのディスク タイプ。 ■ 標準 SSD ■ プレミアム SSD - このオプションは、プレミアム I/O をサポートするモデルを選択した場合にのみ表示されます。 必要な場合、割り当てを作成した後に選択内容を編集できます。

設定	説明
ディスク サイズ	この割り当ての仮想マシンの OS ディスク サイズを GB 単位で入力します。 ■ デフォルト値は、基本イメージの OS ディスク サイズ（通常は 128 GB）です。 ■ サイズを編集する場合、入力する値は基本イメージの OS ディスク サイズよりも大きくなければなりません。また、選択したモデルでサポートされる最大サイズ（通常は 1024 GB）を超えることはできません。 ■ この値は、後で編集することもできます。 **重要：** ディスク サイズを編集する場合は、仮想マシンが予期したとおりに作成されるように、追加のアクションを実行する必要があります。詳細については、ファームまたは VDI デスクトップ割り当てのディスク サイズが増加した場合に必要な管理者のアクションを参照してください。
OS システム	割り当てに含める仮想マシンのオペレーティング システムを指定します。 **ヒント:** この選択は、後続の [イメージ] メニューのフィルタとして機能します。ここで選択したオペレーティング システムを備えたイメージのみが、後続の [イメージ] メニューで選択できます。
ドメイン	お使いの環境に登録されている Active Directory ドメインを選択します。
ディスクの暗号化	デスクトップ インスタンスが暗号化されたディスクを持つようにするには、[はい] を選択します。 **重要：** ■ ディスク暗号化が必要な場合は、VDI マルチクラウド割り当てを作成するときにこの選択を行う必要があります。割り当ての作成後にディスクの暗号化を追加することはできません。 ■ NSX Cloud の機能とディスク暗号化の両方を使用するには、イメージにインストールされている NSX エージェントが最新のエージェント バージョンである必要があります。以前のバージョンの NSX エージェントでディスク暗号化を使用することはサポートされていません。
NSX Cloud 管理	割り当てのデスクトップ インスタンスで NSX Cloud の機能を使用するには、[はい] を選択します。Microsoft Azure のデスクトップでの NSX Cloud 機能の使用については、Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッドおよびそのサブトピックを参照してください。 **重要：** ■ デスクトップ インスタンスで NSX Cloud を使用する場合、VDI マルチクラウド割り当ての作成時にこの選択を行う必要があります。NSX Cloud 管理は、割り当て作成後に有効にすることはできません。 ■ 割り当てのデスクトップ インスタンスで NSX Cloud 管理機能を使用するには、この割り当て用に選択したイメージに NSX エージェントがインストールされている必要があります。この設定を [はい] に切り替えるときは、[イメージ] で選択したイメージに NSX Agent がインストールされている必要があります。システムは、割り当てを作成するときに、選択したイメージに NSX エージェントがあるかどうかを検証しません。 ■ NSX Cloud の機能とディスク暗号化の両方を使用するには、イメージにインストールされている NSX エージェントが最新のエージェント バージョンである必要があります。以前のバージョンの NSX エージェントでディスク暗号化を使用することはサポートされていません。

設定	説明
イメージ	エンド ユーザーに割り当てる各ポッドのイメージを選択します。選択したイメージに関する情報を表示するには、[詳細] をクリックします。 ここには、[OS システム] の選択に対応する各ポッド内の公開イメージのみが表示されます。公開イメージは、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も呼ばれ、ゴールド イメージをデスクトップに変換してシステムに公開したものです。 **注：** イメージを選択しようとすると「有効なイメージを選択して続行してください」というエラー メッセージが表示された場合は、イメージに問題がある可能性があります。[インベントリ] - [イメージ] の順に移動して、問題のイメージのステータスを表示し、提案されている修正処置を実行します。 割り当てに参加しているポッドごとに異なったイメージを選択できるため、Universal Broker が割り当てからリソースを仲介する方法に基づいて、エンド ユーザーが受け取るセッション エクスペリエンスが異なる場合があります。たとえば、あるユーザーは、特定のイメージを使用するポッド A からデスクトップを受信することがあります。ただし、ポッド B からデスクトップを受信する別のユーザーは、ポッド B によって使用されるデスクトップ イメージに基づいて、セッション エクスペリエンスが異なる場合があります。 **重要：** ■ [ディスクを暗号化] を [はい] に設定する場合、ここで選択したイメージにデータ ディスクが接続されていないことを確認してください。フローティング VDI 割り当てにデータ ディスクを使用した仮想マシンのディスク暗号化の使用は、このリリースではサポートされていません。 ■ [NSX Cloud 管理] を [はい] に設定する場合は、ここで選択したイメージに NSX Agent がインストールされていることを確認します。割り当てのデスクトップ インスタンスで NSX Cloud 管理機能を使用するには、この割り当て用に選択したイメージに NSX エージェントがインストールされている必要があります。システムは、VDI デスクトップ割り当てを作成するときに、選択したイメージに NSX エージェントがあるかどうかを検証しません。
仮想マシン名のプリフィックス	この割り当てで作成されたデスクトップ仮想マシンの基底名。仮想マシン名はこの基底名に数値を加えたもの、たとえば、win10-1、win10-2 になります。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。この名前は、エンド ユーザーがこの割り当てからデスクトップにアクセスするときに表示されます。たとえば、エンド ユーザーが Horizon Client を実行してデスクトップの 1 つを使用すると、この名前は Horizon Client に表示されます。
既定のプロトコル	エンド ユーザー セッションで使用するデフォルトの表示プロトコルを選択します。 デフォルトのプロトコルではなく、別のプロトコルが使用される状況が発生する場合があります。たとえば、クライアント デバイスがデフォルトのプロトコルをサポートしない場合や、エンド ユーザーが、選択されているデフォルト プロトコルよりも他のプロトコルを優先して使用する場合があります。 **注：** Microsoft Windows 7 Enterprise オペレーティング システムのイメージの場合、サポートされている選択肢は RDP のみです。
優先クライアント	エンド ユーザーが Workspace™ ONE™ プラットフォームのポータルからデスクトップを起動するときに使用する優先クライアントを選択します。これは Horizon Client、または HTML Access 用のブラウザのいずれかになります。 **注：** Microsoft Windows 7 Enterprise オペレーティング システムのイメージの場合、サポートされている選択肢は Horizon Client のみです。

設定	説明
Windows クライアント ライセンスを持っていますか:	このウィザードでは、イメージ内にあり、デスクトップ仮想マシンに入ることになる Microsoft Windows オペレーティング システムを使用するための適格なライセンスがあることを確認するよう求められます。画面に表示される指示に従います。 クライアント オペレーティング システムの場合、Horizon Cloud はデフォルトで Windows クライアント ライセンス タイプを使用するよう割り当てのデスクトップ仮想マシンを設定します。この設定は変更できません。
パワーオフ保護時間	パワーオンしているデスクトップをシステムが自動的にパワーオフするまでの待機時間（分）を指定します。1 から 60 の値を入力できます。デフォルトは 30 分です。 この保護時間は主として、システムが自動的にデスクトップ仮想マシンをパワーオフする状況で使用されます。この [パワーオフ保護時間] を使用して、[電源管理] フィールドのしきい値設定を満たすように、仮想マシンのパワーオフを開始する前にシステムが指定した時間の間待機するように設定できます。システムは、[パワーオフ保護時間] に指定した時間の間待機した後に、構成されたスケジュールどおりに仮想マシンをパワーオフします。デフォルトの待機時間は 30 分です。

オプションで、詳細プロパティを構成します。

オプション	説明
コンピュータの OU	デスクトップ仮想マシンが配置される Active Directory 組織単位。識別名（たとえば、`OU=RootOrgName,DC=DomainComponent,DC=eng` など）を使用して Active Directory 組織単位を入力します。OU およびネストされた OU 内の各パスには、文字、数字、特殊文字、および空白の任意の組み合わせを含めることができ、最大で 64 文字にすることができます。 ネストされた組織単位を使用する必要がある場合は、ネストされた Active Directory ドメイン組織単位の使用についての考慮事項を参照してください。 **注：** [コンピュータの OU] が `CN=Computers` に設定されている場合、システムは、仮想マシンのデフォルトの Active Directory `Computers` コンテナを使用します。Active Directory には、組織単位クラスのコンテナにリダイレクトされるデフォルトのコンテナがあります。
1 回実行スクリプト	（オプション）仮想マシンの作成プロセスの後に、割り当てのデスクトップ仮想マシンで実行するスクリプトの場所。 **注：** スクリプトは、仮想マシンを再起動するための再起動ステップで終了する必要があります。そうしないと、エンド ユーザーは手動で再起動を実行するまで、デスクトップにログインすることができません。再起動のための Windows コマンド ラインを以下に示します。 `shutdown /r /t 0` スクリプトが再起動ステップで終了する必要がある理由は、sysprep プロセス後にスクリプトが実行されるときのシーケンスのためです。システムが割り当てのデスクトップ仮想マシンを作成すると、仮想マシンが起動し、Windows オペレーティング システムの `sysprep` プロセスを完了します。`sysprep` プロセスが完了したら、デスクトップ仮想マシンのエージェントがドメイン参加を行おうとします。同時に、エージェントはここで指定するスクリプト パスを取得します。エージェントは `Windows RunOnce` パス (`System run once`) を設定し、デスクトップ仮想マシンを再起動します。次の再起動時に、システムはローカル管理者アカウントを使用して Windows オペレーティング システムにログインし、スクリプトを実行します。デスクトップ仮想マシンが、ユーザーのログインに対応できるようになるのは、スクリプトに指定されているように、次回以降の再起動後になります。

オプション	説明
切断済みセッションのログオフ	切断されたデスクトップ セッションからシステムがユーザーをログアウトするタイミングを指定します。 **注：** [切断済みセッションのログオフ]、[セッションのタイムアウト間隔]、[セッションの最大有効期間] の設定によって管理されるセッションは、デスクトップの Windows オペレーティング システムへのユーザー ログインです。これらのセッションは、Horizon Client、Horizon HTML Access、または Workspace ONE のユーザー ログインではありません。 ユーザーのセッションは、ユーザーがデスクトップの Windows オペレーティング システムに対して認証されると開始します。
セッション タイムアウトの間隔	この間隔は、システムがデスクトップから強制的にログアウトする前に、エンド ユーザーのセッションがアイドル状態を保持する時間です。このタイムアウトは、基盤となる Windows オペレーティング システムへのログイン セッションに適用されます。ここで指定する時間は、エンド ユーザーの Horizon Client または HTML Access ログイン セッションを制御するタイムアウト設定とは別のものです。 **注意：** 基盤となる Windows オペレーティング システムのセッションでシステムが強制的にログオフすると、保存されていないデータは失われます。データが意図せずに失われるのを防ぐには、エンド ユーザーのビジネス ニーズに応じてこの間隔の値を十分に大きくします。 デフォルトの間隔は 1 週間（10080 分）です。 **注：** タイムアウトの間隔に達する前にユーザー アクティビティが発生しない場合、30 秒以内に [OK] をクリックしないとログオフされることを示すメッセージがデスクトップに表示されます。ログアウトが発生すると、ドキュメントやファイルなど、保存されていないユーザー データは失われます。
セッションの最大有効期間	システムが単一のユーザー セッションに対して許可する最大分数を指定します。

オプション	説明
電源管理モード	**注：** この設定は、デスクトップ タイプを [フローティング] に設定している場合にのみ使用できます。 電源管理設定は、使用率に応じてフローティング VDI デスクトップ割り当てのパワーオン状態のデスクトップ インスタンスの数を自動的に増やしたり減らしたりする際のしきい値に関連します。使用率が増えて上限を超えると、システムは自動的に新しいデスクトップ インスタンスを起動します。使用率が下限を下回ると、システムは、エンド ユーザーがデスクトップからログアウトすると、デスクトップ仮想マシンをシャットダウンし、その割り当てを解除します。 電源管理の選択は、キャパシティのコストと迅速な可用性のバランスを取ります。 ■ 後からではなく、すぐに次のデスクトップ インスタンスをパワーオンする場合は、[パフォーマンスを優先して最適化] を選択します。ユーザーが要求するよりも早く次のデスクトップを準備することで電源の消費は増えますが、ユーザーが割り当てからデスクトップを起動しようとするときにはすでにデスクトップは起動しているので、そのようなユーザーの要求を満たすのに有効です。 ■ 次のデスクトップ インスタンスをパワーオンする時間をできるだけ遅らせる場合は、[電源を優先して最適化] を選択します。割り当てのデスクトップ セットの占有率は、システムが次のデスクトップ インスタンスを起動する前に高くなります。既存のデスクトップの使用率を高めることでキャパシティのコストは最小限に抑えられますが、この設定では新規ユーザーがログインするときに遅延が発生する可能性が高くなります。これは、システムがデスクトップをパワーオンするまで待機が必要な場合があるためです。 ■ キャパシティのコストとユーザーに対する可用性までの時間のバランスを取るには [バランシング済み] を選択します。 各選択のしきい値の上限と下限は次のとおりです。 ■ [パフォーマンスを優先して最適化] 　■ 低いしきい値：23% 　■ 高いしきい値：50% ■ [電源を優先して最適化] 　■ 低いしきい値：38% 　■ 高いしきい値：80% ■ [バランシング済み] 　■ 低いしきい値：31% 　■ 高いしきい値：66%
Azure リソース タグ	(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。 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、[追加] 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。 ■ 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。 　< > % & \ ? / ■ 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。

オプション	説明
	割り当てが作成されると、Azure リソース タグを追加したり、その割り当てのタグを編集または削除できます。

[デスクトップ] 設定を指定した後、[次へ] をクリックしてウィザードの次のページに進みます。

5 ウィザードの [キャパシティ] ページで、以下の設定を行います。

a 専用 VDI デスクトップ割り当てを作成する場合は、[すべてのポッドのグローバル構成] をクリックし、割り当てに参加しているすべてのポッドに適用する設定を構成できます。

注：

- ここで行った設定は、次の手順でポッドごとの設定を指定するときに、特定のポッドに対して上書きできます。
- これらの設定は、2474.0 より前のマニフェスト バージョンのポッドには適用されません。割り当てに 2474.0 より前のマニフェストを持つポッドが使用されている場合、これらの設定がそれらのポッドにあるデスクトップ仮想マシンでは有効にならないことを示すメッセージが表示されます。

オプション	説明
最大デスクトップ削除	これは、[設定] - [全般設定] ページの [削除保護] で設定したレートに対してカウントされる前に、割り当て内で削除できるデスクトップ仮想マシンの数を設定します。ドロップダウン メニューから次のオプションを 1 つ選択します。 ■ [無制限]:無制限の数のデスクトップ仮想マシンを割り当てから削除できます。この場合、[削除保護] の設定は関係なくなります。 ■ [なし] : [削除保護] で設定したレートに対してカウントされる前に、追加で削除できるデスクトップ仮想マシンはありません。この場合、システムは [削除保護] のみを使用して削除を許可またはブロックします。[なし] は [削除保護] のデフォルト値です。 ■ [カスタム] : [削除保護] で設定したレートに対してカウントされる前に、追加で削除できるデスクトップ仮想マシンの数。[カスタム] を選択した場合は、[カスタム削除数] の数値も入力する必要があります。 たとえば、[最大デスクトップ削除] を 10、[削除保護] を 1 に設定するとします。この場合、最初の 10 台の仮想マシンが削除された後 （数が 10 になるまでの時間に関係なく）、システムはそれ以降、1 時間あたり 1 台の追加の仮想マシンのみを削除できます。 **重要：** 専用デスクトップ割り当てに新しいイメージを指定すると、システムでは必要に応じて [最大デスクトップ削除] の設定を変更して、未割り当てのデスクトップ仮想マシンをすべて新しいイメージで再構築できるようにします。 **注：** [削除保護] で [無制限] を選択した場合、[最大デスクトップ削除数] 設定を使用する必要はありません。 [削除保護] 設定の詳細については、Horizon Cloud テナント環境のカスタマイズ可能な全般設定を参照してください。

オプション	説明
	専用デスクトップ割り当て内のすべての仮想マシンの削除を防止するには、[割り当て] ページの [削除の防止] 設定を使用します。マルチクラウド専用デスクトップ割り当ての削除の防止または削除の許可を参照してください。
カスタム削除の数	[デスクトップの最大削除] の [カスタム] を選択した場合は、削除できる追加のデスクトップ仮想マシンの数を入力してから、[削除保護] に設定したレートに対してカウントします。入力する数値は `1` と `2000` の間にする必要があります。

b ポッド リストのポッドの横にある矢印アイコンをクリックして、参加している各ポッドに必要な設定を構成します。

オプション	説明
電源管理スケジュールの追加	Microsoft Azure でデスクトップ仮想マシンの省電力とパフォーマンスを最適化するため、パワーオン状態のデスクトップ インスタンスの最小数を週単位で繰り返し調整するスケジュールを設定するオプションがあります。 **注：** [フローティング] の割り当てでは、電源管理スケジュールを使用して任意のデスクトップ インスタンスを管理できます。[専用] の割り当てでは、スケジュールを使用して未割り当てのデスクトップ インスタンスのみを管理できます。 次に例を示します。 ■ エンド ユーザーが週末や夜間の時間帯にデスクトップを使用していないことを把握していれば、パワーオン状態のデスクトップ（[フローティング] の割り当ての場合）またはパワーオン状態の未割り当てのデスクトップ（[専用] の割り当ての場合）の数をゼロまたは少数にスケジュール設定できます。 ■ エンド ユーザーの需要が増大することが予測できる特定の日や特定の時間幅に対しては、その需要を満たすには利用可能になるパワーオン状態のデスクトップの最小数が増加するスケジュールを設定できます。 割り当てに対して最大 10 個のスケジュールを指定できます。期間が重複しているのに、デスクトップの最小数の指定値が異なっているスケジュールがある場合は、システムはその重複する期間において大きい値の方のデスクトップの最小数を使用します。 1 [デスクトップの最小数] 列の下にあるカレンダー アイコンをクリックして、そのポッドの [電源管理スケジュールの追加] 画面を開きます。 2 1 番目のスケジュールの日数を選択します。 3 指定された日数の該当する時間を指定します。次のいずれかを行います。 ■ 指定した日数のすべての時間帯でこのスケジュールを有効にするには、[全日] チェック ボックスを選択します。 ■ それぞれの日に期間の開始時間と終了時間を指定します。 **注：** 暗号化された仮想マシンは、暗号化されていない仮想マシンよりもパワーオンに時間がかかります。[ディスクの暗号化] を [はい] に設定し、暗号化された仮想マシンのエンド ユーザー接続が、一日のうちの特定の時間帯に 100% 利用できるように設定したい場合、起動時間をその時間よりも早く設定する必要があります。暗号化された仮想マシンが多数ある場合のファームと VDI デスクトップの割り当ての電源管理のスケジューリングを参照してください。 4 タイムゾーンを選択します。エンド ユーザーの場所に最も近いタイムゾーンが推奨されます。選択されたタイムゾーンに適した夏時間が自動的に適用されます。

オプション	説明
	注： 2 つのスケジュールで同じタイム ゾーン設定が使用されていて、時間の重複がある場合、警告が表示されます。ただし、2 つのスケジュールのタイム ゾーン設定が異なっていて、重複がある場合は、この警告は表示されません。例として、全日土曜日のスケジュールが 2 つ設定されていて、1 つが [ヨーロッパ/ロンドン] タイム ゾーンを選択していてもう 1 つが [アメリカ/トロント] を選択している場合、重複についての警告は表示されません。 5 [デスクトップの最小数] フィールドに、指定した期間内にパワーオンするデスクトップの最小数を入力します。指定された期間内に、その最小数のデスクトップがパワーオンされ、その期間内でエンド ユーザーの要求に対応できます。 ■ [フローティング] の割り当てでは、この数はゼロ (0) から、ポッドの [デスクトップの最大数] に指定されている数までの範囲で指定できます。 ■ [専用] の割り当てでは、この数はゼロ (0) から、ポッドの未割り当てのデスクトップ インスタンスの合計数までの範囲で指定できます。 この数値がゼロ (0) で、スケジュールの開始時点でアクティブなエンド ユーザー セッションがない場合は、ポッドのデスクトップがパワーオフされます。このシナリオでは、その後エンド ユーザーがスケジュールされた期間内にこの割り当てからデスクトップに接続しようとすると、デスクトップが使用可能な状態になるまで遅延が発生します。これは、基盤となるデスクトップ仮想マシンをパワーオンする必要があるためです。 6 追加の電源管理スケジュールを作成するには、[スケジュールの追加] をクリックします。 **注：** デフォルトでは、ユーザーがスケジュールの時間外にあるときにデスクトップからログアウトすると、システムは [パワーオフ保護時間] フィールドに指定した時間、その仮想マシンがパワーオフすることを防止します。デフォルトは 30 分です。
フローティング VDI 割り当てを作成する場合 **仮想マシンの最小数** **仮想マシンの最大数**	この割り当てに選択したポッドに含めるデスクトップの最小数と最大数を指定します。割り当てが最初に作成されると、システムでは [仮想マシンの最大数] 設定で指定された数のデスクトップ仮想マシンをポッドにデプロイし、次に [仮想マシンの最小数] で指定された数を超えた分のデスクトップ仮想マシンをパワーオフします。 最小数のデスクトップ インスタンスのみが最初にパワーオンされます。エンド ユーザーの要求が増加すると、システムは [仮想マシンの最大数] の設定を上限として追加のデスクトップをパワーオンします。その後、エンド ユーザーの要求が減少すると、システムは [仮想マシンの最小数] の設定を下限としてデスクトップをパワーオフします。システムによってデスクトップがパワーオフされる前に、デスクトップからログイン済みユーザー セッションがなくなっている必要があります。 [仮想マシンの最小数] にゼロ (0) を指定すると、デスクトップに対するエンド ユーザーからの要求が発生するまで、システムは割り当てのすべてのデスクトップをパワーオフすることになります。 **重要：** [仮想マシン サブネットの指定] で指定するサブネットは、[仮想マシンの最大数] の値と一致するために必要な IP アドレスの数に対応している必要があります。
専用 VDI 割り当てを作成する場合 **仮想マシンの最小数** **仮想マシンの最大数**	**ヒント:** 専用 VDI デスクトップ割り当てに対するこの [仮想マシンの最小数] 設定は、フローティング VDI デスクトップ割り当ての設定とは少し異なります。専用 VDI デスクトップ割り当ての場合、[仮想マシンの最小数] の設定は、未割り当てのデスクトップを表します。デスクトップがユーザーに割り当てられると、そのデスクトップ仮想マシンは未割り当てのデスクトップではなくなり、その結果、[仮想マシンの最小数] の設定によって管理されるデスクトップのセットの一部とは見なされません。割り当て内の未割り当てのデスクトップ仮想マシンの数が [仮想マシンの最小数] の値よりも小さい場合、パワーオン状態の仮想マシンの数が [仮想マシンの最小数] の値未満であることがわかります。

オプション	説明
	■ [仮想マシンの最小数] - この割り当てによって選択されたポッドで作成されるプールに含める、パワーオンされた未割り当てのデスクトップ仮想マシンの数を設定します。割り当てが最初に作成されるとき、選択されたポッドから割り当て可能な最大数の合計（[仮想マシンの最大数] の数で設定）のうちゼロのデスクトップ仮想マシンが割り当てられます。したがって、その時点では、ここで設定する数は、可能な最大数のうち、最初にパワーオンする未割り当ての仮想マシンの数のサブセットです。[仮想マシンの最小数] にゼロ (0) を指定した場合は、割り当てが最初に作成されるときに未割り当てのデスクトップ仮想マシンをパワーオンしないことを示します。 一部の未割り当ての仮想マシンをパワーオンするように設定することのメリットは、主に、ユーザーがすぐにログインできるように未割り当ての仮想マシンを用意しておくことです。時間の経過とともに、これらのパワーオン状態で未割り当てのデスクトップが、デスクトップを要求する初回のログインを行うユーザーから、または [割り当て] アクションを使用してデスクトップをユーザーに明示的に割り当てる管理者からユーザーに割り当てられると、システムはこのポッドおよびこの割り当てに参加している他のポッド内の追加の未割り当てのデスクトップをパワーオンします。システムがポッドに指定された [仮想マシンの最大数] の値に達すると、システムは、この割り当てのためのポッドのプール内にある未割り当てのデスクトップのパワーオンを停止します。最後に、指定したポッド内のすべてのデスクトップ仮想マシンがユーザーに割り当てられている場合、[仮想マシンの最小数] の値は、ユーザーからのデスクトップの割り当て解除を明示的に開始するまであまり使用されません。 ■ [仮想マシンの最大数] - この割り当てによって定義されたポッドの仮想マシン プールに必要なデスクトップ仮想マシンの総数を設定します。 **重要：** [仮想マシン サブネットの指定] で指定するサブネットは、[仮想マシンの最大数] の値と一致するために必要な IP アドレスの数に対応している必要があります。
仮想マシンの静止	この設定は、割り当てを編集して選択したポッドに指定されているイメージを変更するユースケースで機能します。デスクトップ仮想マシンでの動作は、フローティング VDI デスクトップ割り当ての場合と専用 VDI デスクトップ割り当ての場合でわずかに異なります。 **フローティング VDI デスクトップ割り当ての場合** この設定は、ポッドの選択されたイメージの更新中に同時に静止することができる、選択したポッドにある割り当てのパワーオンされたデスクトップ仮想マシンの数を制御します。たとえば、この割り当てを後で編集して、選択したポッドから別のイメージを使用すると、システムは、セッションのない仮想マシンに対し、パワーオン状態のデスクトップ仮想マシンを同時にこの数だけパワーオフします。（パワーオン状態のデスクトップにセッションがある場合、システムはセッションが終了するまで、そのデスクトップをパワーオフしません）。次に、パワーオフ状態のデスクトップ仮想マシンのセットに対して、システムは新しいイメージをそのセットにプロビジョニングするために必要なアクションを実行します。一般的なユースケースでは、この数は、選択したポッドに対して定義されているデスクトップ仮想マシンの最大数のサブセットに設定されます。ただし、必要に応じて、ここでは [仮想マシンの最大数] の設定に等しい数を指定できます。そのシナリオでは、ポッド内のデスクトップ仮想マシンに新しいイメージを使用するように割り当てを編集するときに、選択したポッド内の割り当てのすべてのパワーオンされたデスクトップ仮想マシンを同時にパワーオフにすることをシステムに許可します。 **専用 VDI デスクトップ割り当ての場合** この設定は、ポッドの選択されたイメージの更新中に同時に静止することができる、選択したポッドにある割り当ての未割り当てのデスクトップの数を制御します。たとえば、この割り当てを後で編集して、選択したポッドから別のイメージを使用すると、システムは、未割り当てのデスクトップ仮想マシンを同時にこの数だけパワーオフします。次に、パワーオフ状態の未割り当てのデスクトップ仮想マシンのセットに対して、

オプション	説明
	システムは新しいイメージをそのセットにプロビジョニングするために必要なアクションを実行します。一般的なユースケースでは、この数は、選択したポッドに対して定義されているデスクトップ仮想マシンの最大数のサブセットに設定されます。ただし、必要に応じて、ここでは [仮想マシンの最大数] の設定に等しい数を指定できます。そのシナリオでは、ポッド内のデスクトップ仮想マシンに新しいイメージを使用するように割り当てを編集するときに、選択したポッド内の割り当てのすべてのパワーオンされた未割り当てのデスクトップ仮想マシンを同時にパワーオフにすることをシステムに許可します。 **注：** ■ フローティング VDI デスクトップ割り当てでは、この設定は、パワーオフされたデスクトップ仮想マシンには関係しません。フローティング VDI マルチクラウド割り当てのポッドのイメージが変更されると、システムはすぐにパワーオフ状態のデスクトップ仮想マシンを削除して、新しいイメージに更新します。 ■ 専用 VDI マルチクラウド割り当てでは、ユーザーにマッピングされたデスクトップは、それらのユーザーに割り当てられている、と言います。専用 VDI デスクトップ割り当ての割り当て解除されたデスクトップは、まだ特定のユーザーにマッピングされていないデスクトップです。
最大デスクトップ削除 **カスタム削除の数**	これらのオプションは、専用 VDI デスクトップ割り当ての場合にのみ表示されます。前の手順の表の説明を参照してください。選択したポッドに対するこれらの設定を変更すると、前の手順で行ったグローバル構成の対応する設定が上書きされます。
仮想マシン サブネットの指定	このトグルを有効にすると、選択した参加しているポッド用に構成されている 1 つ以上の特定のサブネットを選択できます。これらのサブネットは、ファーム用および VDI デスクトップ割り当て用 Horizon Cloud ポッドでの複数のテナント サブネットの使用の概要で説明されているように、そのポッドの構成で定義されたサブネットです。割り当てのデスクトップ仮想マシンはこれらのサブネットに接続されます。トグルを有効にしたら、表示される一覧から特定のサブネットを選択できます。 このトグルがオフに切り替えられている場合、割り当てのデスクトップ仮想マシンはデフォルトでポッドのプライマリ仮想マシン サブネットに接続されます。 **重要：** ■ 割り当てに仮想マシン サブネットの使用を指定すると、選択した仮想マシン サブネットは引き続き有効になり、割り当ての作成後に変更することはできません。 ■ 選択したサブネットによって提供される IP アドレスの総数は、指定された [仮想マシンの最大数] の設定以上である必要があります。たとえば、割り当てにプライマリ サブネットを使用するか、複数の仮想マシン サブネットを使用して割り当てに対し 100 の IP アドレスを使用可能にするかを選択する場合、[仮想マシンの最大数] は 100 を超えることはできません。

[キャパシティ] の設定を構成したら、[次へ] をクリックしてウィザードの次のページに進みます。

6 [ユーザー] ページで、割り当ての使用資格を付与するユーザーとユーザー グループを指定します。

オプション	説明
[ドメイン]	ユーザーとグループが常駐する Active Directory ドメインを指定します。 **注：** 選択できるのは、クラウド構成のドメインのみです。
[ユーザーを検索]	ユーザー名またはグループ名の最初の数文字を入力し、表示されるリストからユーザーまたはユーザー グループを選択します。 選択した項目が [選択されたユーザー/ユーザー グループ] リストに追加されます。[削除] ボタンを使用して、リストから選択したユーザーまたはグループを削除できます。
[ホーム サイトの割り当て]	**注：** この設定は、ウィザードの [定義] ページで [接続のアフィニティ] に [ホーム サイト] を選択した場合にのみ使用できます。 このオプションの設定を使用して、この割り当てにアクセスしている選択したユーザーまたはグループのホーム サイトの上書きを構成します。この場合、Universal Broker は、ユーザーまたはグループの構成済みホーム サイトではなく、上書きサイトで使用可能なデスクトップの検索を開始します。 たとえば、あるユーザーがサンフランシスコにホーム サイトを持っていて、その上書きサイトとしてニューヨークを指定したとします。ユーザーが割り当てにアクセスすると、Universal Broker は最初にサンフランシスコではなく、ニューヨークで利用可能なデスクトップを検索します。 ホーム サイトの上書きを指定するには、ユーザーまたはグループを選択し、[ホーム サイトの割り当て] をクリックします。[ホーム サイトの割り当て] メニューには、この割り当てに参加しているポッドで利用可能なすべてのサイトが表示されます。 ■ ユーザーまたはグループの構成済みホーム サイトではなく、デフォルトとして上書きサイトを指定するには、メニューで上書きサイトを選択します。 ■ 上書きサイトを削除して、代わりにユーザーまたはグループの構成済みホーム サイトを使用するには、[ホーム サイトのクリア] を選択します。

[ユーザー] 設定を指定した後、[次へ] をクリックしてウィザードの次のページに進みます。

7 [サマリ] ページで構成を確認してから、[終了] をクリックします。

結果

システムは、指定したポッドでデスクトップ インスタンスを構成するプロセスを開始し、選択したユーザーに VDI デスクトップを提供します。

注： 暗号化されたデスクトップ仮想マシンの作成は、暗号化されていない仮想マシンの作成の約 2 倍の時間がかかります。その結果、ディスクの暗号化が有効になっている VDI デスクトップの割り当てを作成する場合は、無効になっている場合と比べて、開始から完了までの時間が約 2 倍かかります。

次のステップ

特別なポートを開く必要があるアプリケーションがこのフローティング VDI デスクトップ割り当てのイメージにある場合、この割り当てに関連付けられたネットワーク セキュリティ グループ (NSG) を Microsoft Azure で変更する必要があります。NSG の詳細については、Horizon Cloud ポッド内のネットワーク セキュリティ グループと VDI デスクトップについてを参照してください。

この割り当てに NSX Cloud 管理を指定した場合、NSX Cloud 環境の Service Manager (CSM) を使用して、デスクトップ仮想マシンが NSX Cloud で管理されていることを確認できます。ユーザー環境の CSM にログインし、[クラウド] - [Azure] - [インスタンス] の順に移動します。その [インスタンス] ページに、デスクトップ インスタンスの管理対象のステータスが表示されたら、それらに NSX ポリシーの実装を開始できます。

Microsoft Azure の Horizon Cloud ポッド - VDI マルチクラウド割り当ての詳細の表示

[割り当て] ページとその詳細なサブページを使用して、Microsoft Azure の Horizon Cloud ポッドに基づく VDI マルチクラウド割り当てのステータスを監視できます。

[割り当て] ページの情報

メインの [割り当て] ページの次の列は、VDI マルチクラウド割り当てに関する有用な情報を提供します。オプションの列を表示するには、[割り当て] ページの左下にあるカスタマイズ ボタンを使用します。

[情報] 列	説明
[構成]	割り当ての構成を変更する要求の現在の進行状況を示します。構成の変更には、新しい割り当ての作成、または既存の割り当ての編集または削除が含まれる場合があります。変更要求が割り当てに参加しているすべてのポッドに伝播されると、この列に「完了」ステータスが表示されます。
[健全性]	割り当ての準備状況を示します。割り当ての作成中に参加しているポッドからデスクトップがプロビジョニングされる場合など、割り当てに対して構成の変更が発生している間は、この列には「進行中」ステータスが進行中を示す矢印とともに表示されます。 進行中のタスクの詳細を表示するには、このトピックの次のセクションで説明するように、割り当ての名前をクリックして割り当ての詳細ページを開きます。 すべての参加しているポッドですべての構成タスクが完了し、割り当てを使用する準備ができると、この列には緑色のチェックマークが付いた「オンライン」ステータスが表示されます。
[サイト]	この列の上にカーソルを置くと、割り当てに参加しているポッドに関連付けられているすべてのサイトが一覧表示されます。
[ポッド]	この列には、割り当てに参加しているポッドの合計数が表示されます。この列にカーソルを置くと、すべての参加しているポッドのリストが表示されます。
[キャパシティ]	割り当てのキャパシティの合計。整数値で表されます。 この値は、割り当てに関連付けられているすべてのデスクトップ プールによって提供される仮想マシンの最大数の合計として計算されます。 たとえば、割り当てに 4 つのデスクトップ プールが含まれていて、それぞれのデスクトップ プールが最大で 1 台の仮想マシンを提供するとします。合計キャパシティは、次のように計算されます。 (最初のデスクトップ プールの最大仮想マシン数) + (2 番目のデスクトップ プールの最大仮想マシン数) + (3 番目のデスクトップ プールの最大仮想マシン数) + (4 番目のデスクトップ プールの最大仮想マシン数) = 1 + 1 + 1 + 1 = 4
[ユーザー グループ]	このオプションの列は、割り当ての使用資格が付与されているユーザー グループの合計数を示します。
[占有率]	合計キャパシティのうち使用済みまたは割り当て済みの部分。パーセント値で表します。 占有率は、ポッド レベルのグローバル資格（この VDI マルチクラウド割り当てなど）とローカル資格の両方を介してログインしたユーザーに基づきます。 ■ フローティング割り当ての占有率を求めるには、最初に割り当て内のすべてのフローティング デスクトップ プールのログイン ユーザー セッション（接続状態、切断状態、およびアイドル状態のセッションを含む）の数を合計します。次に、ユーザー セッションの合計を合計キャパシティで除算し、小数値を算出します。最後に、小数値に 100 を乗算して占有率を求めます。 ■ 専用割り当ての占有率を求めるには、最初に割り当て内のすべての専用デスクトップ プールから割り当て済みの仮想マシンの数を合計します。合計値を合計キャパシティで除算して小数値を算出し、次に 100 を乗算して占有率を求めます。 たとえば、フローティング割り当てに 4 つのデスクトップ プールが含まれていて、キャパシティの合計が 4 であるとします。現在アクティブなユーザー セッションは 2 つあります。占有率は (2/4)*100 = 50% です。

[割り当ての詳細] ページの情報

割り当ての健全性ステータスに関する詳細情報を表示するには、メインの [割り当て] ページで割り当ての名前をクリックして、[割り当ての詳細] ページを開きます。

[割り当ての詳細] ページの [サマリ] タブで、参加しているポッドの一覧や各ポッドの健全性ステータスを確認できます。

ポッドの健全性ステータスの詳細を表示するには、[システム アクティビティ] タブをクリックし、ドロップダウン メニューからポッドの名前を選択します。[システム アクティビティ] タブには、ポッドで実行されている現在および最近のタスクのリストと、各タスクのステータスが表示されます。リスト内のタスクの説明をクリックすると、タスクのプロセスに関する詳細情報が表示されます。

ポッドの状態に問題がある場合は、[システム アクティビティ] タブに問題の説明が表示されます。この場合、情報を使用して問題の状態をトラブルシューティングし、割り当ての健全性ステータスを「オンライン」に戻すことができます。

ポッドがオフラインになった場合の Universal Broker 環境での割り当てに関する考慮事項

Universal Broker 環境でエンド ユーザーの割り当てを操作している場合、参加しているポッドのいずれかが接続を失ってオフラインになると、割り当て内のリソースの可用性が制限されることがあります。

Universal Broker 環境でエンド ユーザー割り当てを操作する場合、次の状況が発生する場合があります。

フローティング VDI 割り当て

- フローティング VDI 割り当てに複数のポッドからのデスクトップが含まれており、1 つ以上の参加しているポッドがオフラインになると、Universal Broker は、要求が最大キャパシティを超えない限り、ユーザーの要求を満たすために、オフラインのポッドを無視してオンライン ポッドからのデスクトップのみを検索します。
- フローティング VDI 割り当て内の参加しているポッドがオフラインになってからオンラインに戻った場合、エンド ユーザーにはその割り当てに対して複数のポッド間で複数の接続セッションが表示されることがあります。複数のインスタンスは、通常、オフラインになったポッドで確立された以前のセッションと、ユーザーの要求を満たすために別のオンライン ポッドで開始された新しいセッションを表します。ユーザーがいずれかのセッションを選択すると、もう一方のセッションが自動的にログオフされます。

専用 VDI 割り当て

- エンド ユーザーが専用 VDI 割り当てから専用デスクトップを受信し、そのデスクトップを含むポッドがオフラインになった場合、ユーザーはデスクトップへのアクセスを失います。ユーザーは、ポッドがオンラインに復帰したときにのみ、デスクトップへのアクセス権を取り戻します。
- エンド ユーザーが割り当てからまだ専用デスクトップを受信しておらず、1 つ以上の参加しているポッドがオフラインになると、Universal Broker は、要求が最大キャパシティを超えない限り、ユーザーの要求を満たすために、オフラインのポッドを無視してオンライン ポッドからのデスクトップのみを検索します。

RDSH セッションのデスクトップとアプリケーションの割り当て

- RDSH 割り当てに参加しているポッドがオフラインになった場合、Horizon Universal Console の割り当てまたは含まれているセッション デスクトップにアクセスできません。エンド ユーザーは割り当て内のセッション デスクトップを表示できますが、デスクトップとの接続セッションを開こうとしても失敗します。割り当てとセッション デスクトップは、ポッドがオンラインに復帰したときにコンソールで再び使用できるようになり、エンド ユーザーに提供されます。
- 参加しているがオフラインになったポッドからのアプリケーションが RDSH 割り当てに含まれている場合、コンソールからその特定のアプリケーションにアクセスできません。エンド ユーザーはオフライン ポッドからのリモート アプリケーションを表示することができますが、これらのアプリケーションを使用してセッションを開始しようとすると失敗します。オフライン ポッド以外のポッドからの割り当て内のアプリケーションは、コンソールとエンド ユーザーの両方で使用できます。オフライン ポッドからのアプリケーションは、ポッドがオンラインに復帰したときにコンソールで再び使用できるようになり、エンド ユーザーに提供されます。

Horizon Cloud テナント環境でのマルチクラウド割り当ての管理

Horizon Universal Console では、[割り当て] ページに表示される割り当てに対して複数のアクションを実行できます。

注： Horizon Universal Console では、マルチクラウド割り当てに関連付けられているデスクトップ プールを編集するために Horizon Console を使用することが制限されていません。また、Horizon Universal Console はそのデスクトップ プールのデータを Horizon Console のデータと同期しません。したがって、Horizon Universal Console では、時々、一貫性のない情報が表示されることがあります。

たとえば、Horizon Console を使用して割り当てに関連付けられているデスクトップ プールを削除しても、Horizon Universal Console には削除されたデスクトップ プールが割り当ての一部として表示されます。この一貫性の問題を解決するには、[デスクトップ割り当ての編集] ウィザードを使用して割り当てからデスクトップ プールを手動で削除します。

[割り当て] ページで実行できるアクション

ページ レベルでは、リストで選択した割り当てに対して実行できるアクションのアクション ボタンがコンソールに表示されます。

コンソールには、割り当ての関連ポッド タイプに基づいて、選択した割り当てで実行可能なアクションが動的に表示されます。

ポッド タイプに依存しないアクションは次のとおりです。

新規

このボタンをクリックすると、[新しいデスクトップの割り当て] ウィザードが起動し、デスクトップ割り当てを作成する手順が示されます。ウィザードの使用方法については、Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成または Microsoft Azure の Horizon Cloud ポッド - 第 1 世代環境での VDI マルチクラウド割り当ての作成と表示を参照してください。

編集

既存のデスクトップ割り当ての横にあるチェック ボックスをオンにして、このボタンをクリックすると、[デスクトップ割り当ての編集] ウィザードが開始します。このウィザードでは、デスクトップ割り当ての特定の構成オプションを変更できます。ウィザードは、[新しいデスクトップの割り当て] ウィザードと似ています。既存のデスクトップ割り当てでは変更できないオプションの読み取り専用設定があります。

削除

既存のデスクトップ割り当ての横にあるチェック ボックスをオンにして、このボタンをクリックすると、割り当てが削除されます。アクションを確認するよう求めるメッセージが表示されます。デスクトップの割り当てを完全に削除するには、確認メッセージで [削除] をクリックします。詳細については、Horizon Cloud 環境からのマルチクラウド割り当ての削除を参照してください。

割り当てに含まれているデスクトップ プールは、割り当てが削除された後もそのまま残ります。

デスクトップ割り当ての詳細ページの情報とアクション

デスクトップ割り当てでは、割り当ての詳細ページ内で、その割り当てタイプに固有のアクションを実行できます。これらの詳細ページを表示するには、コンソールの割り当てに関連するページでその割り当てを見つけ、名前をクリックします。最初に、[サマリ] ページが表示されます。

[サマリ] ページ

- キャパシティと使用量

[サマリ] ページには、デスクトップ割り当ての現在のキャパシティと使用量に関する情報が表示されます。

使用タイプ	説明
デスクトップ	デスクトップ割り当てのキャパシティの合計。整数値で表されます。 この値は、デスクトップ割り当てに関連付けられているすべてのデスクトップ プールによって提供される仮想マシンの最大数の合計として計算されます。 たとえば、デスクトップ割り当てに 4 つのデスクトップ プールが含まれていて、それぞれのデスクトップ プールが最大で 1 台の仮想マシン (VM) を提供するとします。デスクトップ キャパシティは、次のように計算されます。 (最初のデスクトップ プールの最大仮想マシン数) + (2 番目のデスクトップ プールの最大仮想マシン数) + (3 番目のデスクトップ プールの最大仮想マシン数) + (4 番目のデスクトップ プールの最大仮想マシン数) = 1 + 1 + 1 + 1 = 4
占有率	デスクトップの合計キャパシティのうち使用済みまたは割り当て済みの部分。パーセント値で表します。 占有率は、グローバル資格（Horizon Cloud デスクトップ割り当てなど）とローカル資格の両方を介してログインしたユーザーに基づきます。 ■ フローティング デスクトップ割り当ての占有率を求めるには、最初に割り当て内のすべてのフローティング デスクトップ プールのログイン ユーザー セッション（接続状態、切断状態、およびアイドル状態のセッションを含む）の数を合計します。ログインは、グローバル資格（Horizon Cloud デスクトップ割り当てなど）とローカル資格の両方から開始できます。次に、ユーザー セッションの合計をデスクトップのキャパシティで除算し、小数値を算出します。最後に、小数値に 100 を乗算して占有率を求めます。 ■ 専用デスクトップ割り当ての占有率を求めるには、最初に割り当て内のすべての専用デスクトップ プールから割り当て済みの仮想マシンの数を合計します。合計値をデスクトップのキャパシティで除算して小数値を算出し、次に 100 を乗算して占有率を求めます。 たとえば、フローティング デスクトップ割り当てに 4 つのデスクトップ プールが含まれていて、デスクトップ キャパシティの合計が 4 であるとします。現在有効なユーザー セッションは 2 つあります。占有率は (2/4)*100 = 50% です。
アクティブ ユーザー数	現在ログイン済みで、デスクトップ上のセッションに接続しているユーザーの合計。整数値で表されます。切断されたセッションおよびアイドル状態のセッションはこの数から除外されます。 アクティブ ユーザー数は、グローバル資格（Horizon Cloud デスクトップ割り当てなど）とローカル資格の両方を介してログインおよび接続したユーザーに基づきます。 アクティブ ユーザー数は、割り当て内の各デスクトップの接続セッションの総数を合計して計算されます。 たとえば、デスクトップ割り当てに 4 つのデスクトップ プールが含まれているとします。1 つのデスクトップ プールに対して 1 つの接続ユーザー セッションがあります。残りの 3 つのデスクトップ プールには接続されたユーザー セッションはありません。この場合、アクティブ ユーザー数は 1 です。

- 全般情報、デスクトップ、およびユーザー設定

  [サマリ] ページには割り当ての現在の設定のリストが表示され、[全般情報]、[デスクトップ]、および [ユーザー] のカテゴリに編成されます。

  [サマリ] ページの上部にある [編集] ボタンをクリックして、システムによって変更がサポートされている設定を変更できます。既存の割り当ての一部の構成は変更できません。詳細については、Horizon Cloud テナント環境でのマルチクラウド割り当ての編集を参照してください。

[システム アクティビティ] ページ

[システム アクティビティ] ページには、電源管理スケジュールを満たすようにデスクトップをパワーオフするなどの、システム アクションによるデスクトップ割り当て内のアクティビティが表示されます。

リストでタスクを選択して [タスクをキャンセル] ボタンをクリックすることによって、いくつかのタスクを完了する前にキャンセルすることができます。

- キャンセルするタスクの選択を行う前に、ビューを更新して表示されているタスクのステータスを最新の状態にします。
- タスクが現在、システムによってキャンセルできる状態になっている場合、そのキャンセル可能なタスクに対応しているチェック ボックスを選択できます。
- 指定されたポッドでは、一度に最大 100 個のタスクをキャンセルできます。

この表はキャンセルできるタスクを示しています。

タスク	タスクがキュー状態にあるときにキャンセル	タスクが実行状態にあるときにキャンセル
ファームの拡張	サポートされています 次の点に注意してください。 ■ システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。 ■ この機能は、マニフェスト バージョン 2474.x 以降を実行する Horizon Cloud ポッドでサポートされています。	サポートされています 次の点に注意してください。 ■ システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。 ■ 仮想マシンや OS/データ ディスクなど、すでに作成されているリソースは、タスクがキャンセルされると破棄されます。仮想マシンが破棄された場合または作成されていない場合、割り当てのサイズは変わります。 ■ この機能は、マニフェスト バージョン 2474.x 以降を実行する Horizon Cloud ポッドでサポートされています。
割り当ての拡張	サポートされています 次の点に注意してください。 ■ システムによって、VDI デスクトップ割り当ての拡張タスクが自動的に作成され、割り当ての作成または更新が進行中である場合は、タスクをキャンセルできます。割り当ての作成または更新の操作が完了した後、キャンセル可能な状態のタスクはありません。 ■ この機能は、マニフェスト バージョン 2474.x 以降を実行する Horizon Cloud ポッドでサポートされています。	サポートされています 次の点に注意してください。 ■ システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。 ■ 仮想マシンや OS/データ ディスクなど、すでに作成されているリソースは、タスクがキャンセルされると破棄されます。仮想マシンが破棄された場合または作成されていない場合、割り当てのサイズは変わります。 ■ この機能は、マニフェスト バージョン 2474.x 以降を実行する Horizon Cloud ポッドでサポートされています。
仮想マシンのイメージへの変換	サポートされています **注：** このタスクをキャンセルして再試行する場合は、まず仮想マシンが変換可能な状態であることを確認します。不明な場合は、仮想マシンをパワーオフしてからパワーオンします。	サポートされています **注：** このタスクをキャンセルして再試行する場合は、まず仮想マシンが変換可能な状態であることを確認します。不明な場合は、仮想マシンをパワーオフしてからパワーオンします。

[ユーザー アクティビティ] ページ

[ユーザー アクティビティ] ページには、割り当てによって提供されるセッションのログインやログオフなど、ユーザー アクションによって発生する VDI デスクトップ割り当て内のアクティビティが表示されます。

[レポートのエクスポート] 機能で、表示されている情報をレポート ファイルとしてエクスポートできます。

レポートをエクスポートすると、[レポート] ページの [エクスポートされたレポート] タブに表示されます。ここから、レポートをダウンロードできます。詳細については、第 1 世代テナント - 第 1 世代 Horizon Universal Console の [レポート] ページを参照してください。

エクスポートを開始するときに、すべてのデータをエクスポートするか、現在フィルタされているデータのみをエクスポートするかを選択できます。次に、レポートが生成中であることを示すメッセージがページの最上部に表示されます。[レポート] ページの [エクスポートされたレポート] タブで、レポートの進行状況を確認したり、エクスポートが完了したレポートをダウンロードできます。この準備はレコードの数に応じて数分間かかります。たとえば、50,000 レコードのレポートには、約 10 分かかります。

アクティビティ関連レポートのエクスポート

割り当てのアクティビティ関連ページの [レポートのエクスポート] ボタンは、コンソールの [監視] - [アクティビティ] ページの [レポートのエクスポート] ボタンと同じように機能します。

コンソールの [レポートのエクスポート] ボタンの使用方法については、[アクティビティ] ページのタブからのレポートのエクスポートを参照してください。

Horizon Cloud テナント環境でのマルチクラウド割り当ての編集

Horizon Universal Console の [編集] アクションを使用して、既存のマルチクラウド割り当ての構成を変更できます。

手順

1 コンソールの左ペインで、[割り当て] をクリックします。Horizon ポッド（Horizon Connection Server テクノロジー ベース）からプロビジョニングされた割り当てを編集するには、[割り当て] メニューから [オンプレミスと VMware Cloud] を選択します。

2 [割り当て] ページで、既存の割り当ての横にあるチェック ボックスをオンにして、[編集] をクリックします。

[デスクトップ割り当ての編集] ウィザードが表示されます。このウィザードは、[新しいデスクトップの割り当て] ウィザードと似ています。既存のデスクトップ割り当てでは変更できないオプションの読み取り専用設定があります。

3 必要に応じて、ウィザードの指示に従って割り当ての構成設定を変更します。

ウィザードの使用方法については、Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成を参照してください。

注： 既存の割り当ての一部の構成は変更できません。たとえば、デスクトップ タイプを [フローティング] から [専用] に変更することはできません。代わりに、新しい割り当てを作成し、作成時にデスクトップ タイプを指定する必要があります。

Horizon Cloud 環境からのマルチクラウド割り当ての削除

[割り当て] ページから割り当てを完全に削除できます。

割り当てを削除すると、割り当てを受け取ったユーザーはその割り当てにアクセスできなくなります。ただし、割り当てに含まれているデスクトップ プールはそのまま残ります。

手順

1 Horizon Universal Console の左ペインで、[割り当て] をクリックします。Horizon ポッド（Horizon Connection Server テクノロジー ベース）からプロビジョニングされた割り当てを削除するには、[割り当て] メニューから [オンプレミスと VMware Cloud] を選択します。

2 [割り当て] ページで、既存の割り当ての横にあるチェック ボックスをオンにして、[削除] をクリックします。

3 アクションの確認を求めるメッセージが表示されたら、[削除] をクリックします。

注： 割り当ての削除はすぐには行われず、完了するまでに時間がかかることがあります。

マルチクラウド専用デスクトップ割り当ての削除の防止または削除の許可

[割り当て] ページの設定を使用して、専用デスクトップ割り当てでの仮想マシンの削除を防止したり、削除を許可したりできます。

[削除を防止] オプションを選択すると、システムは専用デスクトップ割り当てからデスクトップ仮想マシンを削除する要求をすべて拒否します。次のオプションを使用しても、仮想マシンの削除に制限を設定できます。

- [削除保護]：詳細については、Horizon Cloud テナント環境のカスタマイズ可能な全般設定を参照してください。
- [最大デスクトップ削除]：このオプションは専用デスクトップ割り当てを作成または編集するときに設定します。オプションの詳細については、Microsoft Azure の Horizon Cloud ポッド - 第 1 世代環境での VDI マルチクラウド割り当ての作成と表示を参照してください。

重要： 削除防止が有効になっている専用デスクトップ割り当てに新しいイメージを指定すると、システムは削除防止を無効にして削除設定を変更し、未割り当てのデスクトップ仮想マシンをすべて新しいイメージで再構築できるようにします。

削除を防止

1 [割り当て] ページで、割り当てのチェックボックスをオンにします。

その割り当てのオプションが有効になります。

2 [詳細] - [削除を防止] をクリックします。

割り当ての削除を防止することを確認するダイアログ ボックスが表示されます。

3 [続行] をクリックします。

操作が正常に実行されたことを示すメッセージが表示されます。

削除を許可

1 [割り当て] ページで、割り当てのチェックボックスをオンにします。

その割り当てのオプションが有効になります。

2 [詳細] - [削除を許可] をクリックします。

割り当ての削除を許可することを確認するダイアログ ボックスが表示されます。

3 [続行] をクリックします。

操作が正常に実行されたことを示すメッセージが表示されます。

ユーザーの Horizon Cloud on Microsoft Azure 環境

6

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 とペアリングさせる必要があります。Horizon Universal Console を使用して、そのサブスクリプションで環境を立ち上げ、ゴールド イメージを作成します。これらのイメージから、任意のデバイスから安全にアクセスできるように、リモート アプリケーションと単一セッションおよびマルチセッションのデスクトップをエンド ユーザーにプロビジョニングします。

環境では、Horizon Cloud ポッドと呼ばれるものを作成します。リモート アプリケーションと単一セッションおよびマルチセッションのデスクトップは、Microsoft Azure サブスクリプションのキャパシティを使用して、そのポッドからプロビジョニングされます。デプロイされたポッドの場所に応じて、デスクトップとアプリケーションを常駐させる場所を選択します。

Horizon Cloud の概要については、サービスの概要を参照してください。最初の Horizon Cloud ポッド デプロイのアクティビティの推奨ワークフローについては、Horizon Cloud ポッド - 最初のポッドのオンボーディング - ワークフローの概要を参照してください。

デプロイされた Horizon Cloud ポッド

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。

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。

Microsoft Azure 環境で Horizon Cloud が作成したリソース グループの名前には、`vmw-hcs` というプリフィックスが付きます。

注意： 次の場合を除き、Microsoft Azure ポータルを使用してポッド関連のリソースを手動で変更または削除しないでください。

- ゴールド イメージの手動作成。
- 必要に応じて、自分のビジネス環境用にポートを構成するためのファームおよび VDI デスクトップ割り当てネットワークのセキュリティ グループの変更。

Horizon Cloud は、ポッドが確実に設計どおりに動作するようにポッド関連のリソースを自動的に構成します。割り当てられた IP アドレスまたは名前など、ワークフロー実行中に Horizon Cloud が自動的に作成およびデプロイするリソースの設定を手動で変更しないでください。仮想マシン インスタンスを手動でパワーオフしたり、Microsoft Azure ポータルを使用して直接削除したりしないでください。マネージャ仮想マシン、または Unified Access Gateway 仮想マシンを手動で削除しないでください。リソース グループ（特に Unified Access Gateway リソース グループ）から NIC を手動で削除しないでください。生成された設定を変更するか、仮想マシンを手動でパワーオフするか、ポッド デプロイヤによって作成された仮想マシンまたは NIC を手動で削除すると、予測できない結果が発生し、ポッドの操作、ポッドの更新、およびポッドの削除操作が失敗する可能性があります。

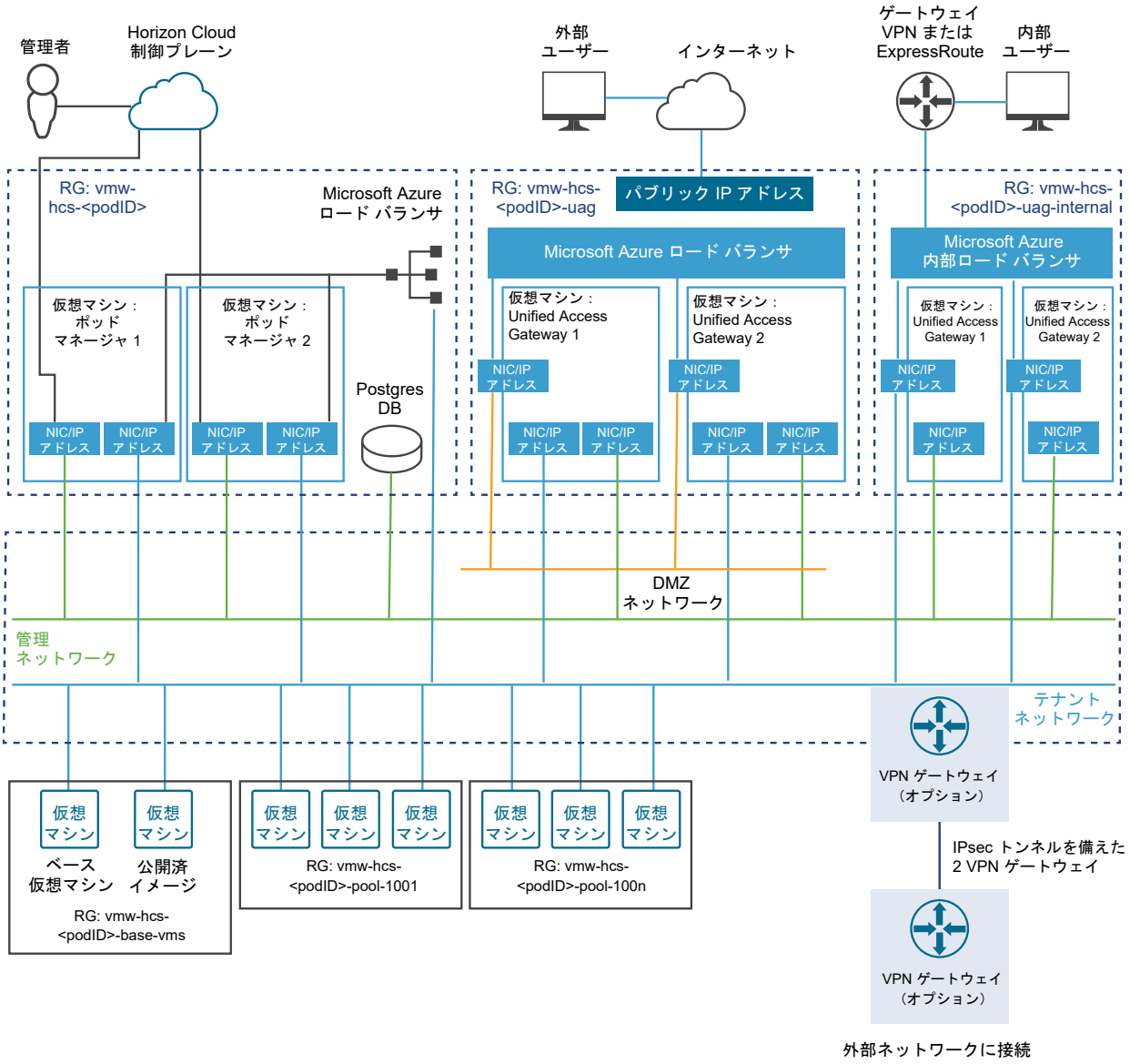
次の図は、外部と内部の両方のタイプのゲートウェイ構成があり、外部ゲートウェイがポッド自身と同じ VNet に存在するデプロイされたポッドを示しています。この図では、`RG` はリソース グループを意味します。

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。

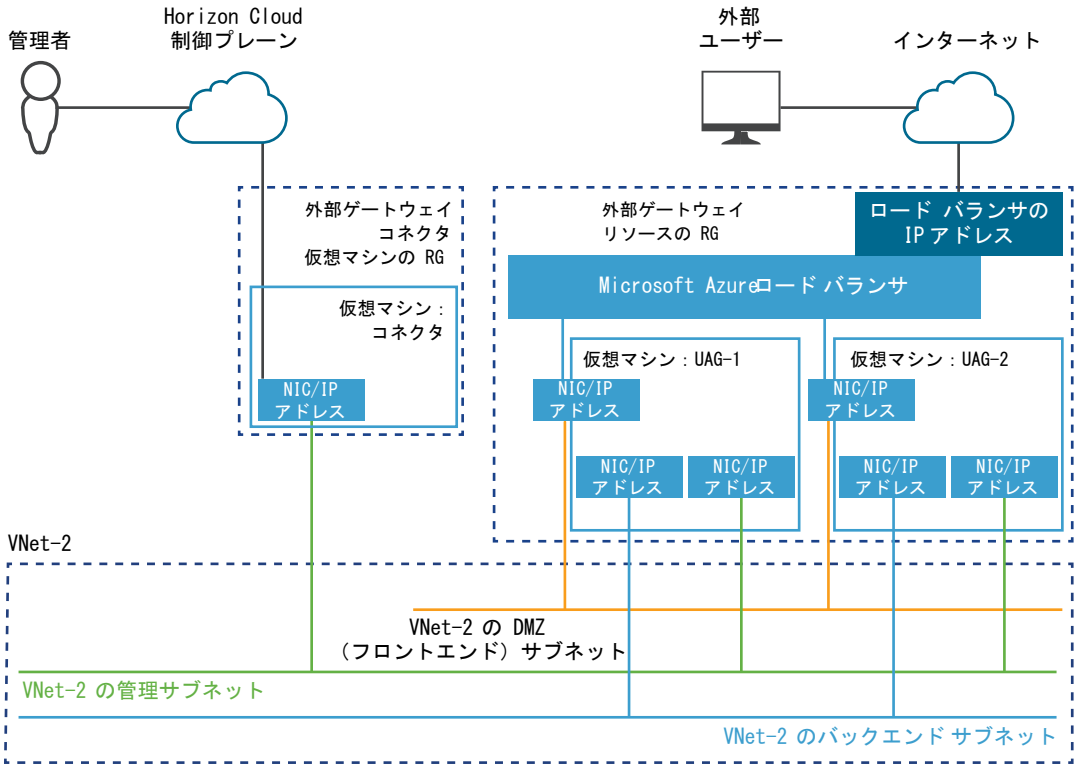
図 6-1. 高可用性が有効で、外部および内部の両方の Unified Access Gateway 構成を持つポッドの Horizon Cloud Pod アーキテクチャの図



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



サブスクリプションとポッドの数

1 つのサブスクリプションにデプロイするポッドの数については、特に大規模に各ポッドを実行させる予定がある場合は、十分に考慮に入れておいてください。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、各ポッド内のファーム RDSH 仮想マシンの数、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ことで、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。

この現在の Horizon Cloud リリースより前にデプロイされた既存のポッドがある場合

Horizon Cloud ポッド - メンテナンスと更新で説明するように、VMware では Horizon Cloud ソフトウェア コンポーネントを定期的に更新して、新しい機能とバグ修正を含めます。クラウド内管理環境は毎週更新され、ポッドのソフトウェア コンポーネントの基盤となるバイナリは通常、ほぼ四半期ごとに更新されます。Horizon Cloud Service のドキュメント ページは、顧客に表示される実質的な機能が初めて登場した各カレンダーの時点の新機能リストが含まれるリリース ノート ページへのアクセスを提供します。

新しいポッドをデプロイすると、そのポッドは常に、現在の実稼働サービス環境の最新のマニフェスト バージョンで作成されます。たとえば、2019 年 8 月に新しいポッドを作成した場合、そのポッドには、その日付の時点での Horizon Cloud の最新のソフトウェア コンポーネントがデプロイされていました。Horizon Cloud 環境の使用期間に応じて、特定のカレンダー日付の時点で、Horizon Cloud 全体の環境には最新リリース バージョンのポッド、およびまだ最新のマニフェストに更新されていない以前のリリース バージョンのポッドが含まれる場合があります。

重要： 一般にこの管理ガイドでは、現在の実稼動リリースで使用でき、ポッドが現在のリリースで使用可能な最新のポッド マニフェスト バージョンである場合に適用できる機能、ワークフロー、および動作について説明します。管理タスクを実行するクラウドベースのコンソールは動的です。コンソールの Web ベースのインターフェイスは通常、コンソールの領域またはアクションでその機能を使用するためにポッドをアップグレードする必要がある場合にメッセージを表示します。このリリースより前に存在したポッドの場合、一部のワークフローでは、この管理ガイドの説明とは異なる手順が必要になる場合があります。現在、このリリースのワークフローのリストが最新のマニフェスト バージョンのポッドと異なる場合は、ドキュメント トピック既存のクラウド接続ポッドを使用している現在の顧客向け — Horizon Cloud リリースについておよびトピックに含まれるセクションを参照してください。

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）	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。 **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。
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）	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。
Azure Resource Manager overview（Azure Resource Manager の概要）	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。
Azure VNet	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。
Azure VNet Peering（Azure VNet ピアリング）	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。
Azure のハブ - スポーク ネットワーク トポロジ	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。
Microsoft Azure ExpressRoute の概要	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 を使用する方法について説明します。
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	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。
Azure Load Balancer の概要	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。
Azure Database for PostgreSQL の概要	この記事では、Microsoft Azure Database for PostgreSQL サービスについて説明します。
Azure 仮想デスクトップの概要	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。

次のトピックを参照してください。

- Horizon Cloud on Microsoft Azure 環境の高可用性の特性
- Microsoft Azure でのデスクトップ イメージと Horizon Cloud ポッドの作成
- Horizon Cloud 環境のファームと VDI デスクトップでの Microsoft Azure Disk Encryption の使用
- Microsoft Azure の Horizon Cloud ポッドからの仮想デスクトップでのデータディスクの使用
- Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッド
- Horizon Universal Console でのファームと割り当ての仮想マシン タイプとサイズの管理
- ネストされた Active Directory ドメイン組織単位の使用についての考慮事項
- Horizon Cloud のファーム
- Horizon Cloud インベントリ内のアプリケーション
- Microsoft Azure の Horizon Cloud ポッドに基づくテナントのデスクトップ割り当ての概要
- シングルポッド ブローカ - Horizon Cloud ポッド - URL リダイレクトのカスタマイズを作成し、ユーザーに割り当てる
- Microsoft Azure での Horizon Cloud ポッドの公開イメージの管理
- Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた割り当ての管理
- Horizon Cloud ポッド - VDI デスクトップ割り当て、ファーム、公開イメージ、ベース仮想マシンにインストールされたエージェント関連ソフトウェアの更新
- Microsoft Azure にデプロイされた Horizon Cloud ポッドの管理

Horizon Cloud on Microsoft Azure 環境の高可用性の特性

このドキュメント ページでは、Horizon Cloud on Microsoft Azure 環境の高可用性の特性について説明します。

v2204 サービス リリース以降、新しい環境はデフォルトで高可用性 (HA) が構成された状態でデプロイされます。

v2204 リリースより前に存在していたポッドがあり、そのポッドで高可用性が現在有効になっていない場合は、Microsoft Azure の Horizon Cloud ポッドで高可用性を有効にするの手順を使用して有効にできます。ポッドの詳細ページでは、そのポッドに対して高可用性が有効であるかが示されます。

簡単な紹介

Horizon Cloud on Microsoft Azure 環境の高可用性の特性は、環境の標準操作を次のシナリオでも引き続き機能させることを目的としています。

- 1 台のポッド マネージャ仮想マシンがダウンした場合、または問題が発生した場合、そのポッド マネージャに向けられたトラフィックは、手動による介入なしに、他のポッド マネージャ仮想マシンに自動的にルーティングされる。
- ゲートウェイ構成で、1 台の Unified Access Gateway 仮想マシンがダウンした場合、または問題が発生した場合、その Unified Access Gateway 仮想マシンに向けられたトラフィックは、手動による介入なしに、他の Unified Access Gateway 仮想マシンにルーティングされる。

設計の要素

Horizon Cloud on Microsoft Azure 環境の HA 設計では、次の要素を使用します。

これらの要素により、ペアリングされた仮想マシンの 1 台に問題や障害が発生した場合に、回復性とフェイルオーバーが発揮されます。

- ペアリングされた仮想マシン
- 仮想マシン ペアごとの Microsoft Azure の可用性セット
- 各ペアの仮想マシンを接続する Microsoft Azure ロード バランサ
- Azure Database for PostgreSQL の Microsoft で管理されたサービス

これらの設計要素を環境で使用する方法の詳細については、このドキュメント ページの以降のセクションを参照してください。

ペアリングされた仮想マシン

Horizon Cloud on Microsoft Azure デプロイヤは、デフォルトで以下をデプロイします。

- Horizon Cloud on Microsoft Azure 環境ごとに 2 台のポッド マネージャ仮想マシン
- デプロイされたゲートウェイ構成ごとに 2 台の Unified Access Gateway 仮想マシン。

注： 独自の VNet にデプロイされた外部ゲートウェイ構成のデプロイ シナリオでデプロイされたゲートウェイ コネクタ仮想マシンの場合、単一のゲートウェイ コネクタ仮想マシンがデプロイされます。ゲートウェイ コネクタがダウンした場合、制御プレーンはアラートを VMware Horizon Cloud オペレーション チームに送信します。チームは、API 呼び出しを使用してゲートウェイ コネクタの状態に対処できます。

仮想マシン ペアごとの Microsoft Azure の可用性セット

各仮想マシン ペアは、Microsoft Azure の可用性セット（仮想マシン ペアごとの可用性セット）に関連付けられます。

可用性セットを使用することで、ペアの仮想マシンは、それぞれ同じ Microsoft Azure データセンター内の別個の物理ハードウェアにデプロイされます。

Microsoft Azure の可用性セットの設計により、ペアリングされた仮想マシンは、その Microsoft Azure データセンター内の個別の物理ハードウェアに常駐するように強制されます。

このバックエンド ハードウェアの分離により、2 台の仮想マシンがともに同時にダウンタイムを生じる可能性を最小限に抑えることができます。Microsoft Azure データセンター全体がダウンした場合にのみ、ペアの両方の仮想マシンがともに影響を受けます。

各ペアの仮想マシンを接続する Microsoft Azure ロード バランサ

ペアリングされた仮想マシンセクションに記載されているように、Horizon Cloud on Microsoft Azure 環境にはポッド マネージャ仮想マシンのペアがあり、デプロイされた各ゲートウェイ構成には Unified Access Gateway 仮想マシンのペアがあります。

デプロイヤは、仮想マシンのペアごとに Microsoft Azure ロード バランサをデプロイします。

ポッド マネージャ仮想マシン - ロード バランサ

デプロイヤは、ポッドのデプロイ中にこの Azure ロード バランサをデプロイします。このロード バランサは、デプロイヤによって構成された健全性プローブとルールに従って、ポッド マネージャ仮想マシンへのトラフィックをルーティングします。

- ポッド マネージャ仮想マシンは、このロード バランサのバックエンド プールに追加されます。
- 1 台のポッド マネージャ仮想マシンが、ポッドでプロビジョニングされたデスクトップおよびアプリケーションへのエンド ユーザー クライアント接続を容易にする上でアクティブな役割を担います。
- ロード バランサは、バックエンド プール内のマネージャ仮想マシンの定義済みルールと健全性プローブに基づいて、アクティブな役割を担うポッド マネージャを決定します。
- その決定に基づいて、ロード バランサはフェイルオーバーが発生するまで、すべての接続要求トラフィックをアクティブな役割を担うポッド マネージャ仮想マシンにシームレスにルーティングします。
- その後、他のポッド マネージャ仮想マシンが、デスクトップおよびアプリケーションへのクライアント接続を容易にする上でアクティブな役割を担います。その時点で、ロード バランサは接続要求をその仮想マシンにルーティングします。
- このフェイルオーバーが発生すると、どのポッド マネージャ仮想マシンがアクティブな役割に変更されたかを知らせる通知が、コンソールに送信されます。

ポッド マネージャ仮想マシンのデプロイ済み Azure ロード バランサは、IP アドレスを持ち、[新規ポッド] ウィザードに [仮想マシン サブネット - プライマリ]（プライマリ テナント サブネットとも呼ばれます）というラベルが付けられた仮想マシンの NIC に接続されます。

ポッド マネージャ仮想マシンのロード バランサは、エンドユーザーのクライアント接続要求とポッド マネージャ仮想マシンの間に配置されます。

ポッドにゲートウェイ構成が設定されている場合、Unified Access Gateway インスタンスからのトラフィックはこのポッド マネージャ仮想マシンの Microsoft Azure ロード バランサにルーティングされ、Azure ロード バランサはそのトラフィックをアクティブなポッド マネージャ仮想マシンにルーティングします。

ポッドにゲートウェイ構成がなく、直接接続用にポッドを構成している場合、エンドユーザーのクライアント接続はポッド マネージャ仮想マシンの Microsoft Azure ロード バランサに移動し、そのトラフィックはロード バランサによってアクティブなポッド マネージャ仮想マシンにルーティングされます。

ゲートウェイ構成 - ロード バランサ

デプロイヤは、ゲートウェイ構成のデプロイ中にこの Azure ロード バランサをデプロイします。このロード バランサは、デプロイヤによって構成された健全性プローブとルールに従って、トラフィックを環境の Unified Access Gateway 仮想マシンにルーティングします。

- Unified Access Gateway 仮想マシンは、このロード バランサのバックエンド プールに追加されます。
- エンドユーザーのクライアント トラフィックでは、各 Unified Access Gateway 仮想マシンにアクティブなロールがあります。Unified Access Gateway 仮想マシンはそれぞれ、Horizon Cloud Service on Microsoft Azure サービス制限 ページで説明する制限まで、ポッドの同時接続セッションを管理します。
- ロード バランサは、仮想マシンの定義されたルールと健全性プローブに基づいて、バックエンド プール内の Unified Access Gateway 仮想マシンが健全な状態で接続要求を受け取ることができるかを判断します。

- ロード バランサは、その決定に基づいて、健全性プローブを満たす仮想マシンに接続要求トラフィックをシームレスにルーティングします。
- バックエンド プールの仮想マシンに問題があるか、ダウンしている場合、ロード バランサは新しい接続要求を健全な仮想マシンにルーティングします。
- 問題が発生している、またはダウンしている仮想マシンへの既存の接続は切断されます。ユーザーはクライアント セッションを手動で再接続する必要があり、ロード バランサはそれらを健全な Unified Access Gateway 仮想マシンに接続します。
- 健全でない仮想マシンが健全な状態に戻り、ロード バランサのルールと健全性プローブを満たすと、ロード バランサはその仮想マシンへの新しい接続要求を許可します。

ゲートウェイ構成のロード バランサは、エンドユーザーのクライアント接続要求と構成の Unified Access Gateway 仮想マシンの間に配置されます。

外部ゲートウェイ構成の場合、デプロイされた Azure ロード バランサは、IP アドレスを持ち、デプロイヤ ウィザードに [DMZ サブネット] というラベルが付けられた仮想マシンの NIC に接続されます。ウィザードを使用して独自の VNet に外部ゲートウェイ構成をデプロイする場合、ウィザードはこのサブネットに [フロントエンド サブネット] というラベルを付けます。

内部ゲートウェイ構成の場合、デプロイされた Azure ロード バランサは、(デプロイヤ ウィザードで [仮想マシン サブネット - プライマリ] というラベルが付いた) ポッドのプライマリ テナント サブネット上の IP アドレスを持つ仮想マシンの NIC に接続されます。

環境の Azure Database for PostgreSQL の Microsoft で管理されたサービス

この環境では、Azure Database for PostgreSQL の Microsoft で管理されたサービスと、その 単一サーバ デプロイ オプション を使用します。

この Microsoft で管理されたサービスを使用すると、ポッド操作に必要なデータを一元化し、マネージャ仮想マシン間でデータ レプリケーションを使用する必要がなくなります。現在のリリースでは、デプロイヤは次の構成を使用します。

- PostgreSQL バージョン 11
- メモリ最適化
- コンピューティング世代：Gen 5
- vCore 数：2
- ストレージ：10 GB
- 自動拡張：いいえ
- バックアップ ストレージ：ローカル冗長

メモリ最適化の構成の詳細については、Microsoft のドキュメントを参照してください。

- Azure Database for PostgreSQL - 単一サーバの価格レベル
- 価格設定 - Azure Database for PostgreSQL

このリリース レベルで作成または更新されたポッドの Microsoft Azure サブスクリプションにおけるコストの影響

このリリースで高可用性をサポートするために必要な要素は、Azure Database for PostgreSQL の使用および仮想マシン ペアの実行のために、Microsoft Azure サブスクリプションのコストに影響します。この記事の作成時点では、Azure ロード バランサまたは可用性セットの使用のコストは発生しません。

現在のリリースで使用される、前述の Microsoft Azure Database for PostgreSQL 構成の価格見積もりについては、https://azure.microsoft.com/en-us/pricing/details/postgresql/server/を参照してください。

関連リソース グループ

ポッド マネージャの HA 関連リソースは、ポッド マネージャ仮想マシンと同じリソース グループに存在します。

ゲートウェイ構成の HA 関連リソースは、そのゲートウェイ構成の Unified Access Gateway 仮想マシンと同じゲートウェイ構成のリソース グループに存在します。

ポッド マネージャのリソース グループは、環境での Microsoft Azure Database for PostgreSQL の Microsoft で管理されたサービスの使用も反映します。

Microsoft Azure ポータルにログインしてそれらのリソース グループに移動すると、サブスクリプションのリソースの詳細を表示できます。

ポッドのリソース グループを識別することの詳細については、Horizon Cloud on Microsoft Azure デプロイ用に作成されたリソース グループを参照してください。

Microsoft Azure の Horizon Cloud ポッドでの高可用性の有効化

高可用性が有効になっていないポッドの場合は、次の手順に従って高可用性を有効にできます。

このページは、高可用性がまだ有効になっていない 1 つ以上のポッドを持つ管理者のみを対象としています。

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すでに高可用性が構成された状態でデプロイされます。ポッドで高可用性がすでに構成されている場合、このページの手順は適用されません。

ポッドの詳細ページに高可用性が有効でないことが示されている場合は、ポッドを編集して高可用性を有効にすることができます。このプロセスでは、2 番目のポッド マネージャ仮想マシンがポッドのリソース グループにデプロイされ、その仮想マシンがポッドの Microsoft Azure ロード バランサと可用性セットで構成されます。

重要： 高可用性のためにポッドを有効にすることは、1 回限りのアクションです。高可用性のためにポッドを有効にすると、後で構成を元に戻して、ポッドでこの機能を無効にすることはできません。

[ポッドの編集] ワークフローの手順を実行して更新を確認すると、サービスはポッドの Microsoft Azure サブスクリプションで 2 番目のポッド マネージャ仮想マシンをインスタンス化し、その仮想マシンと既存の Azure ロード バランサ、Azure PostgreSQL データベース、およびその他の必要なポッド関連タスクとの間に適切な接続を行います。全体のプロセスが完了するまで約 30 分かかることがあります。

前提条件

Horizon Universal Console を使用してワークフローの手順を実行する前に、次の基準を満たしていることを確認します。

- 高可用性を有効にするには、ポッドのソフトウェアがマニフェスト バージョン 1600 以降である必要があります。ポッドのマニフェスト バージョンを確認するには、[キャパシティ] ページからポッドの詳細ページに移動します。
- サブスクリプションに、追加のポッド マネージャ仮想マシンの作成に対応できる、十分な割り当てとコアがあることを確認します。
- ポッドが 1600 より前のマニフェスト バージョンから更新された場合、ポッドの高可用性を有効にする前に、以下を確認する必要があります。
  - ポッドの更新プロセスがそのポッドで完了していること。
  - エージェントが、ポッドのイメージ仮想マシン、ファーム RDSH 仮想マシン、およびデスクトップ割り当て仮想マシンのすべてで、更新されたポッドで実行しているマニフェストと互換性のあるエージェント リリース レベルに更新されていること。ポッドの更新とエージェントの更新の関係については、Horizon Cloud ポッドの更新：エージェントの互換性とサポートを継続するための手順を参照してください。

手順

1 [キャパシティ] ページからポッドの詳細ページに移動します。

2 [編集] をクリックします。

3 [高可用性] セクションで、[有効] トグルをオンに切り替えます。

4 [保存して終了] をクリックします。

5 本当に更新してよいか確認します。

結果

ポッドの詳細ページで、クラスタのステータスに [保留中] の状態が表示されます。構成アクティビティが完了すると、クラスタのステータスに [準備完了] の状態が表示されます。全体のプロセスが完了するまで約 30 分かかります。

Microsoft Azure でのデスクトップ イメージと Horizon Cloud ポッドの作成

デプロイされたポッドからデスクトップまたは RDS ベースのリモート アプリケーションをエンド ユーザーに提供するには、少なくとも 1 つの割り当て可能なデスクトップ イメージを作成する必要があります。この割り当て可能なイメージの作成は複数の手順からなるプロセスです。ベース仮想マシン (VM) を作成して Horizon Cloud とペアリングし、組織のニーズに応じてカスタマイズして、それを割り当て可能なデスクトップ イメージに変換する必要があります。

このページでは、シングルポッドベースのゴールド イメージを作成する手順について説明します。

重要： 第 1 世代 Horizon Cloud on Microsoft Azure デプロイ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 から供給される 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。

イメージで Windows 11 オペレーティング システムが実行されている場合は、Azure Marketplace から直接供給される必要があるほか、イメージを第 1 世代 Horizon Cloud on Microsoft Azure デプロイで有効にサポートするために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。

第 1 世代 Horizon Cloud on Microsoft Azure デプロイでのイメージ関連のワークフローでサポートされる Gen-1 マシンと Gen-2 マシンの組み合わせ、およびどの OS がどのマシン世代でサポートされているかについての追加の考慮事項については、Microsoft Azure のポッドから提供されるイメージのサポートを参照してください。

ここで説明する手順に加えて、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、Horizon Image Management Service およびマルチポッド イメージの機能を使用できます。マルチポッド イメージの詳細については、『クラウドからの Horizon イメージの管理』ガイドとそのサブトピックを参照してください。

注： 2022 年 7 月の時点で、サポートされていないマニフェストのポッドに関連するコンテンツはこのページから削除されました。このようなデプロイは、VMware KB 86476 で記載されているとおり、ジェネラル サポートが終了しました。

簡単な紹介

Horizon Cloud on Microsoft Azure デプロイの場合、最初に Azure Marketplace からベース仮想マシンをインポートします。ベース仮想マシンをカスタマイズすると、ゴールド イメージが作成されます。このゴールド イメージをシーリングすると、テナントのファームおよび単一セッション VDI デスクトップ割り当てで使用できる割り当て可能なイメージが生成されます。

この割り当て可能イメージは、Horizon Cloud のシーリング プロセスが正常に完了したイメージであり、ファーム (RDS ベースのイメージまたは Windows Enterprise マルチセッションで構築されたマルチセッション イメージの場合）または単一セッション VDI デスクトップ（クライアントベースのイメージの場合）をプロビジョニングするために使用できます。Horizon Universal Console では、コンソールのワークフローでイメージをシーリングするために、ラベル [公開] を使用します。

シールドして RDS ファームまたは VDI デスクトップのプロビジョニングに使用できるゴールド イメージを作成する手順の概要を以下に示します。

最初に、ベース仮想マシン (VM) を作成する

自動化されたワークフローを使用するか手動でベース仮想マシンを作成します。

- 推奨される標準的な方法は、管理コンソールの自動化されたワークフローを使用して、Microsoft Azure Marketplace でサポートされている仮想マシン構成の 1 つを使用してベース仮想マシンを作成することです。自動化されたワークフローを使用すると、仮想マシン (VM) の構築が自動化されます。

デフォルトのテナント構成では、自動化されたワークフローは、適切なエージェント関連ソフトウェアのインストールおよび構成など、Horizon Cloud 環境の要件に準拠するように仮想マシンを構成します。この構成では、ワークフローには仮想マシンを最適化するためのオプションもあり、Microsoft Windows Sysprep エラーの発生を防ぐことができます。コンソールの [インベントリ] ページで、[インポート] をクリックしてワークフローを開始します。手順については*ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリング*を参照してください。このウィザードは、App Volumes Agent や Horizon Agent のリモート エクスペリエンス機能など、エージェント関連のオプションが仮想マシンにインストールされるようにするトグルを提供します。ウィザードでリモート エクスペリエンス機能を選択する前に、*Horizon Cloud ファームとデスクトップから最適なリモート エクスペリエンス パフォーマンスを引き出すためにゴールド イメージで実行すべき 5 つの重要な手順*を参照してください。

- 標準的な方法の代替方法としては、Microsoft Azure ポータルを使用して、ウィザードでは自動化されるすべての手順を手動で実行することになります。これらの手動の手順については、*Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートする*を参照してください。この手動ワークフローでは、Horizon Agents Installer (HAI) を手動で実行して、仮想マシンを Horizon Cloud とペアリングするための必須のエージェント ソフトウェアをインストールする必要があります。

  重要： この代替方法を使用する場合は、自己責任で、作成される仮想マシンが、確実に Horizon Cloud 環境で必要となる構成に準拠しているようにします。自動化されたウィザードの [Windows イメージを最適化] および [Windows ストア アプリを削除] で説明されているオプションと同じ構成を適用することを強くお勧めします。これらの構成を使用すると、仮想マシンが後でイメージとして公開される際に、Microsoft Windows の Sysprep でエラーが起きるのを回避することができます。*[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に Windows イメージの最適化を決定する*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に [Windows ストア アプリを削除] オプションを使用する*を参照してください。

次に、イメージ仮想マシンと Horizon Cloud をペアリングする

次の表では、仮想マシンにエージェント ソフトウェアがインストールされているにもかかわらずその仮想マシンがペアリングされていない場合に、リストされた事例ごとに、[インポートされた仮想マシン] ページの [エージェントのステータス] 列に表示される内容について説明します。

作成方法	表示されたステータス
自動ウィザード	ペアなし（インポートに成功しました）
手動	ペアなし

次のスクリーンショットは、自動ウィザードを使用して正常に作成されたにもかかわらず、まだ Horizon Cloud.とペアリングされていない仮想マシンを示しています。

仮想マシンと Horizon Cloud を明示的にペアリングする必要があります。

[インポートされた仮想マシン] ページで、仮想マシンに対して [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、仮想マシンを Horizon Cloud と明示的にペアリングします。この処理には数分かかることがあります。ペアリング処理中に仮想マシンが再起動され、そのエージェントのステータスが **不明**、**有効** に変わります。ステータスの変化を確認するには、円形の矢印アイコンを使用してページを更新する必要があります。

[エージェントのステータス] 列に **有効** および `19.4.0` などのエージェントのバージョンが表示されると、ペアリング処理は完了します。次のスクリーンショットは、ペアリング処理が完了した後の仮想マシンを示します。

3 番目に、仮想マシンをカスタマイズする

ペアリング処理が完了し、ページを更新した後、仮想マシンのエージェントのステータスがアクティブであることが示されている場合は、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使用してイメージ仮想マシンのゲスト Windows オペレーティング システム (OS) をカスタマイズし、カスタマイズされた壁紙、フォントと色、ドライバなど、OS レベルの設定を構成します。手順については、インポートされた仮想マシンの Windows オペレーティング システムをカスタマイズおよび Horizon Cloud on Microsoft Azure - インポートした GPU 対応仮想マシンに適切な GPU ドライバをインストールするを参照してください。

重要： 2019 年 12 月のサービス リリース以降、[仮想マシンのインポート] ウィザードは、ウィザードで作成された仮想マシンを指定された Active Directory ドメインに参加させるか、仮想マシンをドメインに参加させないかのオプションを提供します。2019 年 12 月のサービス リリースより前は、ウィザードで作成された仮想マシンは常に自動的にドメインに参加していました。また組織は、手動で作成された仮想マシンをドメインに参加させ、ドメイン管理者アカウントでログインして、それらの仮想マシンをシーリングする前にカスタマイズすることを選択できます。

ベース仮想マシンが作成中にドメインに参加した場合、ドメイン管理者アカウントで仮想マシンにログインし、カスタマイズできます。

リモート エクスペリエンスのパフォーマンスを最適化するための仮想マシンの構成

特定の組織のニーズに合わせて仮想マシンをカスタマイズしたら、Horizon Cloud ファームとデスクトップから最適なリモート エクスペリエンス パフォーマンスを引き出すためにゴールド イメージで実行すべき 5 つの重要な手順の手順に従って、エンド ユーザーが割り当てられたデスクトップおよびアプリケーションから最適なリモート エクスペリエンス パフォーマンスを確実に得られるようにします。

最後に、ゴールド イメージを公開イメージに変換する

デフォルトのテナント構成では、RDSH イメージと VDI イメージの両方について、[新しいイメージ] ワークフローを使用してこれらの仮想マシンを割り当て可能なデスクトップ イメージに変換します。手順については構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の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。

仮想マシンを変換した後、[イメージ] ページのイメージの [公開済み] ステータスは、Horizon Cloud がイメージ仮想マシンを環境内で使用するためにシールドしたことを示します。[インベントリ - イメージ] ページのイメージに [公開済み] ステータスが表示されている場合、以下を作成できます。

- RDS ベースのイメージから、そのイメージに基づいて作成された RDSH ファーム。同じ公開済み RDS ベースのイメージから両方の種類のファームを作成できます : セッションベースのデスクトップへのエンドユーザー アクセスを提供するデスクトップ ファーム、リモート アプリケーションへのアクセスを提供するアプリケーション ファーム。ファームを作成した場合は、そのファームを使用してユーザーに割り当てを行うことができます。Horizon Cloud のファームを参照してください。
- Windows クライアントベースのイメージからそのイメージに基づく VDI デスクトップ割り当て。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および 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を参照してください。

Microsoft Azure の Horizon Cloud ポッドでの VMware Dynamic Environment Manager エージェント ソフトウェアおよびデスクトップ イメージの作成について

2019 年 7 月の Horizon Cloud リリース以降、VMware Dynamic Environment Manager エージェントのインストールは、Horizon Agents Installer と自動化された [デスクトップのインポート] ワークフローの両方に組み込まれています。VMware Dynamic Environment Manager エージェント コンポーネントは、FlexEngine クライアント コンポーネントとも呼ばれます。Horizon Agents Installer は、[デスクトップのインポート] ワークフローを実行するとき、またはイメージ仮想マシンを手動で作成するときに、エージェントに関連するソフトウェアを新しいイメージ仮想マシンにインストールするソフトウェア パッケージです。ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリングすると、Horizon Agents Installer がバックグラウンドで実行され、エージェントがインストールされます。Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートする場合は、これらの手順の一部として Horizon Agents Installer をダウンロードして実行します。

2019 年 7 月の Horizon Cloud リリースは、Horizon Agents Installer のバージョン 19.2 に対応しています。VMware Dynamic Environment Manager ファイルは、以下に説明するように、作成されたイメージ仮想マシンのファイル パスにインストールされます。

マニフェスト バージョン 1493 以降のポッドの場合は、自動化された [デスクトップのインポート] ワークフローを使用して、そのポッドで基本のイメージ仮想マシンが作成されるとき

このポッドのバージョンは、デフォルトで VMware Dynamic Environment Manager コンポーネントがこれらの基本イメージに自動的にインストールされる最初のバージョンです。結果のインストール ファイル パスは、`C:\Program Files\VMware\Horizon Agents\User Environment` です。

マニフェスト バージョン 1493 以降のポッドの場合は、基本のイメージ仮想マシンが手動で作成されるとき

このポッドのバージョンは、Horizon Agents Installer に VMware Dynamic Environment Manager コンポーネントをインストールするオプションがある最初のバージョンです。手動で作成された基本の仮想マシンで Horizon Agents Installer を実行するときにそのオプションをインストールすることを選択した場合、結果

のインストール ファイル パスは、`C:\Program Files\VMware\Horizon Agents\User Environment` です。

マニフェスト バージョン 1493 以前のポッドの場合は、自動化された [デスクトップのインポート] ワークフローまたは手動の作成方法を使用して、そのポッドで基本のイメージ仮想マシンが作成されるとき

この場合、自動化されたワークフローはデフォルトで VMware Dynamic Environment Manager コンポーネントを結果の仮想マシンにインストールしません。これらの古いポッドの基本イメージの場合は、https://my.vmware.com の Horizon Cloud の [ダウンロード] ページからダウンロードしたスタンドアローンの VMware Dynamic Environment Manager インストーラを手動で実行する必要があります。この場合、結果のインストール ファイル パスは、`C:\Program Files\Immidio\Flex Profiles` です。

ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリング

Microsoft Azure の Horizon Cloud ポッドでは、[仮想マシンのインポート – Marketplace] ウィザードに従って、Microsoft Azure Marketplace のオペレーティング システム イメージを使用して仮想マシン (VM) を作成できます。プロセスでは、仮想マシンは Horizon Cloud 環境の要件に準拠するために必要な要素とエージェントに関連したソフトウェアを使用して自動的に構成されます。作成プロセスの最後に、仮想マシンが [インポートされた仮想マシン] ページに一覧表示され、仮想マシンとクラウド プレーンのペアリング、仮想マシンのカスタマイズ、追加のドライバのインストールなど、さらにアクションを実行できます。

ヒント: 2021 年 7 月のサービス リリースでは、すべての Horizon Cloud ポッドがマニフェスト 2632 以降で、テナントが Universal Broker を使用するように構成されている場合に、Horizon Image Management Service およびマルチポッド イメージ管理の機能が使用可能です。その場合、単一セッションの VDI オペレーティング システムでは、ここで説明するように [インポートされた仮想マシン] ページを使用して仮想マシンをインポートする代わりに、[マルチポッド イメージ] ページを使用して仮想マシンをインポートし、イメージ カタログ内で使用することもできます。[マルチポッド イメージ] ページの概要を参照してください。

このトピックで説明する手順を使用して仮想マシンをインポートすると、自動ワークフローは、Horizon Cloud とまだペアリングされていない仮想マシンになります。仮想マシンが作成され、[インポートされた仮想マシン] ページにリストされたら、[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、仮想マシンをクラウド プレーンとペアリングします。

注意: すべてのコンソールと同様に、このウィザードのユーザー インターフェイスは動的です。ウィザードを通してリスト内の項目を選択したり、トグルを有効または無効にしたりするたびに、ウィザードで表示される選択内容とオプションは自動的に変更されます。ウィザードの表示項目は、Horizon Cloud テナント アカウントに使用が許可されているものが何であるかも反映されます。ここに記載されている内容を読んだ上で、ウィザードをリアルタイムで進んでいくなかで表示内容が変更されない場合は、ウィザードの上部に設定されている選択内容を変更して、ウィザードのオプションの変更を確認してください。この操作を試行した後でも、説明された内容が表示されない場合は、その項目はアカウントの構成に適用されない可能性が極めて高くなります。

ウィザードの一部のデフォルト設定について

デフォルトでは、オペレーティング システムに関係なく、[Windows イメージを最適化]が有効になります。マルチセッション以外の Windows 10 オペレーティング システムの場合、システムはデフォルトで [Windows ストア アプリを削除] を有効にします。後で仮想マシンがイメージとして公開されたときに発生する可能性のある Microsoft Windows Sysprep の問題を回避するため、これらのオプションを有効にすることを強く推奨します。

また、デフォルトで、ウィザードは [詳細オプション] セクションで さまざまなトグルを有効にして、(ウィザードの他の選択項目に対しても適切で関連があり、選択したオペレーティング システムでの Horizon Cloud 環境で使用するためにサポートされている) エージェント関連のカスタム セットアップ オプションをインストールします。デフォルトの選択を変更する場合は、[仮想マシンのインポート - Marketplace] ウィンドウの [詳細オプション] セクションを展開し、必要に応じてトグルを設定します。

たとえば、RDS またはマルチセッションの使用事例をサポートするオペレーティング システムでのみ 3D サポートを提供するエージェント オプションは、[OS] ドロップダウン リストでこれらのオペレーティング システムのいずれかを選択した場合にのみ、デフォルトで [詳細オプション] セクションで有効になります。VDI の使用事例でクライアント オペレーティング システムを選択し、そのエージェント オプションが適用されていない場合、そのエージェント オプションはインストール対象として選択されません。

ウィザードで作成された仮想マシンで使用される NSG ルールについて

2021 年 6 月、Microsoft Azure のベスト プラクティスに準拠するため、ウィザードで作成されたベース仮想マシンでのネットワーク セキュリティ グループ (NSG) の使用がサービスで開始されました。この機能が使用された後にこのウィザードを初めて実行すると、ウィザードは仮想マシンと同じリソース グループに NSG を作成し、作成された仮想マシンの NIC をその NSG に接続します。詳細については、Horizon Cloud の [Marketplace からの仮想マシンのインポート] ウィザードによって作成されたネットワーク セキュリティ グループ (NSG)を参照してください。

指定された Active Directory ドメインに参加する作成された仮想マシンについて

2019 年 12 月のサービス リリース以降、[仮想マシンのインポート] ウィザードは、作成プロセスの最後に、ウィザードで作成された仮想マシンを指定された Active Directory ドメインに参加させるか、仮想マシンをドメインに参加させないかのオプションを提供します。

この自動インポート ウィザードが Azure サブスクリプションで使用する必要がある仮想マシン ファミリ タイプについて

デフォルトでは、この自動インポート ウィザードは、Azure Marketplace の仮想マシン ファミリの特定の仮想マシン モデルを使用します。Azure サブスクリプションで、仮想マシンを作成するための十分な割り当てが関連する仮想マシン ファミリにない場合、自動インポート プロセスは失敗します。

自動化で使用される仮想マシン ファミリ タイプは、ウィザードで行った選択に関連します。

注： Horizon Cloud で Windows 11 OS をサポートするには、ポッドが v2204 リリースのマニフェスト バージョン以降を実行している必要があります。Windows 11 OS サポートの詳細については、「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。

選択	自動的に使用される仮想マシン モデル	vCPU の Azure ファミリ
非 GPU、Windows 11 OS 以外	Standard_DS2_v2	DSv2 ファミリ
非 GPU Windows 11 OS、Windows 11 Enterprise マルチセッション OS	Standard_D4s_v3	Dsv3 ファミリ（Azure ドキュメント Dsv3 シリーズに従い、Dsv3 の「s」は小文字）
GPU 対応	Standard_NV12s_v3	NVv3 ファミリ

注： コンソールの自動化された [仮想マシンのインポート] ウィザードでは、Windows 7 が選択オプションとして提供されなくなりました。その結果、前の表から Windows 7 の行が削除され、このページで説明したエージェント オプションに以前に表示されていた Windows 7 への参照も削除されました。

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

このマトリックスは、「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」のページにも記載されています。

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

自動ウィザードを使用して GPU 対応の仮想マシンをインポートする場合、Microsoft Azure は NV ファミリの割り当てを提供しません

サブスクリプションで Standard_NV12s_v3 仮想マシンを作成できない場合、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 GPU 対応の仮想マシンをインポートすることはできません。自動インポートは失敗します。

その場合、このウィザードを使用して Windows 10 OS または Windows Server OS タイプの GPU 対応仮想マシンをインポートする代わりに、手動のインポート手順を使用して、Azure Marketplace から Standard_NV4as_v4 仮想マシンをインポートすることもできます。v2204 サービス リリース以降、Horizon Cloud では、GPU 対応のゴールド イメージのために NVv4 タイプの仮想マシンを Azure Marketplace から手動でインポートできます。このサポートを取得するには、ポッドが v2204 リリースのマニフェスト バージョンを実行している必要があります。このような仮想マシンを Azure Marketplace から手動でインポートして Horizon Cloud on Microsoft Azure の展開で使用する手順については、Microsoft Azure のポッドに仮想マシンを手動で作成するで始まる一連のページに従い、すべての「[次の手順]」セクションを参照してください。この Azure NVv4 ファミリは、AMD Radeon Instinct グラフィックス ドライバを使用します。

手順

1 [インポートされた仮想マシン] ページで、[インポート] をクリックします。

2 [インポート] ウィザードで、まずポッドに関連付けられた場所を選択し、次にその場所のポッドのリストからポッドを選択して、仮想マシンを作成するポッドを選択します。

場所を選択すると、[ポッド] リストの選択項目がフィルタされ、選択した場所で使用可能なポッドが表示されます。

重要： GPU が有効なデスクトップまたはリモート アプリケーションでこのイメージを使用する予定がある場合は、GPU が有効な仮想マシン (VM) をサポートする Microsoft Azure リージョンに選択したポッドが配置されていることを確認します。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。

3 ベース仮想マシンの詳細を選択します。

オプション	説明
オペレーティング システム	イメージの基盤となる仮想マシンに使用する Microsoft Windows サーバ オペレーティング システムを選択します。 **注：** このドロップ ダウン メニューの項目が入力されるまでにはしばらく時間がかかります。 ■ このイメージを VDI デスクトップで使用する場合は、ドロップダウン リストに表示されている、非サーバの非マルチセッション オペレーティング システムのいずれかを選択します。VDI デスクトップ イメージを作成するには、これらのサーバまたはマルチセッション タイプのいずれのオペレーティング システムも選択しないでください。 ■ このイメージを使用して、マルチセッション デスクトップや RDS ベースのリモート アプリケーションなどの共有使用をサポートするアイテムをプロビジョニングする場合は、リストされているサーバまたは複数セッションのオペレーティング システムのいずれかを選択します。
GPU を含める	このトグルを有効にすると、このベース仮想マシンに対して GPU が有効な仮想マシンを指定します。 NVv3 シリーズをサブスクリプションにインポートできることを確認します。サブスクリプションがそのシリーズから Standard_NV12s_v3 仮想マシンをインポートすることをサポートしていない場合、ユーザー インターフェイスでこのトグルを選択できません。 **重要：** このトグルを使用すると、システムは Standard_NV12s_v3 仮想マシン タイプを使用して Azure Marketplace から仮想マシンをインポートします。インポートされた仮想マシンで GPU 機能を使用するには、インポート プロセスが完了したら、仮想マシンのオペレーティング システムにログインし、サポートされている NVIDIA グラフィックス ドライバをインストールする必要があります。 通常、次の手順 9 で説明するように、仮想マシンで [エージェント ペアリングをリセット] アクションを使用した後にドライバをインストールします。
ドメイン参加	このトグルを有効にすると、自動化プロセスの一部として Horizon Cloud テナントに登録されている Active Directory ドメインの 1 つに作成された仮想マシンを参加させるように指定できます。有効にした場合、ドロップダウン リストから Active Directory ドメインを選択します。その結果、仮想マシンは選択したドメインに参加します。そのドメインのドメイン管理者アカウントは、作成された仮想マシンにログインできます。 このトグルをオフに切り替えると、作成された仮想マシンは Active Directory ドメインに参加しません。作成された仮想マシンにログインするには、このウィザードで指定したアカウント認証情報のみを使用できます。

オプション	説明
パブリック IP アドレスを有効にする	このトグルを有効にすると、このマスター仮想マシンの公開 IP アドレスを構成します。有効にすると、仮想マシンはプライベートとパブリックの両方の IP アドレスを取得します。 このトグルをオフに切り替えると、仮想マシンは Microsoft Azure 環境のプライベート IP アドレスのみを使用して構成されます。 このトグルを有効にすると、ワークフローは静的な割り当て方法を使用して、標準 SKU のパブリック IP アドレスとしてパブリック IP アドレスを作成します。標準 SKU のパブリック IP アドレスは、Microsoft Azure のゾーンの回復性を提供します。標準 SKU の IP アドレスは静的割り当てを使用するため、関連付けられた仮想マシンが `stopped-deallocated` 状態にある場合でも、その IP アドレスに対して Microsoft Azure のサブスクリプション コストが発生します。 また、このトグルを有効にすると、ワークフローは、仮想マシンへの RDP 受信接続を許可する受信ルールを持つ仮想マシンと同じリソース グループにある NSG に仮想マシンの NIC を接続します。このルールにより、作成後に RDP を使用してインターネット経由でインポートされた仮想マシンにログインする機能が提供されます。詳細については、Horizon Cloud の [Marketplace からの仮想マシンのインポート] ウィザードによって作成されたネットワーク セキュリティ グループ (NSG)を参照してください。
Windows イメージの最適化	デフォルトではこのトグルは有効になっていて、ベース仮想マシンの Microsoft Windows オペレーティング システムを最適化するための VMware の推奨事項およびベスト プラクティスに適合したマスター仮想マシンが作成されます。この最適化には、オペレーティング システムのデフォルト サービスと機能を調整してベスト プラクティスに適合させるための次のような作業が含まれています。 ■ 仮想環境に関係しない物理デスクトップ機能を無効にして、より効率的な仮想マシン性能を提供します。 ■ Windows Update など、特定の Windows システム サービスを無効にして、サービスの制御をエンド ユーザーではなく管理者に割り当てます。 詳細については、[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に Windows イメージの最適化を決定するを参照してください。 **重要：** 後で仮想マシンがイメージとして公開されたときに発生する可能性のある Microsoft Windows Sysprep の問題を回避するため、デフォルトの設定にすることを強く推奨します。
Windows Store アプリの削除	このトグルは、[OS] が非マルチセッション Microsoft Windows 10 オペレーティング システムに設定されている場合にのみ表示されます。デフォルトではこのトグルは有効になっていて、次のようなベース仮想マシンが作成されます。 ■ Windows ストア インストーラ サービスを無効にする。 ■ ベースの Windows 10 オペレーティング システムにデフォルトで提供されているほとんどの Windows ストア アプリケーションを削除する。これらの Windows 10 のデフォルト アプリケーションは オペレーティング システムの AppX パッケージで提供されているものです。 **重要：** ■ トグルが有効な場合でも、システムは、システム定義の許可リストに基づいて、デフォルトで一部の AppX パッケージを保持します。これらの許可された AppX パッケージは、仮想マシンのインポート プロセスの最後で仮想マシンにインストールされたままになります。リストについては、以下のトピックのリンクを参照してください。 ■ 後で仮想マシンがイメージとして公開されたときに発生する可能性のある Microsoft Windows Sysprep の問題を回避するため、デフォルトの設定にすることを強く推奨します。 詳細については、[デスクトップのインポート] ウィザードを使用する場合に [Windows ストア アプリを削除] オプションを使用するを参照してください。

4 管理の詳細を指定します。

注： 入力するユーザー名とパスワードは、Microsoft Azure で仮想マシンを作成する場合に許可されるユーザー名とパスワードに対する Microsoft の要件を満たしている必要があります。要件のリストについては、Microsoft のドキュメントの「ユーザー名の要件」と「パスワードの要件」を参照してください。

オプション	説明
ユーザー名	仮想マシンのローカル管理者アカウントに使用する管理者名を入力します。このローカル管理者アカウントは、プロセスで仮想マシン内に作成されます。この名前は仮想マシンのオペレーティング システムにアクセスするためのローカル管理者アカウントに使用され、イメージへの変換プロセスでも使用されます。この名前は最大 15 文字の長さで、ピリオド (.) で終了することはできません。また、Microsoft Azure で仮想マシンを作成するときに許可されていない管理者名を使用することはできません。 **重要：** このローカル管理者のアカウント情報（名前および [パスワード] テキスト ボックスで指定したパスワード）を確実に記憶するようにしてください。あるいは後で情報を取得する際に使用するため、忘れないように書き留めておいてください。この基本イメージにサードパーティのアプリケーションを追加する場合、および [新規イメージ] ワークフローを実行してこのベースイメージをシステムに公開する場合にこれらの認証情報が必要になります。
パスワード	管理者アカウントに使用するパスワードを入力します。パスワードは、Microsoft Azure のパスワード ルールに従う必要があります。 ■ Microsoft Azure で仮想マシンを作成するときに許可されていない管理者アカウント パスワードを使用することはできません。 ■ 12 ～ 123 文字の長さで、次の 4 つの複雑さの要件のうち 3 つを満たす必要があります。 ■ 1 つの小文字を含む ■ 1 つの大文字を含む ■ 1 つの数字を含む ■ 1 つの特殊文字 (! @#$%/^&*) を含む
パスワードの検証	パスワードを再入力します。
Windows ライセンスの質問	ウィザードのユーザー インターフェイスで選択を行うと、この質問がウィザードでトグルとチェックボックスの組み合わせの形式で表示されることがあります。画面に表示される指示に従います。新しいポッド デプロイでの VMware Horizon Cloud Service on Microsoft Azure 要件チェックリストのライセンス セクションに記載されているように、Horizon Cloud は、Microsoft Windows オペレーティング システムの使用で必要となるいかなるゲスト OS のライセンスも提供していません。ユーザーは、Horizon Cloud テナント環境で使用するように選択した Windows ベースの VDI デスクトップ仮想マシンとマルチセッション仮想マシンを作成するための、有効かつ適格な Microsoft ライセンスを持っている必要があります。

5 [名前] フィールドに、マスター仮想マシンの名前とオプションの説明を入力します。

重要： 以前に Horizon Cloud 環境で割り当て可能なイメージに変換されたインポートされた仮想マシンに使用した名前は入力しないでください。たとえば、インポートされた仮想マシンが割り当て可能イメージに変換されイメージ ページに表示されている場合は、ここに同じ名前を入力しないでください。既知の問題として、すでに [イメージ] ページにリストされている名前を再利用した場合、仮想マシンの作成プロセスは警告なしで失敗します。システムは Microsoft Azure に仮想マシンを作成しませんが、管理コンソールにはエラー メッセージが表示されません。

名前は次のルールに従う必要があります。

- アンダースコア文字 (_) を含めることはできません。
- 英数字とハイフンのみを使用することができます。
- 名前は（数字ではなく）英字で始める必要があります。
- 名前の終わりにはハイフン (-) を使用できません。

6 仮想マシンにインストールされる Horizon Agent 機能をカスタマイズするには、[詳細オプション] セクションのトグルを使用します。

オプションのトグルを有効にすると、対応する機能が仮想マシンにインストールされます。このウィザードで選択したオプションに加えて、ワークフロー プロセスはデフォルトで次の主要機能を常にインストールします。

- Horizon Agent - HTML5 マルチメディア リダイレクト。パフォーマンスを最適化するために、Chrome または Edge ブラウザの HTML5 マルチメディア コンテンツをユーザーのローカル システムにリダイレクトします。
- Horizon Agent - Horizon Performance Tracker。表示プロトコルのパフォーマンスとシステム リソースの使用量をモニタリングします。
- Horizon Agent - Horizon Monitoring Service Agent。このイメージに基づいて VDI デスクトップ インスタンスまたはファーム マルチセッション仮想マシンのユーザー セッションからアクティビティ関連のデータを収集し、履歴データの収集とレポートのためにそのデータを Cloud Monitoring Service に送信します。
- VMware Dynamic Environment Manager クライアント コンポーネント FlexEngine クライアント コンポーネントは、標準モードを使用してインストールされます。この機能は、このイメージに基づいてプロビジョニングされた VDI デスクトップ仮想マシンおよびマルチセッション仮想マシンで VMware Dynamic Environment Manager 機能を使用できるようにします。

オプション	説明
App Volumes Agent	App Volumes Agent をベース仮想マシンにインストールするには、このトグルを有効にします。このエージェントは、このベース仮想マシンから、後で構成されるデスクトップ イメージを使用して、App Volumes 機能の使用を提供します。Microsoft Azure 上の Horizon Cloud の App Volumes アプリケーション - 概要および前提条件も参照してください。
Flash MMR を有効にする	パフォーマンスを最適化するために、仮想デスクトップにストリーミングされる Flash マルチメディア コンテンツをリダイレクトしてクライアント コンピュータに直接ストリーミングし、そのクライアント システム上でデコードします。クライアント システムはメディア コンテンツを再生し、仮想デスクトップへの要求を開放します。 このエージェント オプションは、Microsoft Windows 10 Enterprise マルチセッションでの使用ではサポートされていません。
RDSH での 3D サポート **Windows 10 マルチセッションでの 3D サポート**	[OS] の選択が Windows サーバまたは Windows 10 マルチサーバ オペレーティング システムに設定されている場合に適用されます。GPU 対応のマルチセッション仮想マシンで実行されるアプリケーションで 3D グラフィックスを使用できるようにします。
ターミナル サービスの MMR	パフォーマンスを最適化するために、仮想デスクトップにストリーミングされるマルチメディア コンテンツをリダイレクトしてクライアント コンピュータに直接ストリーミングし、そのクライアント システム上でデコードします。クライアント システムはメディア コンテンツを再生し、仮想デスクトップへの要求を開放します。

オプション	説明
クライアント ドライブのリダイレクト	これを使用すると、Horizon Client ユーザーがローカル ドライブを仮想デスクトップおよび RDS ベースのアプリケーションと共有できます。
Skype for Business	**注：** Horizon Cloud Service 2303 リリースの時点では、この機能はマニフェスト バージョン 4136 以降のポッドでは使用できません。この機能は、マニフェスト バージョン 4136 以降のポッドでは使用できません。 マニフェスト 4136 より前のマニフェストのポッドの場合、このオプションにより、仮想デスクトップを使用して Skype for Business で最適化された音声およびビデオ通話を行うことができます。
Webcam サポート（リアルタイム オーディオ ビデオ RTAV）	ユーザーのクライアント システムに接続される Web カメラおよびオーディオ デバイスをリダイレクトするので、それらのデバイスを仮想デスクトップで使用できます。
スマート カード	デフォルトではインストールされません。ユーザーが、PCoIP または Blast Extreme 表示プロトコルの使用時にスマート カードを使用して認証できるようにします。
VMware 出力	インポートされた仮想マシンに Horizon Agent の VMware Integrated Printing 機能をインストールして構成します。この機能によって、ユーザーは追加ドライバをインストールせずに、クライアント コンピュータで使用可能なプリンタを使用できるようになります。
スキャナ リダイレクト	デフォルトではインストールされません。ユーザーのクライアント システムに接続されるスキャン デバイスおよびイメージング デバイスをリダイレクトするので、それらのデバイスを仮想デスクトップまたは RDS ベースのアプリケーションで使用できます。
USB リダイレクト	デフォルトではインストールされません。ユーザーは、ローカルに接続された USB フラッシュ ドライブ、および仮想デスクトップと RDS ベースのアプリケーションのハード ディスクにアクセスできます。 **注：** 組織に、エンド ユーザーのローカルに接続された USB デバイスと仮想デスクトップおよび RDS ベースのアプリケーションとの接続に関する特定のポリシーが設定されている場合があります。たとえば、グループ ポリシー設定を使用して、特定のユーザーの USB リダイレクトを無効にすることができます。関連情報については、VMware Horizon のドキュメントにある VMware Horizon 8 の『Horizon リモート デスクトップ機能と GPO』ガイドの USB 関連情報を参照してください。
URL リダイレクト	デフォルトではインストールされません。Horizon Client が、どの URL をユーザーのクライアント システムで開く代わりに仮想デスクトップまたはアプリケーションで処理するのかを決定し、仮想デスクトップまたは RDS ベースのアプリケーションを使用してそれらの URL を開くことを可能にします。
シリアル ポート リダイレクト	デフォルトではインストールされません。ユーザーのクライアント システムのシリアル ポートに接続されたデバイスをリダイレクトするので、それらのデバイスを仮想デスクトップまたは RDS ベースのアプリケーションで使用できます。
位置情報リダイレクト	デフォルトではインストールされません。クライアント システムの位置情報を、仮想デスクトップ上の Internet Explorer 11 で共有できるようにします。このオプションを使用すると、仮想マシンにエージェントをインストールするときに Horizon 位置情報リダイレクト オプションがインストールされます。インポートされた仮想マシンの準備ができたら、追加の要件が必要になります。詳細については、VMware Horizon のドキュメントにある VMware Horizon 8 の『Horizon リモート デスクトップ機能と GPO』ガイドの位置情報リダイレクトに関するコンテンツを参照してください。

オプション	説明
ヘルプデスク	ライブ デスクトップ セッションから、リアルタイムのパフォーマンス関連の詳細なデスクトップおよびセッションのメトリックを収集する機能を提供します。ライブ セッションは、アクティブ、アイドル、または切断されたセッションです。ログオフされたセッションは、これらのライブ セッションには該当しません。これらのメトリックは、仮想デスクトップの健全性のトラブルシューティングに役立ちます。これらのメトリックは、システムのヘルプ デスク関連機能の一部である第 1 世代テナント - ユーザー カード機能（別称：Horizon Cloud のヘルプ デスク）についてで使用されます。 **注：** このトグルをオフにすると、このイメージに基づくデスクトップ インスタンスまたはファーム マルチセッション インスタンスのライブ ユーザー セッションのパフォーマンス関連メトリックは収集されません。その結果、リアルタイムのライブ ユーザー セッション データはクラウド監視サービスに送信されません。そのため、このようなライブ ユーザー セッション データを、セッションのユーザー カードまたは Workspace ONE Intelligence コンソールのレポート内で報告することはできません。詳細については、第 1 世代テナント - ユーザー カード機能（別称：Horizon Cloud のヘルプ デスク）についておよび第 1 世代テナント - 第 1 世代 Horizon Universal Console の [レポート] ページを参照してください。 履歴セッション データを収集するには、[仮想マシンのインポート] ウィザードがデフォルトでインストールする Horizon Monitoring Service Agent に加え、Horizon Cloud 環境の [全般設定] ページでも監視セッション機能を有効にする必要があります。監視セッション機能が無効になっている場合、Workspace ONE Intelligence コンソールでは Horizon Cloud レポート用にセッションの履歴データを利用できません。監視セッション機能の設定を確認するには、第 1 世代の Horizon Universal Console で、[設定] - [全般設定] - [監視] の設定に移動します。
UNC パス リダイレクト	デフォルトではインストールされません。エンド ユーザーが仮想デスクトップからクライアントに UNC パス アクセスをリダイレクトして開く機能を提供します。 **注：** この機能は、マニフェスト バージョン 4136 以降を実行するポッドで使用可能です。

VDI デスクトップおよび RDS ホストに使用される上記のエージェント関連オプション、およびデフォルトで常にインストールされるすべての Horizon エージェント機能の詳細については、VMware Horizon 製品ドキュメントの Horizon Agent カスタム セットアップ オプション（VDI デスクトップに適用可能なオプション）および RDS ホストに対する Horizon Agent のカスタム セットアップ オプションを参照してください。

7 [インポート] をクリックします。

システムは仮想マシンの作成と構成を開始します。仮想マシンが [インポートされた仮想マシン] ページにパワーオン ステータス（緑色の点）およびエージェント ステータス「ペアなし」で一覧表示される最終ポイントで、プロセス全体が完了するまでに約 45 分かかる場合があります。

仮想マシンが Microsoft Azure クラウドで最初にインスタンス化されると、その名前が [インポートされた仮想マシン] ページに表示されます。ページに仮想マシンの最新のステータスを表示するには、更新アイコンを使用します。

仮想マシンの作成プロセスが失敗すると、失敗に関するシステム通知が生成され、[エージェントのバージョン] 列に [失敗] リンクが表示されます。そのリンクをクリックすると、[通知] ページが開いて、失敗の原因を確認することができます。

重要： Microsoft Azure China クラウドにイメージを作成する場合、プロセスが完了するまでに最大で 2 時間かかることがあります。このプロセスは地理的なネットワークの問題の影響を受け、必要なバイナリがクラウドの制御プレーンからダウンロードされるため、ダウンロードの速度が低下することがあります。

8 自動化プロセスが完了した後、ページを更新し、作成された仮想マシンがパワー オンを示す緑の点で表示され、エージェント ステータスが「ペアなし」であることを確認したら、仮想マシンに対して [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、Horizon Cloud とペアリングします。

自動化プロセスが完了した後、作成された仮想マシンはまだ Horizon Cloud とペアリングされません。次のスクリーンショットに示すように、仮想マシンの [エージェントのステータス] 列には、ペアなし(インポートに成功しました) と表示されます。

仮想マシンを選択し、[詳細] - [エージェント ペアリングをリセット]をクリックします。システムは仮想マシンをクラウド プレーンとペアリングします。この処理は完了まで数分かかることがあります。ペアリング処理中に仮想マシンが再起動され、そのエージェントのステータスが ペアなし(インポートに成功しました) から 不明、有効 に変わります。円形の矢印アイコンを使用して [インポートされた仮想マシン] ページを更新し、仮想マシンの現在のステータスを確認します。

結果

[エージェントのステータス] 列に 有効 および `19.3.0` などのエージェントのバージョンが表示されると、仮想マシンのペアリング処理は完了します。次のスクリーンショットは、ペアリング処理が完了した後の仮想マシンを示します。

次のステップ

- 壁紙などの設定や、仮想マシンによってエンド ユーザーに提供されるアプリケーションのインストールなど、イメージの Windows オペレーティング システムをカスタマイズします。仮想マシンのパブリック IP アドレスを有効にした場合は、Microsoft リモート デスクトップ接続などの RDP クライアントの [インポートされた仮想マシン] ページに表示される IP アドレスを使用して、作成された仮想マシンに接続できます。詳細については、インポートされた仮想マシンの Windows オペレーティング システムをカスタマイズを参照してください。
- ポッドがプロキシを使用するように構成されている場合は、VDI デスクトップ仮想マシンとファーム マルチセッション仮想マシンがプロキシを使用して構成されるようにする必要があります。
- Office 365 を含む Microsoft Windows 10 Enterprise マルチセッション オペレーティング システムのいずれかを選択した場合、Office 365 ProPlus に対する共有コンピュータのアクティベーションを有効にして、この仮想マシンに基づいて RDS ファームからプロビジョニングされる Office 365 アプリケーションをエンドユーザーが使用できるようにする必要がある可能性があります。詳細については、Microsoft のドキュメントのトピック 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を参照してください。
- [GPU を含める] で [はい] を選択した場合は、仮想マシンのオペレーティング システムにログインし、サポートされている NVIDIA グラフィックス ドライバをインストールして、Microsoft Azure の GPU 対応仮想マ

シンの GPU 機能を取得する必要があります。仮想マシンが作成されたらドライバをインストールします。[インポートされた仮想マシン] ページにはエージェントに関連したステータスがアクティブとして表示されます。Horizon Cloud on Microsoft Azure - インポートした GPU 対応仮想マシンに適切な GPU ドライバをインストールするを参照してください。

- NSX Cloud とその NSX-T Data Center コンポーネントの機能を、この仮想マシンに基づいてファーム マルチセッション インスタンスまたは VDI 割り当てデスクトップ インスタンスで使用する場合は、イメージを公開する前に仮想マシン オペレーティング システムにログインして NSX Agent をインストールする必要があります。Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッドおよび Horizon Cloud のインポートされたイメージ仮想マシンへの NSX Tools のインストールのトピックを参照して下さい。
- Horizon Cloud 環境に関連付けられたライセンスで Workspace ONE Assist for Horizon を使用する資格が付与されていて、この仮想マシンに基づくエンドユーザー仮想セッションでリモート サポート機能を使用する場合は、Workspace ONE Assist for Horizon エージェントをこの仮想マシンにインストールします。Workspace ONE Assist for Horizon の使用方法については、VMware Workspace ONE Assist ドキュメント領域にある該当のドキュメントを参照してください。
- インポート プロセスでは、デフォルトで VMware Dynamic Environment Manager クライアント コンポーネントがインストールされます。FlexEngine クライアント コンポーネントは、標準モードを使用してインストールされます。作成される仮想マシンのインストール パスは `C:\Program Files\VMware\Horizon Agents\User Environment Manager` です。このイメージに基づいて VDI デスクトップ仮想マシンおよびファーム マルチセッション仮想マシンで VMware Dynamic Environment Manager を使用する場合は、少なくとも SMB 2 が有効になっている Microsoft Azure サブスクリプションで別のファイル サーバを構成します。次に、そのファイル サーバを使用して VMware Dynamic Environment Manager を構成します。また、FlexEngine が標準モードでインストールされている場合に必要な GPO 設定も構成します。詳細については、Dynamic Environment Manager の製品ドキュメントの VMware Dynamic Environment Manager ドキュメントのトピックを参照してください。

[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に Windows イメージの最適化を決定する

[Marketplace からの仮想マシンのインポート] ウィザードには、インポートされた仮想マシンで Microsoft Windows オペレーティング システムをいくつかの特定の最適化を使用して構成するためのオプションがあります。このオプションを選択してイメージ作成プロセスを実行すると、仮想マシンは、その後 Horizon Cloud で公開アクションを実行するときに障害が発生しないように構成されます。このウィザードは、[仮想マシンのインポート] ウィザードで提供されるすべてのオペレーティング システムで使用できます。

重要： このウィザード オプションは、VMware オペレーティング システム最適化ツール (OSOT) を実行し、そのツールで仮想マシンを最適化することと同じではありません。[仮想マシンのインポート] ウィザードでオプションを有効にしても、VMware オペレーティング システム最適化ツールと同じ動作にはならず、仮想マシンで OSOT ツールが実行されません。

設定結果は、インポートされた仮想マシンにインストールされている Windows オペレーティング システムによって異なります。

すべての Windows オペレーティング システム

最適化オプションを選択すると、イメージ作成プロセスは、次のようにして Windows Update 機能を無効にします。

- 自動更新を防ぐためのレジストリ プロパティを追加します。プロパティの値は 1 に設定されます。

パス	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
プロパティ名	NoAutoUpdate
プロパティ値	1

- wuauserv サービスを停止し、無効にします。このシステム サービスは、Windows Update 機能によって使用されます。

Windows 10 クライアントおよび Windows 10 Enterprise マルチセッション オペレーティング システム以降

最適化オプションが選択されると、仮想マシンのインポート プロセスは次のスケジュール設定タスクを無効にします (存在する場合)。

[タスク スケジューラ] - [タスク スケジューラ ライブラリ]	タスク名
\Microsoft\Windows\UpdateOrchestrator	Schedule Scan USO_UxBroker

[デスクトップのインポート] ウィザードを使用する場合に [Windows ストア アプリを削除] オプションを使用する

[デスクトップのインポート] ウィザードには、ベース仮想マシン上の非マルチセッション Microsoft Windows 10 または 11 クライアントタイプ オペレーティング システムからほとんどの Windows ストア アプリを削除するオプションがあります。このオプションを選択すると、イメージ作成プロセスによって、イメージ公開プロセスが失敗する典型的な原因の多くを回避できる仮想マシンが作成されます。このオプションは特に、公開プロセスで Sysprep エラーが発生するリスクを低減するために使用されます。

注： ウィザードの [Windows ストア アプリを削除] トグルが有効になっている場合でも、システムに実装されているシステム定義の許可リストに基づいて、システムはデフォルトで一部の appx パッケージを保持します。この許可リストにある appx パッケージは、仮想マシンのインポート プロセスが終了しても、ベース仮想マシンにインストールされたままになります。appx パッケージのリストについては、このトピックの最後のセクションを参照してください。

Microsoft Windows 10 または 11 オペレーティング システムで仮想マシンを作成する場合、自動イメージ作成プロセスでは、Microsoft Azure Marketplace で利用可能なバージョンが使用されます。Microsoft ドキュメントの Windows 10 に含まれるさまざまなアプリについてで説明されているように、Microsoft Windows 10 クライアントタイプ システムでは通常、インストールされている Windows アプリおよびプロビジョニングされている Windows アプリ (c:\Program Files\WindowsApps ディレクトリにインストール済み) が含まれています。そのディレクトリにあらかじめインストールされているアプリケーションに加えて、オペレーティング システムの起動後、自動的に Microsoft ストアから Microsoft がおすすめアプリケーションと呼ぶさまざまな Microsoft ストア アプリケーションをダウンロードしてインストールします。これらのアプリのほとんどが Microsoft System

Preparation (Sysprep) ユーティリティに対して問題を生じる可能性があります。公開ワークフローは、そのユーティリティに依存します。これらの Windows アプリの多くが仮想マシンのオペレーティング システムに残っていると、Sysprep の問題が典型的に発生することが、業界では知られており、次の Microsoft リソースに記載されています。

- Microsoft KB 2769827
- Microsoft MVP の記事 615

これらのあらかじめインストールされている Microsoft ストア アプリケーションのほとんどを削除し、仮想マシンのオペレーティング システムによる新しいおすすめアプリケーションの自動サイレント インストールを防止するのは、イメージを公開するときにこのような Sysprep 問題が発生するリスクを低減することを目的としているためです。これらの Windows アプリは、オペレーティング システム内で AppX パッケージとして存在します。Windows ストア アプリを削除するオプションを選択すると、イメージ作成プロセスは、仮想マシンのオペレーティング システムで次の変更を実行します。

- 次のレジストリ値を設定して Microsoft ストアの自動ダウンロードおよび Microsoft コンシューマ エクスペリエンスを無効にします。

  表 6-1. [Windows ストア アプリを削除] オプションで設定されるレジストリ値

レジストリ パス	プロパティ名	値	詳細
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore`	`AutoDownload`	2	Windows ストア アプリの自動ダウンロードを無効にします。
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent`	`DisableWindowsConsumerFeatures`	1	Microsoft コンシューマ エクスペリエンスを無効にします。
`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\ContentDeliveryManager`	`SilentInstalledAppsEnabled`	0	推奨された Microsoft ストア アプリケーションの自動インストールを無効にして、Microsoft Windows がサイレント モードで自動的にダウンロードしてインストールするのを防ぎます。

- Microsoft ストア インストール サービス（`InstallService` サービス）を停止して無効にします。
- 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いるがシステム定義の許可リストにない AppX パッケージ（拡張子 `.appx` のファイル）を削除します。イメージ作成スクリプトは、最初に次のようなコマンドを使用して、仮想マシンのオペレーティング システムにある AppX パッケージの名前を取得します。

```
Get-AppxPackage -AllUsers | Select-Object -Property Name, PackageFullName | Sort-Object
-Property Name
```

  次に、システムの許可リストにない各 AppX パッケージについては、次のようなコマンドを使用して、除外された AppX パッケージを削除します。

```
Remove-AppxPackage  -Name appx-name
```

次にスクリプトは、以下のようなコマンドを使用して、除外された各 AppX パッケージに関連付けられている、アプリケーションがプロビジョニングするパッケージも削除します。

```
Get-AppxProvisionedPackage -Online | Where-Object {$_.DisplayName -like appx-name} |
Remove-AppxProvisionedPackage -Online
```

システム定義の許可された AppX パッケージ

デフォルトでは、以下の AppX パッケージがシステムの許可リストに含まれます。[Windows ストア アプリを削除] トグルが有効になっている場合でも、仮想マシンのインポート プロセスの終了時にこれらは作成されたベース仮想マシンに残ります。

```
Microsoft.DesktopAppInstallers
Microsoft.Messaging
Microsoft.MSPaint
Microsoft.Windows.Photos
Microsoft.MicrosoftStickyNotes
Microsoft.WindowsCalculator
Microsoft.WindowsCommunicationsApps
Microsoft.WindowsSoundRecorder
Microsoft.WindowsStore
Microsoft.Xbox.TCUI
Microsoft.XboxApp
Microsoft.XboxGameCallableUI
Microsoft.XboxGameOverlay
Microsoft.XboxGamingOverlay
Microsoft.XboxIdentityProvider
Microsoft.XboxSpeechToTextOverlay
Windows.CBSPreview
windows.immersivecontrolpanel
Windows.PrintDialog
```

Horizon Cloud の [Marketplace からの仮想マシンのインポート] ウィザードによって作成されたネットワーク セキュリティ グループ (NSG)

NSG を使用して、仮想マシンの NIC にアクセスできるネットワーク トラフィックのタイプを制御することは、Microsoft Azure のベスト プラクティスです。デフォルトでは、特定の Horizon Cloud ポッドに対して Horizon Universal Console の [Marketplace からの仮想マシンのインポート] ウィザードを初めて実行すると、仮想マシンと同じリソース グループに NSG が作成され、作成された仮想マシンの NIC がその NSG に接続されます。ウィザードの次回の実行では、最初の実行でパブリック IP アドレスを作成することを選択したかどうかに応じて、システムは後続の仮想マシンを同じ NSG に接続するか、2 番目の NSG を作成します。これらの NSG のルールによって、ウィザードで作成されたインポートされた仮想マシンに許可されるトラフィックが決まります。

Microsoft Azure ドキュメントで説明するように、Microsoft Azure では、ネットワーク セキュリティ グループ (NSG) は Azure Virtual Network (VNet) に接続されたリソースへのネットワーク トラフィックを管理します。NSG は、そのネットワーク トラフィックを許可または拒否するセキュリティ ルールを定義します。NSG によるネットワーク トラフィックのフィルタ方法の詳細については、Microsoft Azure のドキュメントで「Filter network traffic with network security groups」のトピックを参照してください。Microsoft Azure は、各 NSG が作成されると自動的にいくつかのデフォルトのルールを作成します。作成されるすべての NSG で、Microsoft Azure

はいくつかのインバウンド ルールとアウトバウンド ルールを 65000 以上の優先度で作成します。このような Microsoft Azure のデフォルトのルールは、ユーザーまたはシステムが Microsoft Azure で NSG を作成すると、Microsoft Azure によって自動的に作成されるので、このドキュメントのトピックでは説明されません。これらのルールは Horizon Cloud によって作成されるものではありません。これらのデフォルトのルールの詳細については、Microsoft Azure ドキュメントのデフォルトのセキュリティ ルールトピックを参照してください。

システムの [Marketplace からの仮想マシンのインポート] ワークフローが実行されると、インポートされた仮想マシンが作成されたのと同じリソース グループにこれらの NSG が作成されます。ウィザードが仮想マシンを作成するポッドのリソース グループに使用される名前付けパターンを確認するには、第 1 世代テナント - 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。

[パブリック IP アドレスを有効にする] がオンの場合

ウィザードの [パブリック IP アドレスを有効にする] トグルをオンにして作成された仮想マシンの場合、システムはそれらの仮想マシンを `HCS-Imported-VM-NSG` という名前の NSG に接続します。Microsoft Azure によってすべての NSG で作成されるデフォルトのルールに加えて、この NSG には RDP ポートを使用する受信トラフィックを許可する受信ルールがあります。[パブリック IP アドレスを有効にする] オプションの目的は、パブリック インターネット経由で仮想マシンにログインする機能を提供し、仮想マシンをカスタマイズできるようにすることです。このため、この受信ルールにより、RDP を使用してインターネット経由で仮想マシンにログインできます。

表 6-2. HCS-Imported-VM-NSG の受信セキュリティ ルール

優先順位	名前	ポート	プロトコル	ソース	送信先	アクション
300	AllowRDP	3389	TCP	任意	任意	許可

[パブリック IP アドレスを有効にする] がオフの場合

ウィザードの [パブリック IP アドレスを有効にする] トグルをオフにして作成された仮想マシンの場合、システムはそれらの仮想マシンを `HCS-Imported-VM-NSG-Basic` という名前の NSG に接続します。この NSG には、NSG の作成時に Microsoft Azure によって作成されたデフォルトのルールのみが含まれます。このような Microsoft Azure のデフォルトのルールは、Microsoft Azure によって自動的に作成されるため、このドキュメント トピックでは説明しません。これらのデフォルトのルールの詳細については、Microsoft Azure ドキュメントのデフォルトのセキュリティ ルールトピックを参照してください。

インポートされた仮想マシンの Windows オペレーティング システムをカスタマイズ

インポートされた仮想マシンが作成され、それを Horizon Cloud とペアリングしたら、公開イメージに変換する前に、仮想マシンのゲスト Windows オペレーティング システム (OS) をカスタマイズし、イメージで必要なものをインストールして構成します。仮想マシンがこのカスタマイズを完了した後、ゴールド イメージと呼ばれることもあります。これは、そのイメージに基づいて、エンド ユーザーのデスクトップとリモート アプリケーションのビジネス ニーズを満たすすべての項目でイメージが構成されることを示しています。

仮想マシンをさらにカスタマイズする手順については、次のリンクを参照してください。VMware Blast Extreme を使用するための構成を向上させるためにイメージ仮想マシンをさらに調整するには、Horizon Cloud ファームとデスクトップから最適なリモート エクスペリエンス パフォーマンスを引き出すためにゴールド イメージで実行すべき 5 つの重要な手順のガイダンスに従うことをお勧めします。また、VMware Blast Extreme Optimization Guide を確認し、コーデック オプションの推奨事項に従って、イメージのコーデック オプションに対する追加の調整を行います。

[仮想マシンのインポート] ウィザードで次のオプションを使用していない場合、または基本イメージ仮想マシンを手動で作成した場合に、Sysprep の問題を回避する方法について

[仮想マシンのインポート] ウィザードを使用して基本イメージを作成し、ウィザードで次のリストされたオプションを有効にした場合、インポートされた仮想マシンがシールドされたイメージに変換されたときに実行される、Microsoft Windows システム準備 (Sysprep) プロセスで確認された一般的な問題を回避するために、仮想マシンが構成されました。

- [Windows イメージを最適化] トグル — ウィザードで選択可能なすべてのオペレーティング システムのウィザードで使用可能。このオプションには、[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に Windows イメージの最適化を決定する に記載されています。
- [Windows ストア アプリを削除] トグル — Windows 10 または 11 クライアント タイプのオペレーティング システムのウィザードで使用可能。このオプションには、[デスクトップのインポート] ウィザードを使用する場合に [Windows ストア アプリを削除] オプションを使用する に記載されています。

仮想マシンのインポート ウィザードでこれらのオプションを使用していない場合、またはインポートされた仮想マシンを手動で作成した場合は、シーリング中に、特に Microsoft Windows システム準備 (Sysprep) プロセスに関連する問題が発生することがあります。以下にリンクされているトピックの手順を実行して、インポートされた仮想マシンを公開済みで、シールドされたイメージに変換する前に、次のいくつかの方法を実行することもできます。

- 基本イメージ仮想マシンのサービスおよびレジストリ キーを、[Windows イメージを最適化] および [Windows ストア アプリを削除] トグルを [はい] に設定したときと同じシステム設定に手動で設定します。上記のリストにあるリンクを使用して、これらの設定を参照してください。
- Microsoft KB 2769827 および Microsoft MVP の記事 615 の説明に従って、Microsoft Windows `appx` パッケージを削除します。Windows 10 または 11 では、すべてのアカウントで `appx` パッケージの削除手順を実行して、すべてのアカウントから、それぞれ同じアプリケーションを削除します。すべてのアカウントで `appx` の削除手順を実行するまではアカウントやプロファイルをイメージから削除しないでください。[仮想マシンのインポート] ウィザードの [Windows ストア アプリを削除] トグルを使用しているときにイメージ作成プロセスで実行されるパッケージ削除コマンドについて詳しくは、[デスクトップのインポート] ウィザードを使用する場合に [Windows ストア アプリを削除] オプションを使用するを参照してください。

- VMware Windows オペレーティング システム最適化ツール ガイド に記載されている手順に従ってください。このガイドは他の VMware 仮想デスクトップ製品の使用を想定して書かれたもので、ご利用の Horizon Cloud 環境でサポートされているものとは異なる Windows オペレーティング システムについての記述が含まれていますが、仮想マシンで VMware OS 最適化ツール (OSOT) を使用する方法の詳細が記載されています。

  重要： 広く使用されていますが、VMware OS Optimization Tool (OSOT) はいわゆる VMware Flings であるため、そのサポート プロセスは VMware Flings 利用規約 に準拠していることに注意してください。Flings は、現状のまま提供されており、VMware サポート リクエスト プロセスや VMware Horizon のサービス レベル アグリーメントの対象ではありません。この文書の執筆時点で、VMware OS Optimization Tool を使用する際にヘルプを得る方法は、VMware Flings サイトのその場所にある [Comments] 領域を使用することです。

Microsoft Windows クライアント オペレーティング システムを搭載した Horizon Cloud のインポートされた仮想マシンの場合：組織のニーズに合わせた仮想マシンのカスタマイズ

Microsoft Windows クライアントタイプ オペレーティング システムで構築された仮想マシンがインポートされ、それを Horizon Cloud とペアリングしたら、公開イメージに変換する前に、Windows ゲスト オペレーティング システム (OS) をカスタマイズし、エンド ユーザーの VDI デスクトップに配置するものをすべてインストールして構成します。この時点で、VDI デスクトップで使用可能にするすべてのサードパーティ アプリケーションをインストールします。同じくこの時点で、組織のニーズ応じて必要となる特別なドライバのインストール、壁紙の適用、デフォルトの色とフォントの設定、タスクバー設定の構成、そのような他の OS レベルの項目など、Windows ゲスト OS でのその他のカスタマイズも実行します。カスタマイズ前の仮想マシンは、イメージまたは基本イメージと呼ばれることがあります。カスタマイズ後、仮想マシンはゴールド イメージと呼ばれることがあります。

[インポートされた仮想マシン] ページでインポートされた仮想マシンのエージェントに関連するステータスがアクティブであることが示されたら、RDP ソフトウェアを使用してそれに接続し、基盤となるオペレーティング システムにアプリケーションをインストールします。

前提条件

[インポートされた仮想マシン] ページで、仮想マシンに対してエージェントに関連するステータスがアクティブになっていることを確認します。このステータスを取得するには、仮想マシンで [インポートされた仮想マシン] ページの [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ます。このアクションは、[詳細] ドロップダウン リストにあります。

[インポートされた仮想マシン] ページに表示される仮想マシンの IP アドレスを取得します。

注： Microsoft リモート デスクトップ クライアントを RDP ソフトウェアとして使用して仮想マシンに接続する場合は、それが最新のバージョンであることを確認してください。たとえば、Windows 7 オペレーティング システムのデフォルトの RDP ソフトウェアのバージョンはこの条件を満たしていません。バージョンは、バージョン 8 以降である必要があります。

仮想マシンの作成方法に応じて、仮想マシンのゲスト Windows オペレーティング システムにログインするために、認証情報（ユーザー名とパスワード）の少なくとも 1 つがあることを確認します。

仮想マシンの作成方法	ログインに使用する認証情報
[インポートされた仮想マシン] ページから、仮想マシンのインポート ウィザードを実行します。	2019 年 12 月のサービス リリース日以降、[仮想マシンのインポート] ウィザードは、作成プロセスの最後に、ウィザードで作成された仮想マシンを指定された Active Directory ドメインに参加させるか、仮想マシンをドメインに参加させないかのオプションを提供します。 ■ ウィザードの [ドメイン参加] トグルを有効にして仮想マシンが作成された場合、指定された Active Directory ドメインのドメイン アカウントの認証情報を使用するか、ウィザードで指定されたローカル管理者アカウントを使用できます。 ■ ウィザードの [ドメイン参加] トグルをオフにして仮想マシンが作成された場合、ウィザードで指定されたローカル管理者アカウントを使用する必要があります。この場合、仮想マシンはドメインに参加していないため、ログインするためのアクセス権を持つ唯一のアカウントがローカル管理者アカウントになります。
手動による準備手順 。	通常、仮想マシンを手動で構築するときに、仮想マシンを Active Directory ドメインに加える必要はありません。その仮想マシンにログインするには、次のいずれかの方法を使用します。 ■ 手動で構築された仮想マシンが Microsoft Azure ポータルで作成されたときに指定されたローカル管理者アカウントの認証情報。 ■ その仮想マシンを Active Directory ドメインに手動で参加させた場合、そのドメインのドメインアカウントの認証情報。

重要： ポッド マニフェスト バージョン 1230 以降では、ドメイン アカウントはエージェント ソフトウェアがインストールされているドメイン参加イメージ仮想マシンに直接接続できます。ポッド マニフェスト 1230 より前のバージョンでは、ドメインに参加した仮想マシンにインストールされたエージェント ソフトウェアにより、ドメイン アカウントをその仮想マシンに直接接続できませんでした。2298 より前のマニフェストはサポート対象外であり、ナレッジベースの記事 KB86476 の記載に従って更新する必要があります。

手順

1 仮想マシンのオペレーティング システムに接続するには、RDP ソフトウェアで仮想マシンの IP アドレスを使用します。

   - パブリック IP アドレスを使用して仮想マシンを作成した場合は、その IP アドレスを RDP ソフトウェアで使用できます。
   - 仮想マシンにプライベート IP アドレスがある場合は、次の 2 つの方法のいずれかを使用して RDP を実装する必要があります。
     - パブリック IP アドレスを持つ Microsoft Azure サブスクリプション内で別の仮想マシンを使用し、インポートされた仮想マシンに対してアウトバウンド RDP を実行する。
     - VPN と RDP を企業のネットワーク経由で仮想マシン内で使用する

   注： エージェントに関連するソフトウェア コンポーネントを実行している仮想マシンにアクセスする場合、リモート デスクトップ クライアントのバージョンは 8 以降である必要があります。そうでないと、接続に失敗します。最新のリモート デスクトップ クライアントを使用することをお勧めします。

2 この前提条件に記述されるようにして、、認証情報 (ユーザー名とパスワード) を使用して Windows オペレーティング システムにログインします。

仮想マシンの作成時に [イメージのインポート] ウィザードで指定したローカル管理者アカウントの認証情報を使用する場合は、ユーザー名を `\username` と入力します。

注： 仮想マシンがこの前提条件で記述されているようにするようにしてドメインに参加している仮想マシンであり、ローカル管理者アカウントではなくドメイン アカウントを使用したい場合は、ユーザー名を *ドメイン* `\username` と入力します。ここで *ドメイン* はドメイン名です。

3 オペレーティング システムにログインしているときに、エンド ユーザーが VDI デスクトップ環境で実行できるようにするサードパーティのアプリケーションまたはドライバをインストールします。

4 オペレーティング システムで、VDI デスクトップで使用するカスタム ドライバをインストールします。

5 カスタムの壁紙の追加、デフォルトのフォント、色、テーマの設定、タスクバーのデフォルト設定の調整など、VDI デスクトップに必要なカスタマイズや構成を行います。

6 仮想マシンのゲスト OS の最終調整が完了したら、オペレーティング システムからログアウトします。

次のステップ

目的のビジネス シナリオに基づいてイメージを最適化します。Horizon Cloud ファームとデスクトップから最適なリモート エクスペリエンス パフォーマンスを引き出すためにゴールド イメージで実行すべき 5 つの重要な手順のガイダンスを参照してください。

ベスト プラクティスに従って仮想マシンを最適化し、プロセスで sysprep やその他のエラーが発生しないようにして、ゴールド イメージを Horizon Cloud で割り当て可能なイメージに変換します。これは、イメージの公開またはシーリングとも呼ばれます。インポートされた仮想マシンの Windows オペレーティング システムをカスタマイズを参照してください。

構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の割り当て可能なイメージに変換するに記載されている手順を使用して、ゴールド イメージを割り当て可能なイメージに変換します。

Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムを搭載した Horizon Cloud のインポートされた仮想マシンの場合：組織のニーズに合わせた仮想マシンのカスタマイズ

Microsoft Windows 10 Enterprise または Windows 11 Enterprise マルチセッション オペレーティング システムで構築された仮想マシンがインポートされ、それを Horizon Cloud とペアリングしたら、公開イメージに変換する前に、ゲスト オペレーティング システム (OS) をカスタマイズし、エンド ユーザーのリモート アプリケーションとセッションベースのデスクトップがプロビジョニングされる元の RDSH 仮想マシンに配置するものをすべてインストールして構成します。この時点で、セッションベースのデスクトップで使用できるようにする、またはリモート アプリケーションとして割り当て可能にするすべてのサードパーティ アプリケーションをインストールします。同じくこの時点で、組織のニーズ応じて必要となる特別なドライバのインストール、壁紙の適用、デフォルトの色とフォントの設定、タスクバー設定の構成、そのような他の OS レベルの項目など、Windows ゲスト OS での

その他のカスタマイズも実行します。カスタマイズ前の仮想マシンは、イメージまたは基本イメージと呼ばれることがあります。カスタマイズ後、仮想マシンはゴールド イメージと呼ばれることがあります。

ヒント: Microsoft のドキュメント FAQ で説明されているように、Microsoft Windows 10 または Windows 11 Enterprise マルチセッションは、以前は Microsoft Windows Server オペレーティング システム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。Microsoft Windows 10 または 11 Enterprise マルチセッションは RDSH タイプのオペレーティング システムであるため、Horizon Cloud テナント アカウント構成で使用できるようになっている場合は、Horizon Cloud RDSH に該当するワークフローに表示されます。

[インポートされた仮想マシン] ページでインポートされた仮想マシンのエージェントに関連するステータスがアクティブであることが示されたら、RDP ソフトウェアを使用してそれに接続し、基盤となるオペレーティング システムにアプリケーションをインストールします。

前提条件

インポートされた仮想マシンが、オペレーティング システムのカスタマイズの一環として、デフォルトで Office 365 ProPlus を含む Microsoft Windows 10 または 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 ドキュメントのトピック 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の説明に従って、その Office 365 ProPlus を共有コンピュータのアクティベーションで構成する必要がある可能性があります。Microsoft のドキュメントのトピックを参照して、共有コンピュータのアクティベーションで Office 365 ProPlus を構成する方法を決定します。

[インポートされた仮想マシン] ページで、仮想マシンに対してエージェントに関連するステータスがアクティブになっていることを確認します。このステータスを取得するには、仮想マシンで [インポートされた仮想マシン] ページの [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ます。このアクションは、[詳細] ドロップダウン リストにあります。

[インポートされた仮想マシン] ページに表示される仮想マシンの IP アドレスを取得します。

ヒント: Microsoft リモート デスクトップ クライアントを RDP ソフトウェアとして使用して仮想マシンに接続する場合は、それが最新のバージョンであることを確認してください。バージョンは、バージョン 8 以降である必要があります。

仮想マシンの作成方法に応じて、仮想マシンのゲスト Windows オペレーティング システムにログインするために、認証情報（ユーザー名とパスワード）の少なくとも 1 つがあることを確認します。

仮想マシンの作成方法	ログインに使用する認証情報
[インポートされた仮想マシン] ページから、仮想マシンのインポート ウィザードを実行します。	[仮想マシンのインポート] ウィザードは、作成プロセスの最後に、ウィザードで作成された仮想マシンを指定された Active Directory ドメインに参加させるか、仮想マシンをドメインに参加させないかのオプションを提供します。 ■ ウィザードの [ドメイン参加] トグルを有効にして仮想マシンが作成された場合、指定された Active Directory ドメインのドメイン アカウントの認証情報を使用するか、ウィザードで指定されたローカル管理者アカウントを使用できます。 ■ ウィザードの [ドメイン参加] トグルをオフにして仮想マシンが作成された場合、ウィザードで指定されたローカル管理者アカウントを使用する必要があります。この場合、仮想マシンはドメインに参加していないため、ログインするためのアクセス権を持つ唯一のアカウントがローカル管理者アカウントになります。
Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートする の手動の準備手順。	通常、仮想マシンを手動で構築するときに、仮想マシンを Active Directory ドメインに加える必要はありません。その仮想マシンにログインするには、次のいずれかの方法を使用します。 ■ 手動で構築された仮想マシンが Microsoft Azure ポータルで作成されたときに指定されたローカル管理者アカウントの認証情報。 ■ その仮想マシンを Active Directory ドメインに手動で参加させた場合、そのドメインのドメインアカウントの認証情報。

手順

1 仮想マシンのオペレーティング システムに接続するには、RDP ソフトウェアで仮想マシンの IP アドレスを使用します。

- パブリック IP アドレスを使用して仮想マシンを作成した場合は、その IP アドレスを RDP ソフトウェアで使用できます。
- 仮想マシンにプライベート IP アドレスがある場合は、次の 2 つの方法のいずれかを使用して RDP を実装する必要があります。
  - パブリック IP アドレスを持つ Microsoft Azure サブスクリプション内で別の仮想マシンを使用し、インポートされた仮想マシンに対してアウトバウンド RDP を実行する。
  - VPN と RDP を企業のネットワーク経由で仮想マシン内で使用する

注意: Microsoft リモート デスクトップ クライアントを RDP ソフトウェアとして使用して仮想マシンに接続する場合は、それが最新のバージョンであることを確認してください。バージョンは、バージョン 8 以降である必要があります。

2 この前提条件に記述されるように、認証情報 (ユーザー名とパスワード) を使用して Windows オペレーティング システムにログインします。

仮想マシンの作成時に [イメージのインポート] ウィザードで指定したローカル管理者アカウントの認証情報を使用する場合は、ユーザー名を `\username` と入力します。

注： 仮想マシンがこの前提条件で記述されているように、ドメインに参加している仮想マシンであり、ローカル管理者アカウントではなくドメイン アカウントを使用したい場合は、ユーザー名を *ドメイン*`\username` と入力します。ここで *ドメイン* はドメイン名です。

3 オペレーティング システムにログインしているときに、エンド ユーザーが セッションベースのデスクトップ内で使用できるようにする、またはリモート アプリケーションとして実行できるようにする、サードパーティのアプリケーションやドライバをインストールします。

4 オペレーティング システムで、RDSH ホストで使用できるようにするカスタム ドライバをインストールします。

5 カスタムの壁紙の追加、デフォルトのフォント、色、テーマの設定、タスクバーのデフォルト設定の調整など、セッションベースのデスクトップに必要なカスタマイズや構成を行います。

6 仮想マシンのゲスト OS の最終調整が完了したら、オペレーティング システムからログアウトします。

次のステップ

仮想マシンが、デフォルトで Office 365 ProPlus を含む Microsoft Windows 10 または 11 Enterprise マルチセッションの選択肢のいずれかに基づいている場合は、追加の手順が必要になる可能性があります。Microsoft ドキュメントのトピック Office 365 ProPlus に対する共有コンピューターのライセンス認証の概要の説明に従って、その Office 365 ProPlus を共有コンピュータのアクティベーションで構成する必要がある可能性があります。Microsoft のドキュメントのトピックを参照して、共有コンピュータのアクティベーションで Office 365 ProPlus を構成する方法を決定し、自分の状況に適した手法を使用します。

目的のビジネス シナリオに基づいてイメージを最適化します。Horizon Cloud ファームとデスクトップから最適なリモート エクスペリエンス パフォーマンスを引き出すためにゴールド イメージで実行すべき 5 つの重要な手順のガイダンスを参照してください。

ベスト プラクティスに従って仮想マシンを最適化し、プロセス中に sysprep やその他のエラーが発生しないようにして、ゴールド イメージを Horizon Cloud で割り当て可能なイメージに変換します。これは、イメージの公開またはシーリングとも呼ばれます。インポートされた仮想マシンの Windows オペレーティング システムをカスタマイズを参照してください。

構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の割り当て可能なイメージに変換するに記載されている手順を使用して、ゴールド イメージを割り当て可能なイメージに変換します。

Microsoft Windows Server オペレーティング システムを搭載した Horizon Cloud のインポートされた仮想マシンの場合：組織のニーズに合わせた仮想マシンのカスタマイズ

Microsoft Windows Server オペレーティング システムで構築された仮想マシンがインポートされ、それを Horizon Cloud とペアリングしたら、Horizon Cloud の公開イメージに変換する前、公開イメージに変換する前に、ゲスト オペレーティング システム (OS) をカスタマイズし、エンド ユーザーのリモート アプリケーションとセッションベースのデスクトップがプロビジョニングされる元の RDSH 仮想マシンに配置するものをすべてインストールして構成します。同じくこの時点で、組織のニーズ応じて必要となる特別なドライバのインストール、壁紙の適用、デフォルトの色とフォントの設定、タスクバー設定の構成、そのような他の OS レベルの項目など、Windows ゲスト OS でのその他のカスタマイズも実行します。カスタマイズ前の仮想マシンは、イメージまたは基本イメージと呼ばれることがあります。カスタマイズ後、仮想マシンはゴールド イメージと呼ばれることがあります。

[インポートされた仮想マシン] ページでインポートされた仮想マシンのエージェントに関連するステータスがアクティブであることが示されたら、RDP ソフトウェアを使用してそれに接続し、基盤となるオペレーティング システムにアプリケーションをインストールします。

RDSH サーバにアプリケーションを直接インストールする場合の Microsoft のベスト プラクティスについては、TechNet Magazine の記事「Learn How to Install Applications on an RD Session Host Server」を参照してください。

前提条件

[インポートされた仮想マシン] ページで、仮想マシンに対してエージェントに関連するステータスがアクティブになっていることを確認します。このステータスを取得するには、仮想マシンで [インポートされた仮想マシン] ページの [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ます。このアクションは、[詳細] ドロップダウン リストにあります。

[インポートされた仮想マシン] ページに表示される仮想マシンの IP アドレスを取得します。

注： Microsoft リモート デスクトップ クライアントを RDP ソフトウェアとして使用して仮想マシンに接続する場合は、それが最新のバージョンであることを確認してください。たとえば、Windows 7 オペレーティング システムのデフォルトの RDP ソフトウェアのバージョンはこの条件を満たしていません。バージョンは、バージョン 8 以降である必要があります。

仮想マシンの作成方法に応じて、仮想マシンのゲスト Windows オペレーティング システムにログインするために、認証情報（ユーザー名とパスワード）の少なくとも 1 つがあることを確認します。

仮想マシンの作成方法	ログインに使用する認証情報
[インポートされた仮想マシン] ページから、仮想マシンのインポート ウィザードを実行します。	2019 年 12 月のサービス リリース日以降、[仮想マシンのインポート] ウィザードは、作成プロセスの最後に、ウィザードで作成された仮想マシンを指定された Active Directory ドメインに参加させるか、仮想マシンをドメインに参加させないかのオプションを提供します。 ■ ウィザードの [ドメイン参加] トグルを有効にして仮想マシンが作成された場合、指定された Active Directory ドメインのドメイン アカウントの認証情報を使用するか、ウィザードで指定されたローカル管理者アカウントを使用できます。 ■ ウィザードの [ドメイン参加] トグルをオフにして仮想マシンが作成された場合、ウィザードで指定されたローカル管理者アカウントを使用する必要があります。この場合、仮想マシンはドメインに参加していないため、ログインするためのアクセス権を持つ唯一のアカウントがローカル管理者アカウントになります。
手動による準備手順 。	通常、仮想マシンを手動で構築するときに、仮想マシンを Active Directory ドメインに加える必要はありません。その仮想マシンにログインするには、次のいずれかの方法を使用します。 ■ 手動で構築された仮想マシンが Microsoft Azure ポータルで作成されたときに指定されたローカル管理者アカウントの認証情報。 ■ その仮想マシンを Active Directory ドメインに手動で参加させた場合、そのドメインのドメインアカウントの認証情報。

重要： ポッド マニフェスト バージョン 1230 以降では、ドメイン アカウントはエージェント ソフトウェアがインストールされているドメイン参加イメージ仮想マシンに直接接続できます。ポッド マニフェスト 1230 より前のバージョンでは、ドメインに参加した仮想マシンにインストールされたエージェント ソフトウェアにより、ドメイン アカウントをその仮想マシンに直接接続できませんでした。2298 より前のマニフェストはサポート対象外であり、ナレッジベースの記事 KB86476 の記載に従って更新する必要があります。

手順

1 仮想マシンのオペレーティング システムに接続するには、RDP ソフトウェアで仮想マシンの IP アドレスを使用します。

- パブリック IP アドレスを使用して仮想マシンを作成した場合は、その IP アドレスを RDP ソフトウェアで使用できます。
- 仮想マシンにプライベート IP アドレスがある場合は、次の 2 つの方法のいずれかを使用して RDP を実装する必要があります。
  - パブリック IP アドレスを持つ Microsoft Azure サブスクリプション内で別の仮想マシンを使用し、インポートされた仮想マシンに対してアウトバウンド RDP を実行する。
  - VPN と RDP を企業のネットワーク経由で仮想マシン内で使用する

注： エージェントに関連するソフトウェア コンポーネントを実行している仮想マシンにアクセスする場合、リモート デスクトップ クライアントのバージョンは 8 以降である必要があります。そうでないと、接続に失敗します。最新のリモート デスクトップ クライアントを使用することをお勧めします。

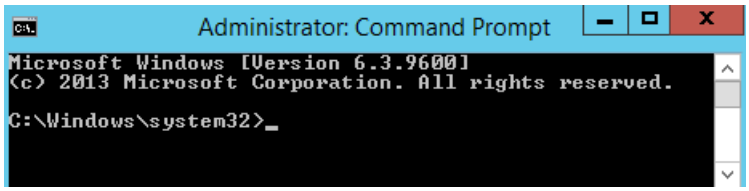
2 この前提条件に記述されるようにして、、認証情報 (ユーザー名とパスワード) を使用して Windows オペレーティング システムにログインします。

仮想マシンの作成時に [イメージのインポート] ウィザードで指定したローカル管理者アカウントの認証情報を使用する場合は、ユーザー名を `\username` と入力します。

注： 仮想マシンがこの前提条件で記述されているようにするようにしてドメインに参加している仮想マシンであり、ローカル管理者アカウントではなくドメイン アカウントを使用したい場合は、ユーザー名を *ドメイン* `\username` と入力します。ここで *ドメイン* はドメイン名です。

3 オペレーティング システムにログインしている場合は、以下の手順に従ってマルチユーザー RDS デスクトップ環境で実行するサードパーティ アプリケーションまたはドライバをインストールします。

a Windows サーバ オペレーティング システムで、[スタート] を右クリックして [コマンド プロンプト（管理者)] をクリックし、管理者としてコマンド プロンプトを開きます。



b そのコマンド プロンプトで `change user /query` コマンドを発行して、サーバの現在のインストール モードを確認します。

応答「`Applicaton EXECUTE mode is enabled`」は、サーバが RD-Execute モードであることを示します。

c そのコマンド プロンプトで `change user /install` コマンドを実行して、サーバを RD-Install モードに切り替えます。

```
C:\Windows\system32>change user /install
User session is ready to install applications.

C:\Windows\system32>_
```

Microsoft のベスト プラクティスのドキュメントで説明するように、RD-Install はアプリケーションをマルチユーザー環境で実行できるようにインストールする特別なインストール モードです。

d エンド ユーザーに提供するサードパーティのユーザー アプリケーションを、RDS デスクトップに、またはリモート アプリケーションとしてインストールします。

e アプリケーションのインストールが完了したら、コマンド プロンプト ウィンドウに戻り、`change user /execute` コマンドを実行してサーバを RD-Execute モードに切り替えます。

```
C:\Windows\system32>change user /execute
User session is ready to execute applications.

C:\Windows\system32>_
```

4 オペレーティング システムで、RDS デスクトップで使用するカスタム ドライバをインストールします。

5 カスタムの壁紙の追加、デフォルトのフォント、色、テーマの設定、タスクバーのデフォルト設定の調整など、RDS デスクトップに必要なカスタマイズや構成を行います。

6 仮想マシンのゲスト OS の最終調整が完了したら、オペレーティング システムからログアウトします。

次のステップ

目的のビジネス シナリオに基づいてイメージを最適化します。Horizon Cloud ファームとデスクトップから最適なリモート エクスペリエンス パフォーマンスを引き出すためにゴールド イメージで実行すべき 5 つの重要な手順のガイダンスを参照してください。

ベスト プラクティスに従って仮想マシンを最適化し、プロセスで sysprep やその他のエラーが発生しないようにして、ゴールド イメージを Horizon Cloud で割り当て可能なイメージに変換します。これは、イメージの公開またはシーリングとも呼ばれます。インポートされた仮想マシンの Windows オペレーティング システムをカスタマイズを参照してください。

構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の割り当て可能なイメージに変換するに記載されている手順を使用して、ゴールド イメージを割り当て可能なイメージに変換します。

Horizon Cloud ファームとデスクトップから最適なリモート エクスペリエンス パフォーマンスを引き出すためにゴールド イメージで実行すべき 5 つの重要な手順

エンド ユーザーによってそのニーズは異なります。Horizon Cloud 環境で使用するためにゴールド イメージをカスタマイズした後、そのイメージに基づく割り当てられたデスクトップとアプリケーションを使用するときにエンド ユーザーに最適なパフォーマンスが提供されることを確認する必要があります。このトピックでは、エンド ユーザーの個人設定に基づいて最適なパフォーマンスを実現するのに役立ついくつかの規範的なガイダンスを提供します。

このトピックには次のセクションが含まれています。

■ 5 つの重要な手順

- オプション：ユーザー エクスペリエンス監視ツールのインストール
- さまざまなエンド ユーザーの個人設定とワークロード タイプで使用されるファームのコーデックの選択と仮想マシン シリーズのサイズに関する推奨事項

ヒント: 他のソースの中でも、これらの 5 つの重要な手順は、VMware Digital Workspace Tech Zone の『VMware Blast Extreme Optimization Guide』および『Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop』に詳しく記載されています。

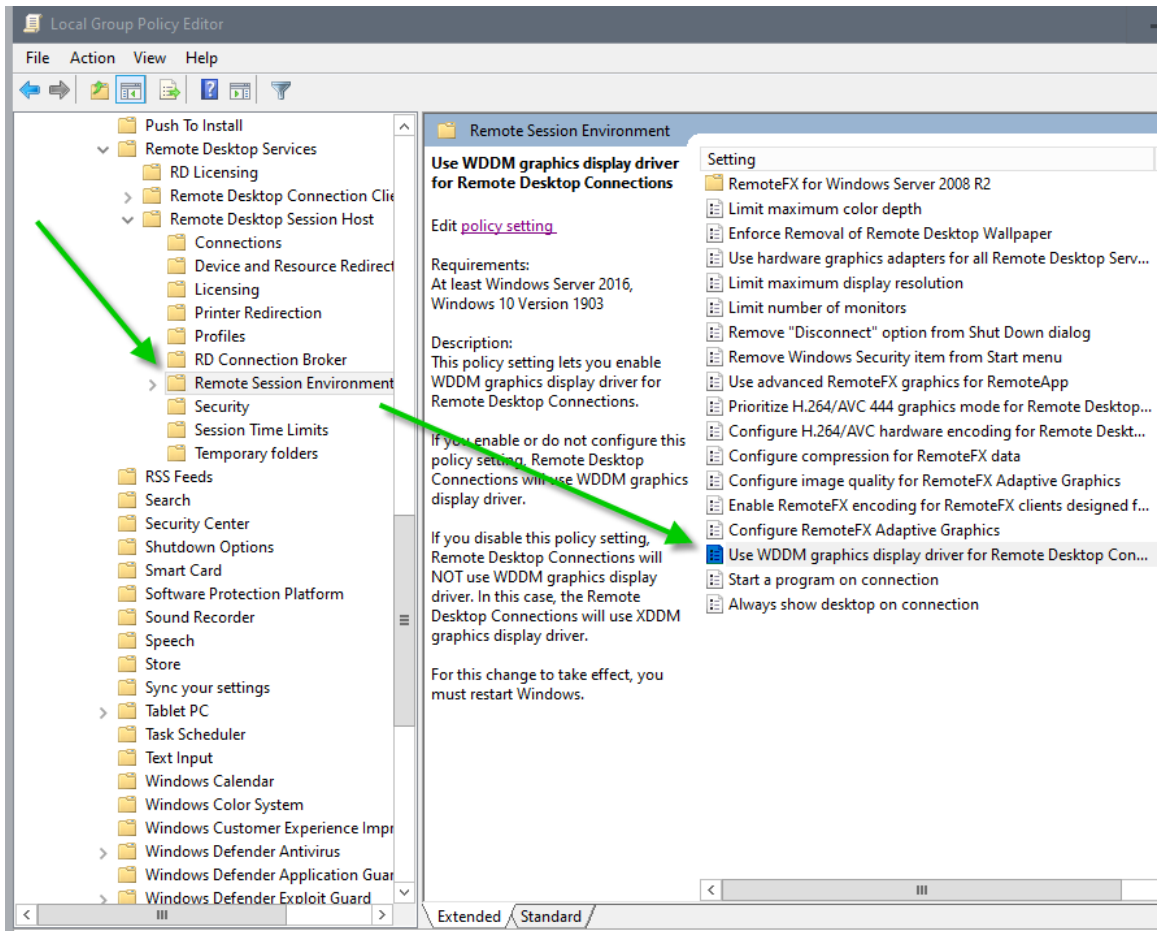
5 つの重要な手順

1 最適なリモート エクスペリエンスを提供できるようにイメージの Microsoft Windows オペレーティング システムを準備するには、Windows OS Optimization Tool for VMware Horizon をゴールド イメージ仮想マシンにダウンロードし、ツールを実行して、ツールの画面上のアドバイスに従ってください。

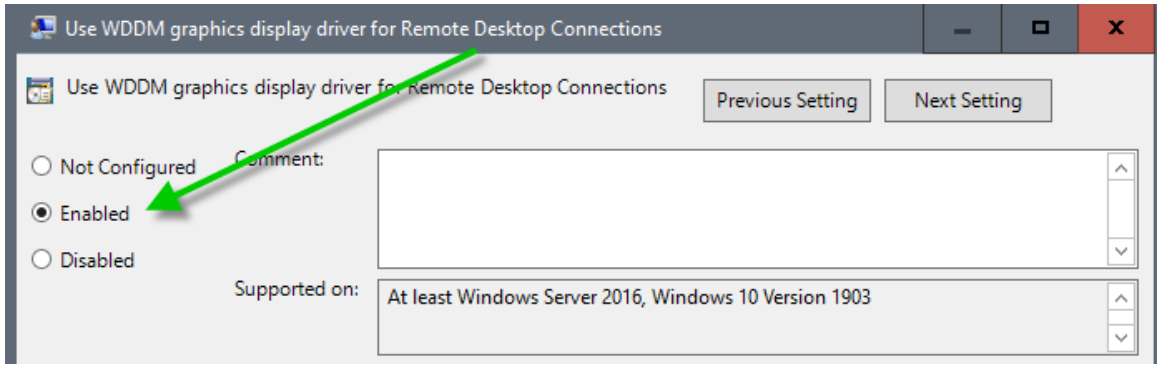
VMware Customer Connect から Windows OS Optimization Tool for VMware Horizon をダウンロードするには、VMware Customer Connect ログインが必要です。

2 ゴールド イメージのオペレーティング システムで、リモート デスクトップ接続に WDDM グラフィックス ディスプレイ ドライバを使用する設定を有効にします。この設定は、複数の方法で有効にできます。設定を有効にする 1 つの方法は、ローカル グループ ポリシー エディタを使用することです。

a ローカル グループ ポリシー エディタで、[ローカル コンピュータ ポリシー] - [管理テンプレート] - [Windows コンポーネント] - [リモート デスクトップ サービス] - [リモート デスクトップ セッション ホスト] - [リモート セッション環境] の順に移動します。次のスクリーンショットにこの場所を示します。



b [リモート デスクトップ接続に WDDM グラフィックス ディスプレイ ドライバを使用する] という名前のポリシーを [有効] に設定します。



変更を有効にするには、WDDM グラフィックス ディスプレイ ドライバを有効にした後に仮想マシンを再起動する必要があります。

3 仮想マシンで、予想されるエンドユーザーのワークロードに適したコーデックを設定します。

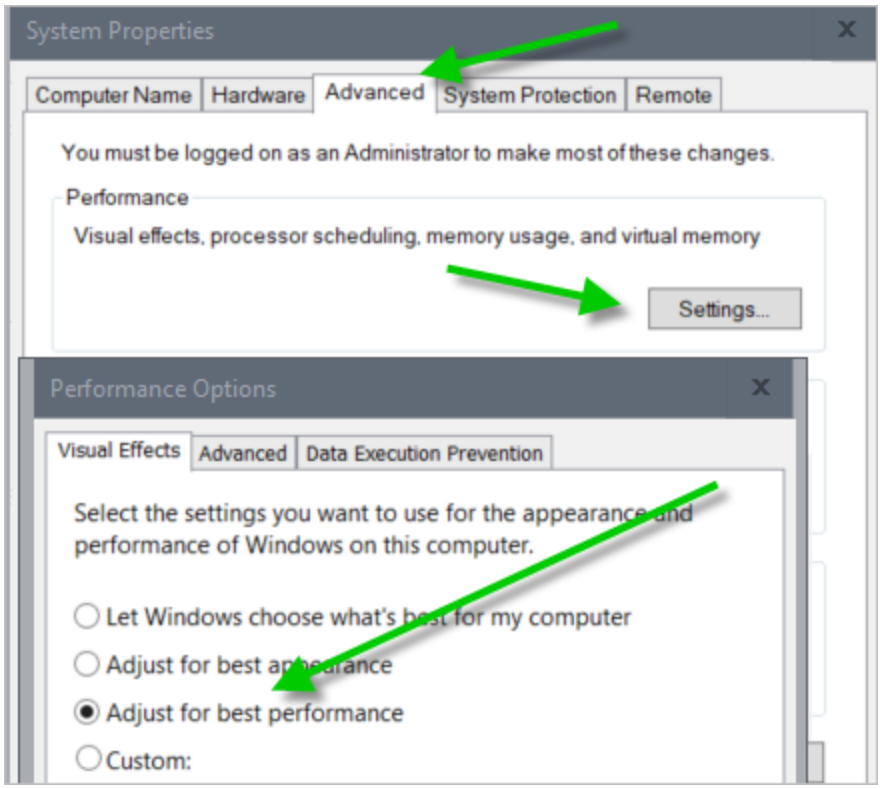
VDI デスクトップ割り当てについては、『VMware Blast Extreme Optimization Guide』の「Codec Options」セクションと、各コーデックに最適なアプリケーションの表を参照してください。

Microsoft Windows 10 Enterprise マルチセッションまたは Windows Server オペレーティング システム上に構築されたイメージを使用するファームについては、セクションさまざまなエンド ユーザーの個人設定とワークロード タイプで使用されるファームのコーデックの選択と仮想マシン シリーズのサイズに関する推奨事項のガイドラインを参照してください。

重要： 『VMware Blast Extreme Optimization Guide』の「Enabling Codecs and Codec Options」セクションの表 2 で説明されているように、一部のコーデック オプションには、対応する Horizon Client 設定が必要です。Blast コーデックと H.264 コーデックの場合、エンド ユーザーは Horizon Client で適切な選択を行う必要があります。

4 ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリングで説明されているように、ウィザードの [詳細オプション] は、ゴールド イメージの作成時に Horizon リモート エクスペリエンス機能を有効にするオプションを提供します。これらのトグルの一部は、イメージにインストールするためにデフォルトで有効になっています。ウィザードで、仮想マシンを作成するためにウィザードを送信する前に、ビジネス ニーズに特に必要なリモート エクスペリエンス機能のみが有効になっていることを確認する必要があります。簡単な例として、クライアント ドライブ リダイレクトのトグルはデフォルトでオンになっています。ビジネス ニーズにおいてエンド ユーザーがクライアント ドライブ リダイレクトを要求する必要があると判断しない限り、そのトグルをオフに切り替えて、クライアント ドライブ リダイレクトが有効にならないようにします。

5 仮想マシンの [システム プロパティ] - [詳細システム設定] - [パフォーマンス オプション] の順に開き、設定を確認して、仮想マシンが目的のパフォーマンスに対して適切に設定されていることを確認します。最適な設定は、[最適なパフォーマンスに合わせて調整する] です。次のスクリーンショットは、これらの設定の場所を示しています。



オプション：ユーザー エクスペリエンス監視ツールのインストール

ユーザー エクスペリエンス監視ツールをインストールすると、FPS、帯域幅、CPU 消費量、コーデック タイプなど、仮想マシンのオペレーティング システム内のさまざまなパフォーマンス メトリックを測定するのに役立ちます。このようなツールの 1 つに、サードパーティのツール RDAnalyzer があります。

さまざまなエンド ユーザーの個人設定とワークロード タイプで使用されるファームのコーデックの選択と仮想マシン シリーズのサイズに関する推奨事項

次の仮想マシンの例とサイズの提案は、Horizon Cloud のファームからの一般的なワークロードに基づいています。ファームは、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エンド ユーザーにプロビジョニングします。ファームは、Microsoft Windows 10 Enterprise マルチセッションまたは Microsoft Windows Server オペレーティング システムを実行しているイメージに基づいています。個々のビジネス シナリオで最良の結果を得るために最適なサイズを決定する必要があります。最適なサイズを決定するために、VMware はシミュレーション ツールを使用して環境でテストを実行することをお勧めします。これは特に、Microsoft が時間の経過とともにより新しく高速な仮想マシン サイズを発表しているためです。追加のガイダンスが必要な場合は、VMware 担当者にお問い合わせください。以下にリストされているコーデックの設定の詳細については、『VMware Blast Optimization Guide』の Enabling Codecs and Codec Options および Configuration Settings for Administrators セクションを参照してください。

Microsoft Azure の仮想マシン シリーズ	ワークロード タイプ	仮想 CPU あたりの最大ユーザー数/ユーザーの合計	個人設定	最適なコーデック	説明	アプリケーションの例
D2s_v3、F2s_v2	低	vCPU あたりの最大値 = 6 合計 = 12	タスクワーカー	Blast コーデック	CPU および帯域幅の使用率が低い。最適なエクスペリエンスを実現するために、帯域幅とフレーム レートをより厳密に管理します。	データベース エントリ アプリケーション、コマンドライン インターフェイス (CLI)
D4s_v3、F4s_v2	中	vCPU あたりの最大値 = 4 合計 = 16	コンサルタントと市場調査員	Blast コーデック	CPU および帯域幅の使用率が低い。最適なエクスペリエンスを実現するために、帯域幅とフレーム レートをより厳密に管理します。	データベース エントリ アプリケーション、コマンドライン インターフェイス (CLI)、Microsoft Word、静的 Web ページ

Microsoft Azure の仮想マシン シリーズ	ワークロード タイプ	仮想 CPU あたりの最大ユーザー数/ユーザーの合計	個人設定	最適なコーデック	説明	アプリケーションの例
D4s_v3、F4s_v2	高	vCPU あたりの最大値 = 2 合計 = 8	エンジニアとコンテンツ作成者	H.264	CPU および帯域幅の使用率が中程度。マルチメディアに適したエクスペリエンス。	データベース エントリ アプリケーション、コマンドライン インターフェイス (CLI)、Microsoft Word、静的 Web ページ、Microsoft Outlook、Microsoft PowerPoint、動的 Web ページ
D4s_v3、F4s_v2、NV6	電源	vCPU あたりの最大値 = 1 合計 = 4	グラフィック デザイナー	H.264	CPU および帯域幅の使用率が中程度。フレーム レートを 60 FPS（フレーム/秒）に変更することで、マルチメディアおよび 3D グラフィックス アプリケーションに適した卓越したエクスペリエンスを提供できます。NV6 を使用する場合は、グラフィックスにハードウェア アクセラレーションを利用します。	データベース エントリ アプリケーション、コマンドライン インターフェイス (CLI)、Microsoft Word、静的 Web ページ、Microsoft Outlook、Microsoft PowerPoint、動的 Web ページ、Adobe Photoshop、Adobe Illustrator、コンピュータ支援設計 (CAD)、コンピュータ支援製造 (CAM)

追加情報

リモート エクスペリエンスのユースケース向けに仮想マシンを最適化する方法の詳細については、以下を参照してください。

- Microsoft のドキュメント トピック仮想マシンのサイズ設定のガイドラインには、仮想マシンが Azure 仮想デスクトップ (AVD) で実行されている場合の Microsoft Windows 10 Enterprise マルチセッションのサイズ設定に関する推奨事項が含まれています。
- VMware Digital Workspace Tech Zone の『VMware Blast Extreme Optimization Guide』

- VMware Digital Workspace Tech Zone の『Windows OS Optimization Tool for VMware Horizon Guide』
- VMware Digital Workspace Tech Zone の『Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop』

Horizon Cloud on Microsoft Azure - インポートした GPU 対応仮想マシンに適切な GPU ドライバをインストールする

Azure Marketplace からインポートされた GPU 対応仮想マシンの GPU 機能を利用するには、仮想マシンの Microsoft Windows オペレーティング システムにログインし、仮想マシン タイプに適したグラフィックス ドライバをインストールする必要があります。

Horizon Cloud on Microsoft Azure デプロイでは、GPU 対応の仮想マシンを Azure Marketplace からインポートするために次の方法がサポートされています。

コンソールの [Marketplace からの仮想マシンのインポート] ウィザードを使用する

ウィザードは、特に Standard_NV12s_v3 仮想マシン タイプをインポートします。

Azure Marketplace から仮想マシンを手動でインポートする

手動インポート方法を使用する場合、Horizon Cloud on Microsoft Azure は、選択したオペレーティング システムに応じて、Azure Marketplace からの次の仮想マシン モデルのインポートをサポートします。

オペレーティング システム	Azure Marketplace でサポートされる仮想マシン タイプ
■ Windows Server ■ Windows 10 単一セッションまたはマルチセッション ■ Windows 11 単一セッションまたはマルチセッション	Standard_NV12s_v3 Microsoft Azure によって提供され、Microsoft Azure のドキュメントに記載されている NVIDIA GRID ドライバを使用します。https://docs.microsoft.com/en-us/azure/virtual-machines/windows/n-series-driver-setup の NVIDIA GRID セクションを参照してください。
■ Windows Server ■ Windows 10 単一セッションまたはマルチセッション	Standard_NV8as_v4 Microsoft Azure によって提供され、Microsoft Azure のドキュメントに記載されている AMD Radeon Instinct ドライバを使用します。https://docs.microsoft.com/en-us/azure/virtual-machines/windows/n-series-amd-driver-setup を参照してください。

仮想マシンが作成され、コンソールにエージェントのステータスがアクティブであることが示されたら、適切なドライバをインストールする必要があります。

概要レベルでは、ワークフローは次のとおりです。

1 インポートされた仮想マシンのシリーズおよび Windows オペレーティング システムに適したドライバを取得します。前述の表を参照してください。

2 インポートした仮想マシンに接続してログインします。

3 上記の Microsoft Azure ドキュメント ページのインストール手順に従ってドライバをインストールします。

注意： 他のドライバではなく、これらの Microsoft ページで説明および提供されているドライバをインストールします。

前提条件

[インポートされた仮想マシン] ページで、仮想マシンに対してエージェントに関連するステータスがアクティブになっていることを確認します。このステータスを取得するには、仮想マシンで [インポートされた仮想マシン] ページの [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ます。このアクションは、[詳細] ドロップダウン リストにあります。

注： Microsoft リモート デスクトップ クライアントを RDP ソフトウェアとして使用して仮想マシンに接続する場合は、それが最新のバージョンであることを確認してください。たとえば、Windows 7 オペレーティング システムのデフォルトの RDP ソフトウェアのバージョンはこの条件を満たしていません。バージョンは、バージョン 8 以降である必要があります。

仮想マシンの作成方法に応じて、仮想マシンのゲスト Windows オペレーティング システムにログインするために、認証情報（ユーザー名とパスワード）の少なくとも 1 つがあることを確認します。

仮想マシンの作成方法	ログインに使用する認証情報
[インポートされた仮想マシン] ページから、仮想マシンのインポート ウィザードを実行します。	2019 年 12 月のサービス リリース日以降、[仮想マシンのインポート] ウィザードは、作成プロセスの最後に、ウィザードで作成された仮想マシンを指定された Active Directory ドメインに参加させるか、仮想マシンをドメインに参加させないかのオプションを提供します。 ■ ウィザードの [ドメイン参加] トグルを有効にして仮想マシンが作成された場合、指定された Active Directory ドメインのドメイン アカウントの認証情報を使用するか、ウィザードで指定されたローカル管理者アカウントを使用できます。 ■ ウィザードの [ドメイン参加] トグルをオフにして仮想マシンが作成された場合、ウィザードで指定されたローカル管理者アカウントを使用する必要があります。この場合、仮想マシンはドメインに参加していないため、ログインするためのアクセス権を持つ唯一のアカウントがローカル管理者アカウントになります。
手動による準備手順 。	通常、仮想マシンを手動で構築するときに、仮想マシンを Active Directory ドメインに加える必要はありません。その仮想マシンにログインするには、次のいずれかの方法を使用します。 ■ 手動で構築された仮想マシンが Microsoft Azure ポータルで作成されたときに指定されたローカル管理者アカウントの認証情報。 ■ その仮想マシンを Active Directory ドメインに手動で参加させた場合、そのドメインのドメインアカウントの認証情報。

手順

1 仮想マシンの Windows オペレーティング システムに接続するには、RDP ソフトウェアで仮想マシンの IP アドレスを使用します。

   - パブリック IP アドレスを使用して仮想マシンを作成した場合は、その IP アドレスを RDP ソフトウェアで使用できます。
   - 仮想マシンにプライベート IP アドレスがある場合は、次の 2 つの方法のいずれかを使用して RDP を実装する必要があります。
     - パブリック IP アドレスを持つ Microsoft Azure サブスクリプション内で別の仮想マシンを使用し、インポートされた仮想マシンに対してアウトバウンド RDP を実行する。

- VPN と RDP を企業のネットワーク経由で仮想マシン内で使用する

注： エージェントに関連するソフトウェア コンポーネントを実行している仮想マシンにアクセスする場合、リモート デスクトップ クライアントのバージョンは 8 以降である必要があります。そうでないと、接続に失敗します。最新のリモート デスクトップ クライアントを使用することをお勧めします。

2 この前提条件に記述されるように、認証情報 (ユーザー名とパスワード) を使用して Windows オペレーティング システムにログインします。

仮想マシンの作成時にコンソールの [Marketplace からの仮想マシンのインポート] ウィザードで指定したローカル管理者アカウントの認証情報を使用する場合は、ユーザー名を `\username` と入力します。

注： 仮想マシンがこの前提条件で記述されているように、ドメインに参加している仮想マシンであり、ローカル管理者アカウントではなくドメイン アカウントを使用したい場合は、ユーザー名を *ドメイン*`\username` と入力します。ここで *ドメイン* はドメイン名です。

3 前述の Microsoft Azure ドキュメント ページの説明に従って、インポートした仮想マシンのタイプに該当するドライバをインストールします。

4 ドライバがインストールされたら、仮想マシンを再起動します。

5 仮想マシンに再接続してログインし、ドライバが仮想マシンにインストールされ、動作していることを確認します。

ドライバがインストールされ、動作していることを確認する方法については、インストールされているドライバの Microsoft ドキュメント ページとそのページの「[ドライバのインストールの確認]」セクションを参照してください。これらのすべての Microsoft ページには、「[ドライバのインストールの確認]」セクションがあります。

6 仮想マシンの Windows オペレーティング システムからログアウトします。

構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の割り当て可能なイメージに変換する

インポートされた仮想マシンを、エンド ユーザーにプロビジョニングするデスクトップおよびリモート アプリケーションのビジネス ニーズに一致するようにカスタマイズすると、その仮想マシンがゴールド イメージになります。システムがエンドユーザーに付与できる割り当てのイメージを使用できるようにするには、Horizon Universal Console 公開ワークフローを使用してイメージをシーリングする必要があります。そのゴールド イメージを公開すると、イメージがシーリングされ、割り当て可能なイメージになります。

このページは、Horizon Cloud on Microsoft Azure ポッドにあるシングルポッド イメージに適用されます。

コンソールに [イメージ - マルチポッド] が表示されている場合は、Horizon Image Management Service およびマルチポッド イメージ管理の機能を使用できます。マルチポッド イメージの場合、参加しているポッドにこれらのマルチポッド イメージを公開するには、さまざまな手順を使用します。その場合は、クラウドからの Horizon イメージの管理に記載されたマルチポッド イメージの公開の手順を実行してください。

重要： Microsoft Azure のポッドがプロキシを使用するように構成されている場合は、このイメージを使用して作成されているファーム仮想マシンまたは VDI デスクトップ仮想マシンがプロキシとともに構成されるようにするための手段を提供する責任があります。

前提条件

構成済みのイメージが、割り当て可能なイメージを作成するポッドで使用可能であることを確認します。

重要： 第 1 世代 Horizon Cloud on Microsoft Azure デプロイ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 から供給される 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。

イメージで Windows 11 オペレーティング システムが実行されている場合は、Azure Marketplace から直接供給される必要があるほか、イメージを第 1 世代 Horizon Cloud on Microsoft Azure デプロイで有効にサポートするために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。

第 1 世代 Horizon Cloud on Microsoft Azure デプロイでのイメージ関連のワークフローでサポートされる Gen-1 マシンと Gen-2 マシンの組み合わせ、およびどの OS がどのマシン世代でサポートされているかについての追加の考慮事項については、Microsoft Azure のポッドから提供されるイメージのサポートを参照してください。

次のスクリーンショットに示すように、[インポートされた仮想マシン] ページで、仮想マシンがパワーオンの状態（緑色のステータス）で、エージェントに関連するステータスがアクティブであることを確認します。

イメージ仮想マシンに有効になっているローカル管理者アカウントの認証情報があることを確認します。ゴールド イメージを公開済みの状態に変換するイメージ シーリング プロセスで、システムはローカル管理者アカウントを使用します。通常、仮想マシンに対して有効に設定されているローカル管理者アカウントは、Microsoft Azure に Horizon Cloud ポッドのデスクトップ イメージを作成およびそのサブトピックに記載されているように、イメージ仮想マシンを作成したときに名前を付けたアカウントになります。

重要： イメージ仮想マシンに手動でローカル管理者アカウントを追加していない限り、仮想マシンのローカル管理者アカウントは、[仮想マシンのインポート] ウィザードを実行したとき、またはゴールド イメージの仮想マシンを手動で作成したときに指定したものに限られます。

手順

1 コンソールで [インベントリ] - [イメージ] の順にクリックして、[新規] をクリックします。

2 必要な情報を入力します。

オプション	説明
場所	イメージが構成されたポッドに関連付けられている場所を選択します。このフィールドは、[ポッド] リストで選択できるように表示されるポッドのセットをフィルタリングします。
ポッド	構成されたイメージのあるポッドを選択します。 **ヒント:** 選択するポッドが表示されない場合は、[場所] リストにポッドがない場所が表示されていないことを確認します。[場所] フィールドは [ポッド] リストに表示され、選択した場所に関連付けられていないポッドを除外します。すでに場所にポッドがあり、そのポッドを削除するか別の場所に移動して、表示された場所にポッドが存在しなくなると、[ポッド] リストにはエントリが表示されなくなります。場所はアルファベット順に表示されているため、画面を開くと、アルファベット順で最初の場所が自動的に選択されます。その場所にポッドが関連付けられていない場合は、場所を別のエントリに切り替える必要があります。
デスクトップ	このフィールドには、システムが割り当て可能イメージに変換できる選択済みポッド上にある仮想マシンが一覧表示されます。任意の仮想マシンを選択します。 選択を行った後、選択した仮想マシンについて、ステータスなどの情報が表示されます。
イメージ名	このフィールドには、[デスクトップ] での選択に関連付けられたイメージ名が自動的に入力されます。
会社名	識別名を入力します。この名前は、このイメージに基づいて作成される仮想デスクトップに表示されます。公開プロセスは、レジストリ キー `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner` をこの値に設定します。名前は、登録済みの組織および所有者として仮想デスクトップの [Windows について] ダイアログに表示されます。
タイムゾーン	デフォルトのままにします。
[デスクトップの管理者認証情報]	イメージ仮想マシンで有効になっているローカル管理者アカウントの認証情報を入力します。通常、イメージ仮想マシンの作成時に指定されたローカルの管理者アカウントのみが有効になります。 **注：** この公開プロセスには、Microsoft Windows Sysprep プロセスの実行が含まれます。仮想マシンが Microsoft Windows Server オペレーティング システムの場合、Sysprep プロセスによって、組み込みの管理者アカウント パスワードがここで入力したパスワードにリセットされます。このパスワードのリセットは、Sysprep プロセスが完了した後に組み込みの管理者アカウントを保護するために行われます。組み込みの管理者パスワードは、この手順で組み込みの管理者アカウントまたは別のローカル管理者アカウントを指定するかどうかにかかわらず、ここで入力したパスワードにリセットされます。

3 [公開] をクリックします。

公開プロセスは完了するまで数分かかります。このプロセスを実行中は、ページに [移行中] ステータスが表示されます。更新アイコンを使用して、最新ステータスを表示できます。

結果

プロセスが正常に実行されると、イメージのステータスは [公開済み] に変更されます。イメージのステータスが [公開済み] の場合は、Horizon Cloud にシールドされたものとみなされます。シールドされたイメージは、システムが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ために RDSH ファームで使用できる

仮想マシン（RDSH 対応の Windows オペレーティング システムの場合）または VDI デスクトップ割り当てで使用できる仮想マシン（単一セッションの Windows クライアント オペレーティング システムの場合）です。

注意: イメージを公開し、Horizon Cloud でそのイメージがシールドされた状態にある場合は、そのイメージの仮想マシンに対してアクションを実行するために Microsoft Azure ポータルを使用しないでください。Microsoft Azure ポータルを使用して、Horizon Cloud で公開されている状態の仮想マシンに対して直接アクションを実行することはサポートされておらず、予期しない動作を引き起こします。シールドされたイメージに対してアクションを実行する際は、必ず Horizon Universal Console を使用してください。

シールドされた仮想マシンのゲスト Windows オペレーティング システムで変更が必要な場合は、状況に応じて次のトピックの手順を使用します。

- シールドされたイメージを、Microsoft Windows Server や Windows 10 または 11 Enterprise マルチセッション オペレーティング システムなどの RDSH タイプのオペレーティング システムで更新するには、Horizon Cloud でのファームに使用されるイメージの変更を参照してください
- シールドされたイメージを Microsoft Windows クライアント オペレーティング システムで更新するには、VDI デスクトップ割り当てに使用されるイメージの変更を参照してください。

ステータスが [公開済み] のイメージは [インポートされた仮想マシン] ページには表示されません。[公開済み] の状態になるとイメージは [インポートされた仮想マシン] ページから削除されます。この時点で、これらのシールドされた仮想マシンは [イメージ] ページで利用可能になります。

公開操作に失敗した場合、[監視] - [アクティビティ] を選択し、失敗したジョブを見つけます。問題を修正してから、イメージの横のチェック ボックスを選択し、[詳細] - [デスクトップへの変換] の順にクリックして、公開操作を再試行します。次に [新規] をクリックして、必要な情報を入力し、[公開] をクリックしてイメージを公開します。

Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートする

次の手順は、Microsoft Azure のポッドでゴールド イメージとして使用する仮想マシンを手動でインポートする方法の一部です。Horizon Cloud にインポートするための環境の要件に準拠する仮想マシンを手動で構築する場合は、マルチステップ プロセスで行います。これらの手順のほとんどは、Microsoft Azure ポータルで実行します。最初にベース仮想マシンを作成して構成し、そのベース仮想マシンにエージェントに関連するソフトウェア コンポーネントをインストールしてから、それらのエージェントに関連するコンポーネントの特定のプロパティを構成します。

自動化ウィザードを使用せずに Microsoft Azure ポータルを使用して手動で仮想マシンを構築する場合、または Microsoft Azure ポータルを使用してすでに手動で仮想マシンを構築済みで、その仮想マシンを Horizon Cloud でゴールド イメージの基盤として使用する場合のみに、これらの手順を使用します。Microsoft Azure のポッドのゴールド イメージを自動的に構築するために推奨される方法は、ウィザードを使用することです。自動化されたウィザードの使用の詳細については、ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリングを参照してください。

重要： Microsoft Azure に仮想マシンがあり、それをゴールド イメージ用に Horizon Cloud にインポートする場合は、Microsoft Azure のポッドに仮想マシンを手動で作成するに記載されている手動の手順を使用して仮想マシンが構築およびインポートされるときと同じ条件に確実に準拠するようにする必要があります。仮想マシンが同じ条件に準拠していない場合、Horizon Cloud はそれを使用してコンソールに表示したり、[イメージに変換] ワークフローで使用したりすることはできません。次の条件が重要です。

- エージェントに関連するソフトウェアをインストールする前に、ベース仮想マシンで [ストレージ - 管理対象ディスクを使用] を [はい] に設定する必要があります。ベース仮想マシンがこの設定に従っていない場合、Horizon Cloud はこの仮想マシンを使用できません。
- ベース仮想マシンは、ベース仮想マシンを使用するポッドと同じ Microsoft Azure の場所にある必要があります。
- ベース仮想マシンは、Microsoft Azure サブスクリプションの特定のリソース グループに配置される必要があります。このリソース グループは、ベース仮想マシンを使用する予定のポッドに属しているものになります。リソース グループは `vmw-hcs-`*`podID`*`-base-vms` という名前で、*podID* はポッドの UUID 識別子です。
- ベース仮想マシンは、ポッドが接続されている同じ仮想ネットワークに接続される必要があります。
- ベース仮想マシンは、ポッドの `vmw-hcs-`*`podID`*`-net-tenant` という名前のサブネットに接続する必要があります。
- ベース仮想マシンは、この Horizon Cloud リリースでの使用が現在サポートされているオペレーティング システムを使用する必要があります。サポートされているオペレーティン グシステムに関するナレッジベースの記事へのリンクは、ドキュメント トピック Horizon Cloud — 環境、オペレーティング システム、および互換性にあります。
- IPv6 IP アドレスを使用するようにベース仮想マシンを構成しないでください。Horizon Cloud では、IPv6 IP アドレスを使用する仮想マシンに基づく仮想マシンについて、[デスクトップの健全性] タブで IP アドレス異常のアラートが報告されます。

ベース仮想マシンをさらに構成するのを始める前にそれが条件を満たしていることを確認するには、Horizon Cloud にログインして、[インベントリ仮想マシン] ページに移動し、そのページにベース仮想マシンが一覧表示されていることを確認します。一覧表示されている場合は、そのベース仮想マシンは上記の条件を満たしており、エージェントをインストールする前に手動で作成した仮想マシンを準備するに一覧表示されているトピックから始まる残りの構成の手順を安全に進めることができます。

手順

1 Microsoft Azure のポッドに仮想マシンを手動で作成する

2 エージェントをインストールする前に手動で作成した仮想マシンを準備する

Microsoft Azure でポッドの仮想マシンを手動で構築してインポートする場合、エージェントに関連するソフトウェア コンポーネントをインストールする前に、ベース仮想マシンを入念に準備するためにいくつかの追加タスクを実行する必要があります。Microsoft Azure ポータルを使用し、新しい仮想マシンに接続してこれらの手順を実行します。

3 手動で作成した仮想マシンでのエージェント関連のソフトウェア コンポーネントのインストールおよび Horizon Cloud とのペアリング

このドキュメント ページでは、Horizon Cloud に必要で適切なエージェントに関連するコンポーネントを手動でインストールし、仮想マシンをクラウド プレーンとペアリングする手順について説明します。ベース仮想マシンの Windows オペレーティング システムでは、Horizon Agents Installer を実行します。仮想マシンを再起動した後、Horizon Cloud 管理コンソールを使用して、仮想マシンとクラウド プレーンをペアリングします。

4 廃止 - ポッドのマニフェスト バージョンが 1600 未満の場合、エージェントに関連するソフトウェア コンポーネントをベース仮想マシンにインストールする

マニフェストが 1600 未満のポッドのエージェントに関連するソフトウェアのインストールに関するこのドキュメント ページは、関連がなくなりました。これらのデプロイはジェネラル サポートが終了しました。

Microsoft Azure のポッドに仮想マシンを手動で作成する

Microsoft Azure ポータルでは、VDI クライアント ベースのデスクトップ、RDS ベースのセッション デスクトップ、または RDS ベースのリモート アプリケーションで使用する Windows ゲスト OS を使用して仮想マシン (VM) を作成します。この仮想マシンは、Horizon Cloud ポッドで使用したものと同じサブスクリプションを使用して作成します。

この仮想マシンは、ポッドが接続されている同じ Microsoft Azure VNet（仮想ネットワーク）で作成される必要があります。また、この仮想マシンは、`vmw-hcs-`*`podID`*`-base-vms` という名前のリソース グループに作成する必要があります。ここで、*podID* はポッドの UUID 識別子です。Horizon Cloud は、そのリソース グループにある仮想マシンを自動的に検出します。[ストレージ - 管理対象ディスクを使用] を [はい] に設定している場合、Horizon Cloud はコンソールのインベントリ画面にそれらの仮想マシンをリストします。

手動でインポートした仮想マシンを Horizon Cloud で使用できるようにするには、次の手順を実行する必要があります。

- Microsoft Azure Marketplace から Microsoft Windows 仮想マシンを入手します。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。
- このリリースの Horizon Cloud での使用がサポートされているオペレーティング システムに合わせます。サポートされているオペレーティング システムに関するナレッジベースの記事へのリンクは、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 ページにあります。
- Azure Marketplace から Microsoft Windows 仮想マシンを作成する場合は、次のリストにある対応する仮想マシン モデルを使用します。

次の表に示すモデルは、Horizon Cloud での使用が検証されたモデルです。これらのモデルを使用して、手動でインポートされたイメージをコンソールの [インポートされた仮想マシン] ページに表示し、そのページで使用可能なワークフロー アクションを実行することができます。

注： Horizon Cloud で Windows 11 OS のサポートを有効にするには、ポッドが v2204 リリースのマニフェスト バージョン以降を実行していること、そして仮想マシンが直接 Azure Marketplace から提供されていることが必要です。イメージを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。Horizon Agents Installer (HAI) を実行してエージェントを Windows 11 仮想マシンにインストールする場合は、バージョン 22.1 以降を使用する必要があります。

使用事例	手動インポート用の仮想マシン モデル
非 GPU、Windows 11 以外のオペレーティング システム	Standard_DS2_v2
非 GPU、Windows 11 OS または Windows 11 Enterprise マルチセッション OS	Standard_D4s_v3
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	■ Standard_NV12s_v3 ■ Standard_NV4as_v4 インポートされた Standard_NV4as_v4 仮想マシンを Horizon Cloud で使用するには、ポッドが v2204 リリースのマニフェスト バージョン以降を実行していること、仮想マシンが直接 Azure Marketplace から提供されていること、そして Windows 10 OS（単一セッションまたはマルチセッション）または Windows Server OS を使用することが必要です。(Horizon Cloud は現在、Windows 11 OS を使用するインポートされた Standard_NV4as_v4 の使用をサポートしていません。)
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_NV12s_v3
Windows 7 OS、GPU なし	Standard_DS2_v2。Windows 7 では、GPU はデフォルトでサポートされていません。

注： Microsoft GPU 対応の NV シリーズ、NVv4 シリーズ、および NCv3 シリーズは、一部の Microsoft Azure リージョンでのみ使用できる場合があります。ポッドで GPU ベースのデスクトップまたはリモート アプリケーションをプロビジョニングするには、Microsoft がそれらの GPU 対応の仮想マシン シリーズを使用できるようにしている Microsoft Azure リージョンにポッドを配置する必要があります。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。

Horizon Cloud の Microsoft Azure 仮想マシンのタイプとサイズの詳細については、VMware ナレッジベースの記事 KB77120 を参照してください。Microsoft Azure ドキュメントの仮想マシンのサイズの詳細については、Azure の Windows 仮想マシンのサイズを参照してください。

前提条件

仮想マシンを作成している対象のポッドに関する次の情報を取得します。この情報を表示するには、Horizon Cloud 管理コンソールで [設定] - [キャパシティ] に移動し、ポッドの名前をクリックして、ポッドの詳細ページを開きます。ポッドの [サマリ] タブから次を取得します。

- ポッドを接続する仮想ネットワークの名前。仮想マシンの作成では、同じ仮想ネットワークを選択する必要があります。
- 仮想マシンを作成している対象のポッドの ID。ポッドの ID は、UUID 形式の識別子です。この UUID は Microsoft Azure ポータルでそのポッドのリソース グループを識別するために必要になります。これにより、どのリソース グループで仮想マシンを検索すればよいかを特定できます。
- ポッドを手動で作成されたサブネットにデプロイした場合は、デスクトップ（テナント）サブネットの名前を取得します。仮想マシンを作成するときは、同じサブネットを選択する必要があります。

手順

1 ポッドのデプロイに使用するサブスクリプションに関連付けられている Microsoft Azure アカウントを使用して、Microsoft Azure ポータルにログインします。

2 ポータルで、ポッドの `vmw-hcs-`*`podID`*`-base-vms` リソース グループに移動します。

3 その `vmw-hcs-`*`podID`*`-base-vms` リソース グループで、[作成] をクリックします。

この時点で、Microsoft Azure ポータルには通常、[リソースの作成] ペインが表示されます。

4 Azure Marketplace を使用して、使用する Microsoft Windows オペレーティング システムを見つけて選択します。

この仮想マシンを単一セッション VDI デスクトップ、マルチセッション デスクトップ、またはリモート アプリケーションのどのゴールド イメージとして使用するかに基づいて、オペレーティング システムを選択します。Horizon Cloud によってサポートされるオペレーティング システムについてのナレッジベースの記事へのリンクについては、ドキュメントのトピック Horizon Cloud（環境、オペレーティング システム、互換性）を参照してください。

重要： GPU ベースの RDS ベース デスクトップの基盤として NVIDIA GRID ドライバの NV シリーズ仮想マシンを使用する計画の場合は、Microsoft Windows Server 2012 R2 の使用を避けます。NVIDIA ドライバの制限により、各 Windows Server 2012 R2 ファーム仮想マシンにアクセスするエンド ユーザー セッションの数は、それぞれ最大 20 セッションに制限されます。

GPU ベースのデスクトップを使用する場合は、Microsoft Windows 7 を選択しないでください。Horizon Cloud では、GPU とともに Windows 7 を使用することはサポートされていません。

ポータルに [仮想マシンの作成] ウィザードが表示されます。

5 [基本] の手順で、以下の情報に従って必須フィールドに入力します。この表に記載されていない項目については、デフォルトのままにします。

オプション	説明
[サブスクリプション]	このゴールド イメージを作成するポッドに対して、ポッドのサブスクリプションがここで選択されていることを確認します。
[リソース グループ]	そのポッドの base-vms リソース グループ (`vmw-hcs-podID-base-vms`) を選択します。
[仮想マシン名]	この仮想マシンに最大 15 文字の英数字の名前を付けます。
[リージョン]	ポッドの Microsoft Azure リージョンと一致するリージョンを選択します。 **注：** GPU ベースの仮想マシンを使用する場合、サブスクリプションには、使用可能な NV シリーズまたは NVv4 のいずれかの仮想マシン タイプに対する Microsoft Azure リージョンの割り当てが必要です。すべての仮想マシン シリーズがすべての Microsoft Azure リージョンで使用できるわけではありません。
[可用性オプション]	通常は [インフラストラクチャの冗長性なし] を選択します。
[イメージ]	選択内容が使用する Windows オペレーティング システムと一致していることを確認します。
[サイズ]	前の使用事例と仮想マシン モデルの表に基づいて、仮想マシンのサイズを選択します。次の表に、Horizon Cloud のイメージ インポートおよびイメージ公開ワークフローでの使用が検証されたモデルを示します。
[ユーザー名]	仮想マシンのデフォルト管理者アカウントの名前を入力します。
[パスワード] [パスワードの確認]	デフォルトの管理者アカウントのパスワードを入力して確定します。 パスワードは、Microsoft Azure が仮想マシンに対して定義するパスワードの複雑さのルールに準拠している必要があります。通常、パスワードの長さは 12 文字以上で、1 つの小文字、1 つの大文字、1 つの数字、およびバックスラッシュ (¥) またはハイフン (-) 以外の 1 つの特殊文字を含む必要があります。
[パブリック受信ポート]	RDP を使用してインターネット経由で仮想マシンに接続することによってエージェントをインストールできるようにする場合は、[選択したポートを許可] を選択してから、[RDP]（ポート 3389）を選択します。
[ライセンス] セクション	画面に表示される指示に従います。選択した Microsoft オペレーティング システムで組織が使用している有効なライセンスに適した選択肢を選択します。

6 [ディスク] の手順に進みます（[次: ディスク>]）。

7 [ディスク] の手順で、[オペレーティング システム ディスク タイプ] に [標準の SSD] または [標準の HDD] を選択します。

この仮想マシンを GPU ベースのゴールド イメージで使用する場合は、ディスク タイプに [標準 HDD] を選択します。それ以外の場合は、デフォルトの [SSD] 設定を保持するか、必要に応じて [HDD] を選択します。

8 （オプション）[ディスク] の手順で、この基本イメージに基づく仮想デスクトップまたは RDSH インスタンスがデータ ディスクを持つようにする場合は、[データ ディスク] セクションを使用して、データ ディスクを作成してこのベース仮想マシンに接続します。

データ ディスクを指定する場合は、[ソース タイプ] で、[なし（空のディスク）] を選択します。他の選択肢については、デフォルトをそのまま使用するか、変更することができます。データ ディスクの名前はカスタマイズできます。必要な設定を指定したら、[OK] をクリックします。

データ ディスクが [ディスク] の手順に表示されている場合、オプションでデータ ディスクの [ホスト キャッシュ] 設定を選択できます。通常、データ ディスクの使用目的に最も適している設定に応じて、設定を選択します。

9 [ディスク] の手順で、[詳細] セクションを展開し、[管理対象ディスクを使用] が選択されていることを確認します。

注意： Horizon Cloud でこの仮想マシンを使用するには、[管理対象ディスクを使用] を選択する必要があります。エージェントに関連するソフトウェア コンポーネントをインストールするインストーラを実行する前に仮想マシンで [管理対象ディスクを使用] が選択されていない場合、Horizon Cloud はこの仮想マシンを使用できないため、別のものを新しく作成する必要があります。

10 [ネットワーク] の手順に進みます（[次: ネットワーク >]）。

11 [ネットワーク] の手順で、以下で説明するように仮想ネットワークとサブネットを設定し、[確認および作成] をクリックして構成内容を保存して、確認の手順に進みます。

その他すべての設定ではデフォルト値を使用します。

注目:

- 上記の前提条件セクションの説明のように、ポッドが使用する VNet と同じように [仮想ネットワーク] を設定する必要があります。
- [ネットワーク] 画面のその他のオプションは変更しないでください（拡張機能なし、など）。これらのオプションはデフォルト設定のままにします。次の表に記載されている内容以外は変更しないでください。

オプション	説明
[仮想ネットワーク]	[仮想ネットワーク] をクリックし、ポッドが接続されているのと同じ仮想ネットワーク (VNet) を選択します。
[サブネット]	[サブネット] をクリックし、ポッドのデスクトップ（テナント）サブネットを 1 つ選択します。ポッドをデプロイしたときに、ポッド デプロイヤが自動的にサブネットを作成した場合、このサブネットは `vmw-hcs-podID-net-tenant` という名前になります。
[パブリック IP アドレス]、[NIC ネットワーク セキュリティ グループ]、[パブリック受信ポート]、[受信ポートの選択]	RDP を使用してインターネット経由で仮想マシンに接続することによってエージェントをインストールできるようにする場合は、新しいパブリック IP アドレス、基本ネットワーク セキュリティ グループを作成することを選択し、[選択したポートを許可] を選択してから、[RDP]（ポート 3389）を選択します。 VNet に接続された VPN 経由または Azure Bastion を使用してエージェントをインストールする場合は、[パブリック IP アドレス] に対して [なし] を選択し、ネットワーク セキュリティ グループに対して独自の選択を行い、受信ポートを防止することができます。
[ネットワークの高速化]	本書の執筆時点では、Azure ポータルはデフォルトでこれを選択します。デフォルトをそのまま使用することも、この設定をクリアすることもできます。

[確認および作成] をクリックすると、検証が実行されます。検証に成功すると、ウィザードは最後の手順に移動します。

12 最後の手順ではサマリを確認します。特にリソース グループ、仮想ネットワーク、サブネットの設定が正しいこと、そして [管理対象ディスクを使用] が `Yes` に設定されていることを確認します。

リソース グループとサブネット名には、ポッドの UUID (*podID*) が含まれています。

設定	値
リソース グループ	`vmw-hcs-podID-base-vms`
管理対象ディスクを使用	`Yes`

設定	値
仮想ネットワーク	ポッドの仮想ネットワーク。
サブネット	`vmw-hcs-podID-net-tenant`

13 ペインの下部にある [作成] ボタンをクリックして仮想マシンのデプロイを開始します。

結果

Microsoft Azure は新しい仮想マシンのリソース グループへのデプロイを開始します。Microsoft Azure で仮想マシンが正常にデプロイされると、Horizon Cloud コンソールの [インポートされた仮想マシン] ページに仮想マシンが表示されます。このページでは、エージェント関連のコンポーネントをまだインストールしていないため、仮想マシンのエージェントの状態が `Not Paired` として表示されます。

注： 管理ディスクを使用して仮想マシンを作成することや、ポッドのプライマリ テナント サブネットに接続することや、ポッドの `base-vms` リソース グループに配置することなどの条件を遵守しているにもかかわらず、ページに仮想マシンが表示されない場合があります。これは、タグが付いていない仮想マシンをポッドが認識しないというまれに生じる問題が原因である可能性があります。この問題を回避するには、Microsoft Azure ポータルで、仮想マシンにタグを手動で追加します。タグには任意の値を指定できます。Microsoft Azure ポータルで、[仮想マシンの概要] ページで、[タグ（変更）] が表示されたら、[変更] をクリックして、タグを追加します。[インポートされた仮想マシン] ページを更新します。

次のステップ

仮想マシンの完全なデプロイには数分かかることがあります。仮想マシンが作成され、準備が完了したことがポータルのダッシュボードに示されたら、仮想マシンのパブリック IP アドレスへのリモート デスクトップ接続を行い、ベース仮想マシンの構成を続行します。エージェントをインストールする前に手動で作成した仮想マシンを準備するの手順を完了させます。

エージェントをインストールする前に手動で作成した仮想マシンを準備する

Microsoft Azure でポッドの仮想マシンを手動で構築してインポートする場合、エージェントに関連するソフトウェア コンポーネントをインストールする前に、ベース仮想マシンを入念に準備するためにいくつかの追加タスクを実行する必要があります。Microsoft Azure ポータルを使用し、新しい仮想マシンに接続してこれらの手順を実行します。

仮想マシンにインストールされている Microsoft Windows オペレーティング システムのタイプに応じて、以下のトピックの手順を実行します。

Horizon Cloud が必要とするエージェントのインストールのためのサーバ仮想マシンの準備

次の手順を使用して、ポッドの RDSH ファームでの使用を予定している手動作成のサーバ仮想マシンを準備します。これらの手順は、Horizon Cloud Agent 関連のソフトウェアをインストールする前に実行します。Microsoft Azure ポータルを使用して、新しい仮想マシンに接続します。

概要レベルでは、実際にエージェントをインストールする前に仮想マシンを準備する手順は次のとおりです。

1 RDS の役割を有効にします。

2 [パスワードは無期限です] に、仮想マシンのローカル管理者アカウントのプロパティを設定します。デフォルトでは、作成された仮想マシンのローカル セキュリティ ポリシーにより、アカウントには 42 日間のパスワードの最大有効期間が設定されています。このローカル管理者アカウントのパスワードが有効期限切れにならないようにすると、このローカル アカウントが後で使用できなくなる可能性がなくなります。Horizon Cloud イメージ公開のワークフローは、仮想マシンのローカル管理者アカウントを使用し、作成されるシールドされた仮想マシンをドメインから削除します。アカウントのパスワードの有効期限が切れるようにすると、将来のある時点において、そのアカウントを使用して仮想マシンにログインすることができない状況になります。

3 Horizon Agents Installer を仮想マシンにダウンロードします。

前提条件

Microsoft Azure のポッドに仮想マシンを手動で作成する の手順を完了させます。ここで記載している手順以外で Microsoft Azure で作成したベース仮想マシンを使用している場合は、そのベース仮想マシンが Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートするに示されている条件を満たしているようにします。

注意： Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートするで説明するように、[ストレージ - 管理対象ディスクを使用] を [はい] に設定し、正しい仮想ネットワークとサブネットを使用して仮想マシンが作成されていることを確認します。そうでない場合、この仮想マシンを構成してエージェントに関連するコンポーネントをインストールした後も Horizon Cloud で使用することができなくなり、最初から作成し直す必要があります。

仮想マシンがその基準を満たしていることを事前に確認して、構成に時間を費やさないようにするには、Horizon Cloud にログインして [インベントリ仮想マシン] ページに移動し、仮想マシンが一覧表示されているか確認します。一覧表示されている場合は、仮想マシンが必要な基準を満たしているので、構成を安全に進めることができます。

手順

1 仮想マシンに接続し、Windows システムにログインします。

これを行う方法の 1 つは、Microsoft Azure ポータルの仮想マシンの詳細ページに移動し、ポータルの [接続] アクションを使用することです。

このログインはオペレーティング システムへの最初のログインであるため、Windows によりネットワーク プロンプトの質問が右側に表示されます。プロンプトは、ネットワーク上の PC、デバイス、およびその他のアイテムを自動的に検索するかを尋ねます。通常、このプロンプトを閉じるには、[いいえ] をクリックします。

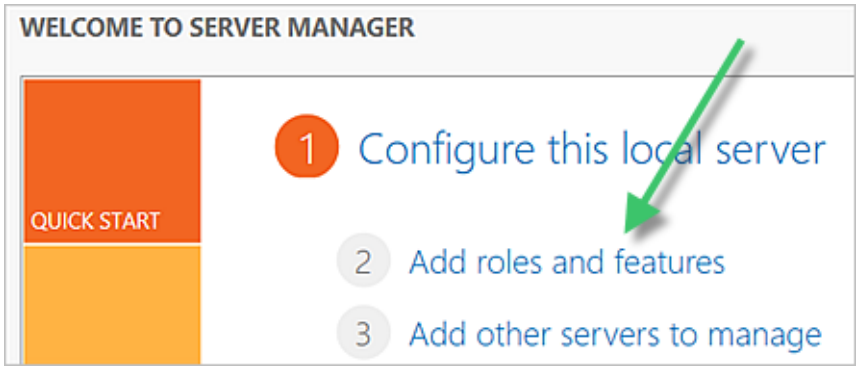
Server Manager がその初回構成ウィザードを自動的に開きます。

2 仮想マシンで RDS ロールを有効にします。

RDS ロールを有効にすると、RDSH ファームでこのサーバ仮想マシンを使用し、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できます。

a Microsoft Azure ポータルで、パワーオンした仮想マシンに接続します。

b Server Manager ダッシュボードで [ロールと機能の追加] をクリックします。



c [ロールベースまたは機能ベースのインストール] を選択して、ウィザードを進みます。

d [サーバの選択] の手順では、デフォルトの設定のままにして [次へ] をクリックします。

e [サーバ ロール] 手順で、[リモート デスクトップ サービス] を選択し、[次へ] をクリックします。

f [機能] の手順では、デフォルトの設定のままにして [次へ] をクリックします。

g クリックして [ロール サービス] 手順に進み、[リモート デスクトップ セッション ホスト] を選択します。

h オプションとして、リモート デスクトップ ライセンス診断機能ツールに関するプロンプトの設定を保持します。

i プロセスを開始します。

ウィザードが RDS の役割のインストールを開始します。画面に再起動が保留中であることが表示されたら、ウィザードを閉じて、RDP セッションを閉じます。

j Microsoft Azure ポータルで、[停止] クリックして仮想マシンを完全にパワーオフします。

k 仮想マシンが完全に停止したことがポータルに反映されたら、[開始] をクリックして再びパワーオンします。

l 前述のように、パワーオン状態である仮想マシンに再接続します。

ウィザードに [完了] の手順が表示され、成功を示すメッセージが表示されたら、[閉じる] をクリックしてウィザードを閉じます。

3 仮想マシンで、[パスワードは無期限です] に、仮想マシンのローカル管理者アカウントのパスワードを設定します。

ローカル管理者アカウントのパスワードを設定する方法の 1 つとして、`lusrmgr.msc` を実行してアカウントのプロパティを更新することで、ローカル ユーザーとグループを開くことができます方法があります。

4 Internet Explorer で一時的に Horizon Agents Installer ソフトウェアをダウンロードできるようにするには、管理者とユーザーの両方で [IE セキュリティ強化の構成] をオフにします。

次のステップ

エージェントに関連するソフトウェア コンポーネントをインストールするには、ポッドのマニフェスト バージョンに適用されるトピックに記載されている手順を実行します。

- 手動で作成した仮想マシンでのエージェント関連のソフトウェア コンポーネントのインストールおよび Horizon Cloud とのペアリング
- 廃止 - ポッドのマニフェスト バージョンが 1600 未満の場合、エージェントに関連するソフトウェア コンポーネントをベース仮想マシンにインストールする

注： ドメイン アカウントを使用して仮想マシンにログインできるようにする場合は、必要に応じて仮想マシンを Active Directory ドメインに参加させることができます。それ以外の場合は、ローカル管理者アカウントを使用して、エージェント ソフトウェアをインストールし、仮想マシンをカスタマイズするときに仮想マシンにログインします。

Horizon Cloud が必要とするエージェントのインストール用に Microsoft Windows 10 または 11 Enterprise マルチセッション仮想マシンを準備する

次の手順は、エージェントをインストールする前に、Microsoft Windows 10 または Windows 11 Enterprise マルチセッション クライアント オペレーティング システムがある仮想マシンを手動で準備するためのものです。Microsoft Azure ポータルを使用し、新しい仮想マシンに接続してこれらの手順を実行します。

注意: Microsoft のドキュメント FAQ で説明されているように、Microsoft Windows 10 または Windows 11 Enterprise マルチセッションは、以前は Microsoft Windows Server オペレーティング システム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。Horizon Cloud テナント アカウント構成でその使用が許可されている場合、Horizon Cloud 環境で Microsoft Windows 10 または 11 Enterprise マルチセッションを使用できます。

概要レベルでは、実際にエージェントをインストールする前に仮想マシンを準備する手順は次のとおりです。

1 [パスワードは無期限です] に、仮想マシンのローカル管理者アカウントのプロパティを設定します。デフォルトでは、作成された仮想マシンのローカル セキュリティ ポリシーにより、アカウントには 42 日間のパスワードの最大有効期間が設定されています。このローカル管理者アカウントのパスワードが有効期限切れにならないようにすると、後でこのローカル アカウントを使用できなくなる可能性がなくなります。Horizon Cloud イメージ公開のワークフローは、仮想マシンのローカル管理者アカウントを使用し、作成されるシールドされた仮想マシンをドメインから削除します。アカウントのパスワードの有効期限が切れるようにすると、将来のある時点において、イメージを公開するときに問題が発生する可能性があります。

2 Horizon Agents Installer を仮想マシンにダウンロードします。

前提条件

Microsoft Azure のポッドに仮想マシンを手動で作成する の手順を完了させます。これらの記載されている手順以外で Microsoft Azure で作成したベース仮想マシンを使用している場合は、ベース仮想マシンが Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートするに示されている条件を満たしていることを確認します。

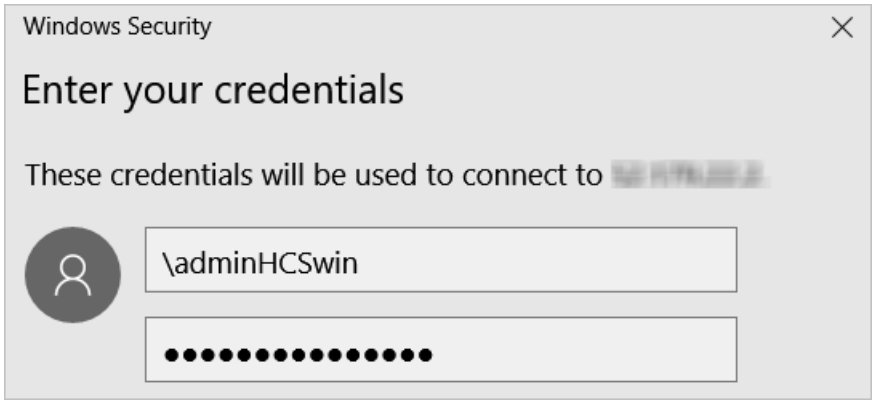
注意： Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートするで説明するように、[ストレージ - 管理対象ディスクを使用] を [はい] に設定し、正しい仮想ネットワークとサブネットを使用して仮想マシンが作成されていることを確認します。そうでない場合、この仮想マシンを構成してエージェントに関連するコンポーネントをインストールした後も Horizon Cloud で使用することができなくなり、最初から作成し直す必要があります。

構成に費やした時間を無駄にしないよう、仮想マシンがその基準を満たしていることを事前に確認するには、Horizon Cloud にログインして、[インベントリ仮想マシン] ページに移動し、仮想マシンが一覧表示されているかを確認します。一覧表示されている場合は、仮想マシンが上記の基準を満たしているので構成の手順を安心して続けることができます。

手順

1 選択した方法（RDP など）、または Microsoft Azure の Windows 仮想マシンに接続するときに通常使用する方法を使用して仮想マシンに接続します。

接続方法では、仮想マシンの作成ウィザードで指定したデフォルトのユーザー名とパスワードを使用します。ドメインなしでログインするには、ユーザー名の先頭にバックスラッシュ (\) を含めます。次のスクリーンショットは、RDP クライアントの使用例です。リモート システムに進むには、証明書に関する警告に対して [はい] を選択する必要がある場合があります。



これはオペレーティング システムへの最初のログインであるため、Windows によりネットワーク プロンプトの質問が右側に表示される場合があります。プロンプトは、ネットワーク上の PC、デバイス、およびその他のアイテムを自動的に検索するかを尋ねます。ネットワーク プロンプトが表示される場合は、[いいえ] をクリックして閉じます。

2 仮想マシンで、[パスワードは無期限です] に、仮想マシンのローカル管理者アカウントのパスワードを設定します。

ローカル管理者アカウントのパスワードを設定する方法の 1 つとして、`lusrmgr.msc` を実行してアカウントのプロパティを更新することで、ローカル ユーザーとグループを開くことができます方法があります。

次のステップ

エージェントに関連するソフトウェア コンポーネントをインストールするには、ポッドのマニフェスト バージョンに適用されるトピックに記載されている手順を実行します。

- 手動で作成した仮想マシンでのエージェント関連のソフトウェア コンポーネントのインストールおよび Horizon Cloud とのペアリング
- 廃止 - ポッドのマニフェスト バージョンが 1600 未満の場合、エージェントに関連するソフトウェア コンポーネントをベース仮想マシンにインストールする

注： ドメイン アカウントを使用して仮想マシンにログインできるようにする場合は、必要に応じて仮想マシンを Active Directory ドメインに参加させることができます。それ以外の場合は、ローカル管理者アカウントを使用して、エージェント ソフトウェアをインストールし、仮想マシンをカスタマイズするときに仮想マシンにログインします。

Horizon Cloud が必要とするエージェントのインストールのための VDI デスクトップ仮想マシンの準備

次の手順は、エージェントをインストールする前に、Microsoft Windows クライアント オペレーティング システムがある仮想マシンを手動で準備するためのものです。Microsoft Azure ポータルを使用し、新しい仮想マシンに接続してこれらの手順を実行します。

概要レベルでは、実際にエージェントをインストールする前に仮想マシンを準備する手順は次のとおりです。

1 [パスワードは無期限です] に、仮想マシンのローカル管理者アカウントのプロパティを設定します。デフォルトでは、作成された仮想マシンのローカル セキュリティ ポリシーにより、アカウントには 42 日間のパスワードの最大有効期間が設定されています。このローカル管理者アカウントのパスワードが有効期限切れにならないようにすると、後でこのローカル アカウントを使用できなくなる可能性がなくなります。Horizon Cloud イメージ公開のワークフローは、仮想マシンのローカル管理者アカウントを使用し、作成されるシールドされた仮想マシンをドメインから削除します。アカウントのパスワードの有効期限が切れるようにすると、将来のある時点において、イメージを公開するときに問題が発生する可能性があります。

2 Horizon Agents Installer を仮想マシンにダウンロードします。

前提条件

Microsoft Azure のポッドに仮想マシンを手動で作成する の手順を完了させます。これらの記載されている手順以外で Microsoft Azure で作成したベース仮想マシンを使用している場合は、ベース仮想マシンが Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートするに示されている条件を満たしていることを確認します。

注意： Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートするで説明するように、[ストレージ - 管理対象ディスクを使用] を [はい] に設定し、正しい仮想ネットワークとサブネットを使用して仮想マシンが作成されていることを確認します。そうでない場合、この仮想マシンを構成してエージェントに関連するコンポーネントをインストールした後も Horizon Cloud で使用することができなくなり、最初から作成し直す必要があります。

構成に費やした時間を無駄にしないよう、仮想マシンがその基準を満たしていることを事前に確認するには、Horizon Cloud にログインして、[インベントリ仮想マシン] ページに移動し、仮想マシンが一覧表示されているかを確認します。一覧表示されている場合は、仮想マシンが上記の基準を満たしているので構成の手順を安心して続けることができます。

手順

1 仮想マシンに接続し、Windows システムにログインします。

これを行う方法の 1 つは、Microsoft Azure ポータルの仮想マシンの詳細ページに移動し、ポータルの [接続] アクションを使用することです。

このログインはオペレーティング システムへの最初のログインであるため、Windows によりネットワーク プロンプトの質問が右側に表示されます。プロンプトは、ネットワーク上の PC、デバイス、およびその他のアイテムを自動的に検索するかを尋ねます。通常、このプロンプトを閉じるには、[いいえ] をクリックします。

2 仮想マシンで、[パスワードは無期限です] に、仮想マシンのローカル管理者アカウントのパスワードを設定します。

ローカル管理者アカウントのパスワードを設定する方法の 1 つとして、`lusrmgr.msc` を実行してアカウントのプロパティを更新することで、ローカル ユーザーとグループを開くことができます方法があります。

次のステップ

エージェントに関連するソフトウェア コンポーネントをインストールするには、ポッドのマニフェスト バージョンに適用されるトピックに記載されている手順を実行します。

- 手動で作成した仮想マシンでのエージェント関連のソフトウェア コンポーネントのインストールおよび Horizon Cloud とのペアリング
- 廃止 - ポッドのマニフェスト バージョンが 1600 未満の場合、エージェントに関連するソフトウェア コンポーネントをベース仮想マシンにインストールする

注： ドメイン アカウントを使用して仮想マシンにログインできるようにする場合は、必要に応じて仮想マシンを Active Directory ドメインに参加させることができます。それ以外の場合は、ローカル管理者アカウントを使用して、エージェント ソフトウェアをインストールし、仮想マシンをカスタマイズするときに仮想マシンにログインします。

手動で作成した仮想マシンでのエージェント関連のソフトウェア コンポーネントのインストールおよび Horizon Cloud とのペアリング

このドキュメント ページでは、Horizon Cloud に必要で適切なエージェントに関連するコンポーネントを手動でインストールし、仮想マシンをクラウド プレーンとペアリングする手順について説明します。ベース仮想マシンの Windows オペレーティング システムでは、Horizon Agents Installer を実行します。仮想マシンを再起動した後、Horizon Cloud 管理コンソールを使用して、仮想マシンとクラウド プレーンをペアリングします。

このタスクを実行するときは、次の点に注意してください。

- このドキュメント トピックの手順は、サポートされているマニフェスト バージョンのポッドを対象としています。Horizon Cloud on Microsoft Azure ポッド マニフェストのサポート ステートメントについては、VMware KB86476 を参照してください。ポッドの詳細ページを使用してポッドのマニフェスト バージョンを確認するには、「3 章 第 1 世代テナント - 第 1 世代 Horizon Cloud がサポートするすべてのポッド タイプのクラウド接続ポッドの管理」を参照してください。

  ポッドのマニフェスト バージョンが 1600 未満の場合は、これらの手順を使用しないでください。1600 未満のマニフェストはジェネラル サポートの終了に達しました。マニフェストが 1600 未満のポッドの場合、このページの手順は失敗します。

- ポッドのマニフェスト レベルに適したバージョンの Horizon Agents Installer を使用して、エージェントに関連するソフトウェアをインストールする必要があります。ポッドのマニフェスト バージョンと一致する Horizon Agents Installer のバージョンについては、Horizon Cloud リリース ノートで、ポッドのマニフェスト バージョンを示すセクションを見つけます。対応する Horizon Agents Installer バージョンが近くに表示されます。

- ポッドのマニフェスト レベルに適したバージョンよりも 4 つ以上古いバージョンの Windows 仮想マシンに Horizon Agents Installer をインストールすると、イメージ仮想マシンに基づいてファームと VDI デスクトップ割り当てを作成するときに、ダウンストリームの問題が発生する可能性があります。たとえば、古いバージョンの Horizon Agents Installer をインストールしたイメージ仮想マシンに基づいてファームを作成すると、システムはプロトコルとして HTML Access (Blast) を選択する場合があります。ただし、この選択は、正常に適用されたように見えてもファームの RDS 仮想マシンには適用されません。

- 仮想マシンで Windows 11 OS タイプ（単一セッションまたはマルチセッション）が実行されている場合は、Horizon Agents Installer バージョン 22.1 以降を使用する必要があります。

- ヘルプデスクのプラグイン オプションがデフォルトでインストールされます。このオプションをインストールしない場合、このイメージに基づくデスクトップ インスタンスまたはファーム RDSH インスタンスのユーザー セッションからのパフォーマンス関連のメトリックは収集されません。そのため、このようなセッションでは、ユーザー カードで一部のデータが入手できなくなります。詳細については、第 1 世代テナント - ユーザー カード機能（別称：Horizon Cloud のヘルプ デスク）についてを参照してください。

- デフォルトでは、Horizon Monitoring Service Agent オプションがインストールされています。このオプションをインストールしない場合、このイメージに基づく VDI デスクトップ インスタンスまたはファーム マルチセッション インスタンスのユーザー セッションからのアクティビティ関連データはクラウド プレーンに報告されません。その結果、エンドユーザー アクティビティや他の種類のデスクトップ アクティビティのデータは、Workspace ONE Intelligence コンソールの関連レポートには表示されません。

- デフォルトでは、App Volumes Agent オプションは有効ではありません。このオプションを選択すると、App Volumes Agent がインストールされます。これにより、この仮想マシンを使用して、Horizon Cloud ポッドで使用するためにサポートされている App Volumes 機能を利用できます。Microsoft Azure 上の Horizon Cloud の App Volumes アプリケーション - 概要および前提条件を参照してください。
- デフォルトでは、Dynamic Environment Manager オプションは有効ではありません。このオプションを選択すると、FlexEngine と呼ばれる VMware Dynamic Environment Manager クライアント コンポーネントがインストールされます。このオプションを選択すると、標準モードを使用して FlexEngine がインストールされます。標準モードでは、VMware Dynamic Environment Manager グループ ポリシーを構成するためのインストール後の構成手順が必要です。VMware Dynamic Environment Manager の使用の詳細については、Dynamic Environment Manager の製品ドキュメントを参照してください。VMware Dynamic Environment Manager は、ポッドによってプロビジョニングされるデスクトップのエンドユーザー データ、設定、およびプロファイルの維持に必要な各種オプションを提供します。

  注： インストールに Dynamic Environment Manager オプションを選択すると、インストール パスは `C:\Program Files\VMware\Horizon Agents\User Environment Manager` になります。

前提条件

Microsoft Azure のポッドに仮想マシンを手動で作成する および エージェントをインストールする前に手動で作成した仮想マシンを準備する の説明に従って、仮想マシン (VM) が作成および構成されていることを確認します。

ポッドのマニフェスト レベルに適したバージョンの Horizon Agents Installer があることを確認します。ポッドのマニフェスト バージョンは、3 章 第 1 世代テナント - 第 1 世代 Horizon Cloud がサポートするすべてのポッド タイプのクラウド接続ポッドの管理 のポッドの詳細ページで確認できます。ポッドのマニフェスト バージョンと一致する Horizon Agents Installer のバージョンを確認するには、Horizon Cloud リリース ノートで、ポッドのマニフェスト バージョンを示すセクションを見つけます。

App Volumes Agent をインストールして、この仮想マシンがポッドの App Volumes 機能を利用できるようにする場合は、エージェントがポッドで実行されている App Volumes Manager と通信するために使用する IP アドレスが必要です。エージェント オプションで App Volumes Agent が選択されている場合、Horizon Agents Installer に、[App Volumes Manager の IP アドレスを指定] と表示されます。使用する IP アドレスは、ポッドの詳細ページの [ポッド マネージャのロード バランサの IP アドレス] ラベルの横にあります。次の画像は、ポッドの詳細ページと [ポッド マネージャのロード バランサの IP アドレス] の場所の例です。

手順

1 インストーラのダウンロード場所に移動して起動します。

重要： このベース仮想マシンによって生成されるデスクトップまたは RDS ベースのリモート アプリケーションで URL リダイレクト オプションを使用する場合は、コマンドラインを使用してインストーラを起動する必要があります。コマンドには `VDM_URL_FILTERING_ENABLED=1` パラメータを追加します。

次に例を示します。

```
VMware-Horizon-Agents-Installer-x.y.z-build-x64.exe VDM_URL_FILTERING_ENABLED=1
```

この場合、*x.y.z* と *build* はファイル名の数字と一致します。

数分後、インストール ウィザードに [ようこそ] 画面が表示されます。インストーラは、クライアント オペレーティング システムで実行しているか、Remote Desktop Session Host (RDSH) タイプのオペレーティング システムで実行しているかを検出し、適切な [ようこそ] 画面を表示します。RDSH タイプのオペレーティング システムには、RDS ロールが有効になっている Microsoft Windows Server オペレーティング システムと、Microsoft Windows 10 Enterprise マルチセッション オペレーティング システムが含まれています。

- Microsoft Windows クライアント オペレーティング システムを実行している仮想マシンの場合は、Horizon Cloud Endpoint Desktop イメージが表示されます。

- Remote Desktop Session Host (RDSH) タイプのオペレーティング システムを実行している仮想マシンの場合、Horizon Cloud RDSH アプリケーション イメージが表示されます。

2 [構成] をクリックします。

ウィザードの次の手順が表示されます。次の画像は、RDSH タイプのオペレーティング システムを実行する仮想マシンでこの手順を実行する場合の例です。

注： Windows 7 Enterprise 仮想マシンの場合、Windows 7 Enterprise オペレーティング システムでの使用がサポートされているエージェント オプションのみを選択できます。

3 下にスクロールして、機能のオプションを表示します。

次の画像は、RDSH タイプのオペレーティング システムを実行する仮想マシンでこの手順を実行する場合の例です。

4 インストールする機能のチェックボックスを選択し、矢印をクリックして次の手順に移動します。

GPU を搭載した Windows RDSH タイプのオペレーティング システム仮想マシンの場合は、[3DRDSH] オプションを選択します。

注： ヘルプ デスク プラグイン オプションをインストールしない場合、このイメージに基づくデスクトップ インスタンスまたはファーム RDSH インスタンスのユーザーセッションからのパフォーマンス関連のメトリックは収集されません。そのため、このようなセッションでは、ユーザー カードで一部のデータが入手できなくなります。詳細については、第 1 世代テナント - ユーザー カード機能（別称：Horizon Cloud のヘルプ デスク）についてを参照してください。

5 USB リダイレクトを安全に使用するよう指示するメッセージが表示された場合は、[OK] をクリックします。

6 [App Volumes Agent] を選択すると、インストーラに [App Volumes Manager の IP アドレスを指定] が表示されます。前のセクションで説明したように、使用する IP アドレスは、ポッドの詳細ページの [ポッド マネージャのロード バランサの IP アドレス] ラベルの横にあります。

7 最後の手順で、[インストールを続ける] をクリックします。

インストーラがコンポーネントのインストールを開始します。

注： VMware ディスプレイアダプタをインストールするかどうかを確認するメッセージが表示されたら、[インストール] をクリックします。

すべてのコンポーネントがインストールされると、ウィザードには [終了] が表示されます。次の画像は、RDSH 対応イメージでインストーラを実行し、デフォルト オプションのみを選択したときにインストールされるコンポーネントのリストを示しています。特定のエントリは、オペレーティング システムおよび選択するオプションによって異なる場合があります。

8 完了したことがウィザードに表示されたら、[終了] をクリックします。

9 [今すぐ再起動] をクリックして、仮想マシンを再起動し、構成の変更を有効にします。

10 仮想マシンが再びパワーオンされたら、Horizon Cloud の [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、Horizon Cloud 環境とペアリングします。

a [インベントリ] - [インポートされた仮想マシン] に移動し、仮想マシンの横に仮想マシンがパワーオンされていることを示す緑色のドットが表示されていることを確認します。

エージェント ソフトウェアが仮想マシンにインストールされていても、仮想マシンはまだ Horizon Cloud とペアリングされていません。次の画像に示すように、仮想マシンの [エージェントのステータス] 列には、**ペアなし** と表示されます。

b 仮想マシンを選択し、[詳細] - [エージェント ペアリングをリセット] を選択して、仮想マシンと Horizon Cloud をペアリングします。

注： ペアリング処理は完了まで数分かかることがあります。ペアリング処理中に仮想マシンが再起動され、そのエージェントのステータスが **ペアなし** から **不明**、**有効** に変わります。円形の矢印アイコンを使用して [インポートされた仮想マシン] ページを更新し、仮想マシンの現在のステータスを確認します。

結果

[エージェントのステータス] 列に **有効** および `20.2.0` などのエージェントのバージョンが表示されると、仮想マシンのペアリング処理は完了します。次の画像は、ペアリング処理が完了した後の仮想マシンを示します。この時点で、ベース仮想マシンは、シールドされたイメージとも呼ばれる、割り当て可能なイメージを作成するための Horizon Cloud 環境の要件に準拠しています。

次のステップ

仮想マシンを Active Directory ドメインに参加させている場合は、ドメイン アカウントを使用して仮想マシンに接続し、イメージをカスタマイズすることができます。仮想マシンを Active Directory ドメインに参加させなかった場合は、ローカル管理者アカウントを使用して仮想マシンに接続し、イメージをカスタマイズできます。

壁紙などの設定や、この仮想マシンによってエンド ユーザーに提供されるアプリケーションのインストールなど、イメージの Windows オペレーティング システムをカスタマイズします。仮想マシンのパブリック IP アドレスを有効にした場合は、Microsoft リモート デスクトップ接続などの RDP クライアントの [インポートされた仮想マシン] ページに表示される IP アドレスを使用して、作成された仮想マシンに接続できます。詳細については、インポートされた仮想マシンの Windows オペレーティング システムをカスタマイズおよび次のサブトピックを参照してください。

- Microsoft Windows Server オペレーティング システムの場合：Microsoft Windows Server オペレーティング システムを搭載した Horizon Cloud のインポートされた仮想マシンの場合：組織のニーズに合わせた仮想マシンのカスタマイズ
- Microsoft Windows 10 Enterprise マルチセッション オペレーティング システムの場合：Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムを搭載した Horizon Cloud のインポートされた仮想マシンの場合：組織のニーズに合わせた仮想マシンのカスタマイズ
- Microsoft Windows クライアントタイプ オペレーティング システムの場合：Microsoft Windows クライアント オペレーティング システムを搭載した Horizon Cloud のインポートされた仮想マシンの場合：組織のニーズに合わせた仮想マシンのカスタマイズ

重要： インポートされた仮想マシンの Windows オペレーティング システムをカスタマイズ、[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に Windows イメージの最適化を決定する、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に [Windows ストア アプリを削除] オプションを使用するの説明に従ってイメージ仮想マシンを最適化することをお勧めします。

ヒント: イメージ仮想マシンをさらに調整して、VMware Blast Extreme を使用するための構成を改善するには、ベスト プラクティスとして Horizon Cloud ファームとデスクトップから最適なリモート エクスペリエンス パフォーマンスを引き出すためにゴールド イメージで実行すべき 5 つの重要な手順のガイダンスに従うことをお勧めします。もう 1 つのベスト プラクティスとして、『VMware Blast Extreme Optimization Guide』を参照し、コーデック オプションに関するガイドの推奨事項に従って、イメージ内のコーデック オプションの追加の調整を実行することです。

App Volumes Agent のインストールを選択した場合は、Microsoft Azure 上の Horizon Cloud の App Volumes アプリケーション - 概要および前提条件に記載されているサブトピックを続行して、このイメージをサポートされている App Volumes 機能と共に使用します。

Dynamic Environment Manager オプションのインストールを選択した場合は、少なくとも SMB 2 が有効になっている Microsoft Azure サブスクリプションに別のファイル サーバを構成します。次に、そのファイル サーバを使用して VMware Dynamic Environment Manager を構成します。GPO 設定も構成します。詳細については、VMware Dynamic Environment Manager（旧称 VMware User Environment Manager）のドキュメントを参照してください。

Horizon Agent の使用に関するセキュリティを強化するために、Active Directory サーバ ドメイン ポリシーの GPO（グループ ポリシー オブジェクト）を構成して、SSL および TLS プロトコルの脆弱な暗号を無効にします。SSL/TLS プロトコルを使用して通信する際の脆弱な暗号の無効化に関する Horizon Agent の情報については、VMware Horizon のドキュメントで適切な情報を参照してください。そのドキュメント ページからリンクされている Horizon Agent 情報で「脆弱な暗号」という語句を検索します。

NV シリーズまたは NVv4 シリーズの仮想マシン タイプを選択した場合は、仮想マシンのオペレーティング システムにログインし、サポートされている適切なグラフィックス ドライバをインストールして、仮想マシンの GPU 機能を取得する必要があります。仮想マシンが作成されたらドライバをインストールします。[インポートされた仮想マシン] ページには仮想マシンのエージェント状態がアクティブであることが表示されます。Horizon Cloud on Microsoft Azure - インポートした GPU 対応仮想マシンに適切な GPU ドライバをインストールするを参照してください。

Horizon Cloud 環境に関連付けられたライセンスで Workspace ONE Assist for Horizon を使用する資格が付与されていて、この仮想マシンに基づくエンドユーザー仮想セッションでリモート サポート機能を使用する場合は、Workspace ONE Assist for Horizon エージェントをこの仮想マシンにインストールします。Workspace ONE Assist for Horizon の使用方法については、VMware Workspace ONE Assist のドキュメントを参照してください。

イメージのカスタマイズが完了したら、イメージを割り当て可能なイメージに変換します。

- イメージにマルチセッション タイプのオペレーティング システムがある場合、またはテナント環境がマルチポッド イメージ管理機能を利用するための基準をまだ満たしていない場合は、[新しいイメージ] ワークフローを使用してイメージを割り当て可能なイメージに変換します。構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の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。
- イメージに単一セッション VDI タイプのオペレーティング システムがあり、テナント環境でマルチポッド イメージ管理機能が使用可能な場合は、マルチポッド イメージに移動ワークフローを実行することで、これらの機能でこのイメージを使用できます。2021 年 7 月のサービス リリースでは、すべての Horizon Cloud ポッドがマニフェスト 2632 以降で、テナントが Universal Broker を使用するように構成されている場合に、Horizon Image Management Service およびマルチポッド イメージ管理の機能が使用可能です。

  注意： [マルチポッド イメージに移動] ワークフローの使用には、特にイメージに App Volumes Agent をインストールし、それをコンソールの [マルチポッド イメージ] ページに移動して、イメージを公開し、App Volumes on Azure 機能でそのゴールド イメージを使用する予定の場合には、いくつか注意が必要です。監視対象の詳細については、「マルチポッド イメージに移動ワークフロー」ページを参照してください。

廃止 - ポッドのマニフェスト バージョンが 1600 未満の場合、エージェントに関連するソフトウェア コンポーネントをベース仮想マシンにインストールする

マニフェストが 1600 未満のポッドのエージェントに関連するソフトウェアのインストールに関するこのドキュメント ページは、関連がなくなりました。これらのデプロイはジェネラル サポートが終了しました。

この廃止されたページは、自動リダイレクトが機能するようになるまで、しばらく保持されます。

- Horizon Cloud on Microsoft Azure ポッド マニフェストのサポート ステートメントについては、VMware KB86476 を参照してください。
- サポートされているマニフェストのインストール手順については、手動で作成した仮想マシンでのエージェント関連のソフトウェア コンポーネントのインストールおよび Horizon Cloud とのペアリングを参照してください。

Horizon Cloud 環境のファームと VDI デスクトップでの Microsoft Azure Disk Encryption の使用

RDSH ファームまたは VDI デスクトップ割り当てを Microsoft Azure の Horizon Cloud ポッドに作成する場合、ディスクの暗号化を有効にするかどうかを決めることができます。ファームまたは VDI デスクトップ割り当てに対してディスクの暗号化を有効にすると、そのファームまたは VDI デスクトップ割り当てに含まれるすべての仮想マシンのすべてのディスクが暗号化されます。ファームまたは VDI デスクトップ割り当てを作成するときにディスクの暗号化を指定します。ファームまたは割り当てを作成した後に、暗号化の状態を変更することはできません。

ファームおよび VDI デスクトップ割り当てを作成するワークフローには、ディスクの暗号化を有効にするためのトグルが含まれます。これらのワークフローの詳細については、次を参照してください。

- 第 1 世代 Horizon Cloud ポッド - ファームの作成と管理
- 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

注：

- このリリースでは、データ ディスクが接続されたイメージ仮想マシンを使用するフローティング VDI 割り当てのディスク暗号化をサポートしていません。

ディスク暗号化がパフォーマンスに与える影響

ディスク暗号化機能は、Microsoft Azure クラウドの Azure Disk Encryption (ADE) 機能によって提供されます。ADE では、Microsoft Windows の BitLocker 機能を使用して、Microsoft Azure の仮想マシンの OS およびデータ ディスクに暗号化を提供します。一般的に、BitLocker は 1 桁レベルの性能オーバーヘッドを課すので、暗号化された仮想マシンのパフォーマンスに著しい影響があります。仮想マシンの暗号化の欠点は、データ、ネットワーク、コンピューティング リソースの使用量を増加させ、その結果としてライセンスやサブスクリプション コストの追加になるおそれがあることです。仮想マシンは単純にディスクからデータを読み取ってデータを暗号化されていないディスクに書き込むのではなく、データを復号化して読み取り、データを暗号化してから暗号化されたディスクに再び書き込みます。このプロセスにおいては、キーを Azure 内のキー コンテナから読み込むので、ネットワーク使用量が増加し、CPU サイクルは暗号化の実行に使用されます。Microsoft のドキュメントで Azure Disk Encryption に関する FAQ および BitLocker の展開と管理のよく寄せられる質問を参照してください。

暗号化キー コンテナ

ポッドの暗号化されたファームと VDI デスクトップの割り当てに使用されるキー コンテナが、ポッドのマネージャ仮想マシンを含む同一の Microsoft Azure リソース グループに作成されます。1 つのキー コンテナはポッドのすべての暗号化ファームおよびデスクトップ割り当てに使用されます。暗号化された仮想マシンの最初の作成時に、システムは関連付けられたファームまたは VDI デスクトップの割り当てを作成し、結果的にこの暗号化キー コンテナが作成されます。最初の暗号化された仮想マシンが作成されるまで、このキー コンテナはポッドのリソース グループに表示されません。

システムはポッドの ID を使用してキー コンテナの名前を生成します。これは、UUID 形式の識別子です。Microsoft Azure の命名規則に従い、システムはキー コンテナの名前を次のように設定します。

1 ポッドの ID を取得する。

2 文字 `kv` を先頭に追加します。

3 英数字以外の文字をすべて削除します。

4 最大長を 24 文字に抑えるために必要な文字を切り詰めます。

次のスクリーンショットに、ポッドに暗号化されたファームがある場合にポッドのマネージャ仮想マシンのリソース グループにある項目を示します。スクリーンショットには、2 つのキー コンテナが示されています。1 つは、ポッドのデプロイ中に作成されたこのポッドのキー コンテナ。もう 1 つは、ディスクの暗号化が有効になっているファームまたは VDI デスクトップの割り当てが作成された結果として、最初の暗号化された仮想マシンが作成されたときに、作成されたキー コンテナです。このスクリーンショットでは、次のことを確認できます。

- ポッドの ID は、ポッドのマネージャ仮想マシンの名前の `e1c80e74-7f6f-434f-bd79-c1e3772f6c5a` です。
- 暗号化キー コンテナの名前は `kve1c80e747f6f434fbd79c1` です。これはその UUID の取得、`kv` の先頭への追加、ハイフンの削除、および名前を 24 文字にするための切り詰めによって決まります。

注意： ポッドのマネージャ仮想マシンのリソース グループにあるどのキー コンテナも削除してはいけません。暗号化キー コンテナが削除されると、暗号化された仮想マシンはパワーオンされなくなります。ポッド自体のキー コンテナが削除されると、ポッドのマネージャ仮想マシンはパワーオンされなくなります。

暗号化された仮想マシンの作成および削除

暗号化された仮想マシンごとに暗号化シークレットが使用されます。暗号化されたファームまたは VDI デスクトップ割り当てで仮想マシン インスタンスが作成されると、キー コンテナにシークレットが作成されます。暗号化されたファームまたは VDI デスクトップ割り当てから仮想マシン インスタンスが削除されると、そのシークレットはキー コンテナから削除されます。

Horizon Cloud 管理コンソールを使用して暗号化されたファームまたは VDI デスクトップ割り当てを削除すると、システムは、キー コンテナから関連付けられているシークレットを削除します。ポッド自体を削除すると、暗号化された仮想マシンのキー コンテナも削除されます。

注： 暗号化されたファーム仮想マシンまたはデスクトップ仮想マシンの作成は、暗号化されていない仮想マシンの作成の約 2 倍の時間がかかります。その結果、ディスクの暗号化が有効になっているファームまたは VDI デスクトップの割り当てを作成する場合は、無効になっている場合と比べて、開始から完了までの時間が約 2 倍かかります。

また、イメージ仮想マシンにデータ ディスクがある場合は、そのイメージ仮想マシンに基づいて、暗号化されたファーム仮想マシンまたはデスクトップ仮想マシンを作成するための追加の時間が必要になります。一般に、Windows Server オペレーティング システムを実行しているデータ ディスクを使用する仮想マシンのディスク暗号化にかかる時間は、データ ディスクを使用する Windows 10 または Windows 11 仮想マシンの場合よりも短くなります。より大きい、テラバイト単位のサイズのデータ ディスクがある Windows 10 または 11 オペレーティング システムでは、時間が最も長くかかります。

暗号化された仮想マシンが多数ある場合のファームと VDI デスクトップの割り当ての電源管理のスケジューリング

暗号化された仮想マシンをパワーオンしてから、この仮想マシンにエンド ユーザーの接続を受け入れる準備が完了するまでの時間は、暗号化されていない仮想マシンよりも長くなります。仮想マシンにあるコアの数が少ない場合、たとえは A1 サイズのときなどは、約 12 分間かかります。コア数が多くなるほど時間は短くなり、約 6 分程度になります。

予測されるエンド ユーザーの要件を満たすために、多数の仮想マシンをパワーオン状態にする電源管理機能をシステムで使用している環境で、仮想マシンが暗号化されている場合は、これらの仮想マシンにさらに時間がかかることを考慮する必要があります。システムは最大 125 台の仮想マシンを同時にパワーオンします。VDI デスクトップの割り当てまたはファームに 125 台を超える仮想マシンがあり、電源管理スケジュールで午前 8 時に割り当てまたはファームをパワーオンすると設定した場合、システムは午前 8 時に 125 台の仮想マシンのパワーオンを一度に開始します。仮想マシンが最小の A1 サイズで暗号化されている場合に、125 台の仮想マシンのバッチ処理と、接続可能になるまでにかかる 12 分を組み合わせると、準備完了までの時間はおおよそ次のようになります。

- 午前 8 時 12 分までに、125 台の仮想マシンが準備完了
- 午前 8 時 24 分までに、250 台の仮想マシンが準備完了
- 午前 8 時 36 分までに、375 台の仮想マシンが準備完了

結果として、VDI デスクトップ割り当てに小さな A1 サイズの暗号化された仮想マシンが 2,000 台ある場合、すべてをパワーオン状態にし、エンド ユーザー接続の準備が完了するまでの所要時間は約 3.5 時間になります。この暗号化された A1 サイズのデスクトップをすべて午前 8 時に準備完了の状態にする場合は、電源管理のスケジュールを午前 4 時 30 分に起動するように設定することを検討しなければなりません。

より大きなサイズの仮想マシンでは、準備完了までの時間は約半分になります。つまり 2,000 台の暗号化された仮想マシンが A4 サイズなどより大きなサイズの場合、暗号化された VDI デスクトップ割り当てがすべて完了し、エンド ユーザー接続を受け入れる準備ができるまでに 75 分程度かかります。

同様に、暗号化された VDI デスクトップの割り当てでデスクトップの数がより少ない場合、大きな 2,000 プールのサイズよりも準備完了までの時間が早くなります。500 台の小さな A1 サイズの暗号化されたデスクトップのプールの場合、プールがすべて準備完了になるまでに約 48 分かかります。仮想マシン 500 台をバッチ 1 つ分の 125 で割ると 4 バッチとなり、これに 12 分を乗算し、48 分となります。

Microsoft Azure の Horizon Cloud ポッドからの仮想デスクトップでのデータディスクの使用

データ ディスクを使用すると、エンドユーザーにデータ、アプリケーション、または追加のストレージを提供できます。[マーケットプレイスからの仮想マシンのインポート] ウィザードによって自動的に作成されたイメージ仮想マシン、または手動で作成し、Horizon Cloud 環境とペアになっているイメージ仮想マシンで、データ ディスクを使用できます。システムは、RDSH ファーム、フローティング VDI デスクトップ割り当て、および専用 VDI デスクトップ割り当てのセッションベースのデスクトップとリモート アプリケーションでのデータディスクの使用をサポートしています。ただし、割り当てタイプにはさまざまな性質があるため、使用事例はタイプごとに異なります。

データ ディスクと専用 VDI デスクトップ割り当て

専用 VDI デスクトップ割り当ては、データ ディスクの最も一般的な使用事例です。初期状態では、割り当ての仮想マシン プール内の各デスクトップ仮想マシンのデータ ディスク構成と内容は、割り当てが基づいている元のイメージ仮想マシンと同じです。使用資格が付与されたすべてのエンドユーザーに提供するデータとアプリケーションを初期データディスクに提供することがあります。専用 VDI デスクトップ割り当ての各エンドユーザーには、特定の仮想デスクトップが割り当てられます。割り当てられたエンドユーザーは、デスクトップを起動してログインするたびに、同じ仮想デスクトップに戻ります。データ ディスクはその仮想デスクトップで保持されるため、割り当てられたエンドユーザーはデータディスク上のデータを変更でき、ユーザーの変更はすべてセッション間で保持されます。

データ ディスクとフローティング VDI デスクトップ割り当て

フローティング VDI デスクトップ割り当てでは、エンドユーザーがデスクトップからログアウトすると、各仮想デスクトップの仮想マシンは元のイメージ仮想マシンの初期状態に戻ります。専用のケースと同様に、最初に割り当ての仮想マシンプール内の各デスクトップ仮想マシンのデータ ディスク構成とコンテンツは、割り当てが基づいている元のイメージ仮想マシンと同じです。また、専用の場合と同様に、使用資格が付与されたすべてのエンドユーザーに提供するデータとアプリケーションを初期データ ディスクに提供することもあります。エンドユーザーがプールからデスクトップに接続するたびに、そのエンドユーザーは、初期状態のデータディスクがあるデスクトップに接続されます。

専用のケースとは異なり、エンドユーザーがデスクトップからログアウトすると、仮想デスクトップのデータ ディスクは初期データ ディスクの構成と内容に戻されます。これらのディスクにエンドユーザーが保存した可能性のあるすべてのファイルは、ユーザーがログアウトすると失われます。

データディスクおよび RDSH ベースのデスクトップとアプリケーションの割り当て

RDSH 仮想マシンでデータディスクを使用する主な使用事例としては、共有される読み取り専用のデータまたはアプリケーションを、セッションベースのデスクトップおよび RDSH ファームからプロビジョニングされたリモート アプリケーションの使用を付与するすべてのエンドユーザーに提供することがあります。RDSH 仮想マシンに接続されているすべてのデータ ディスクは、その仮想マシンに接続するすべてのエンドユーザーが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使用できるようになります。また、エンドユーザーが資格が付与されたデスクトップまたはアプリケーションを使用するためにログインするたびに、エンドユーザーが別の仮想マシン インスタンスに接続されることがあるため、特定のエンドユーザーが以前のセッションでデータ ディスクに保存したデータにアクセスできるという保証はありません。そのため、このシナリオでは、個人データのためのデータディスクを使用することは一般的に回避されています。

はじめに

ポッドでプロビジョニングされた仮想デスクトップとリモート アプリケーションでデータ ディスクを使用できるようにするには、Microsoft Azure ポータルを使用してディスクを作成し、それらをイメージを発行する前にゴールド イメージ仮想マシンに添付します。高レベルでは、次のようになります。

1 作成したデータ ディスクを仮想マシンに接続します。

2 Microsoft azure ドキュメントのトピック Azure ポータルを使用した、管理対象データ ディスクの Windows 仮想マシンへの接続の手順に従ってこれらのデータ ディスクを初期化します。これらの手順には、必要に応じてディスクの初期化、ボリュームの定義、およびパーティションのフォーマットが含まれます。

3 データディスクに必要な初期内容を追加します。

これらの手順は、ゴールド イメージを公開イメージに変換する前に実行する必要があります。システムのイメージ公開プロセスは、イメージを封印シールドするときにデータ ディスクの初期状態をキャプチャします。イメージを公開した後、その封印されたシールドされたイメージにデータディスクを追加することはできません。データ ディスクの追加など、何らかの理由で封印されたシールドされたイメージを更新するには、Microsoft Azure での Horizon Cloud ポッドの公開イメージの管理 およびそのサブトピックの情報に従ってイメージを更新します。

Horizon Cloud で使用されるイメージ仮想マシンのデータ ディスクを準備する詳細な手順については、Horizon Cloud のイメージ仮想マシンのデータ ディスクの設定を参照してください。

仮想マシンあたりのデータ ディスク数

イメージ仮想マシン上の Horizon Cloud でサポートされるデータ ディスクの数についての現在の推奨は、最大で 5 つのデータ ディスクです。特定の仮想マシン サイズに接続できるデータディスクの数に関する Microsoft Azure ポリシーや、ポッドがデプロイされる Microsoft Azure リージョンといった追加要因によって、仮想マシンに接続できるデータディスクの数が制限される場合があります。Microsoft Azure ドキュメントのトピック Arure における Windows 仮想マシンのサイズおよび各 Microsoft Azure 仮想マシン サイズに対する最大数を示した表のさまざまな仮想マシン タイプに対するページを参照してください。

データ ディスクのライフサイクル

Horizon Cloud 管理コンソールを使用して仮想マシンを削除すると、システムは仮想マシンに関連付けられているすべてのリソースを検索し、それらのリソースを削除します。Microsoft Azure ポータルでデータ ディスクを手動で作成した場合でも、データ ディスクが Horizon Cloud の仮想マシンに接続されていると、システムは仮想マシンを削除するときにそれらのデータ ディスクを削除します。

ファーム RDSH インスタンスと VDI デスクトップ インスタンスが、データ ディスクが接続されたイメージから作成されると、RDSH およびデスクトップ仮想マシンが作成および削除される際に、システムの標準動作に応じて、それらのインスタンスのデータ ディスクが自動的に作成および削除されます。

Horizon Cloud のイメージ仮想マシンのデータ ディスクの設定

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 アプリケーションでデータ ディスクを提供するには、Microsoft Azure ポータルを使用して管理データディスクを作成し、そのデータディスクをイメージ仮想マシンに追加します。次に、データ ディスクを初期化してフォーマットします。ディスクのフォーマット後、必要に応じてディスクの初期構成で必要なコンテンツをロードすることができます。これらの手順は、イメージを公開イメージに変換する前に実行する必要があります。

Horizon Cloud では、[Marketplace からの仮想マシンのインポート] ウィザードによって自動的に作成されたイメージ仮想マシン、または手動で作成し、環境とペアになっているイメージ仮想マシンで、データ ディスクを使用できます。Horizon Cloud 環境でデータ ディスクを使用する方法については、Microsoft Azure の Horizon Cloud ポッドからの仮想デスクトップでのデータディスクの使用 を参照してください。

このトピックでは、仮想マシンが Horizon Cloud とペアリングされており、その仮想マシンにデータ ディスクが接続されていない状態ですでに存在する場合に、Horizon Cloud ポッドに関するベスト プラクティス ワークフローについて説明します。システムの自動インポート ウィザードは、データ ディスクなしで仮想マシンを作成します。基本の仮想マシンを手動で作成し、作成時にデータ ディスクを接続した場合は、仮想マシンにログインして、イメージを公開する前にデータ ディスクを初期化する必要があります。仮想マシンのデータ ディスクを初期化するには、Microsoft Azure ドキュメントのトピック新しいデータディスクの初期化に記述される手順に従います。

データ ディスクを仮想マシンに追加して初期化するための一般的な手順は、Microsoft Azure ドキュメントのトピック Azure ポータルを使用した管理対象データディスクの Windows 仮想マシンへの接続にあります。このプロセスの概要は次のとおりです。

- Microsoft Azure ポータルで、イメージ仮想マシンを特定し、データ ディスクを追加します。
- 仮想マシンにログインし、そのデータ ディスクを初期化します。

前提条件

[インポートされた仮想マシン] ページで、仮想マシンに対してエージェントに関連するステータスがアクティブになっていることを確認します。このステータスを取得するには、仮想マシンで [インポートされた仮想マシン] ページの [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ます。このアクションは、[詳細] ドロップダウン リストにあります。

[インポートされた仮想マシン] ページに表示される仮想マシンの名前および IP アドレスを取得します。この名前を使用して、Microsoft Azure ポータルのポッドのリソースグループ内の仮想マシンを見つけ、データ ディスクを仮想マシンに接続できるようにします。IP アドレスを使用して仮想マシンにログインし、接続後にデータ ディスクを初期化します。

注： Microsoft リモート デスクトップ クライアントを RDP ソフトウェアとして使用して仮想マシンに接続する場合は、それが最新のバージョンであることを確認してください。たとえば、Windows 7 オペレーティング システムのデフォルトの RDP ソフトウェアのバージョンはこの条件を満たしていません。バージョンは、バージョン 8 以降である必要があります。

仮想マシンの作成方法に応じて、仮想マシンのゲスト Windows オペレーティング システムにログインするために、認証情報（ユーザー名とパスワード）の少なくとも 1 つがあることを確認します。

仮想マシンの作成方法	ログインに使用する認証情報
[インポートされた仮想マシン] ページから、仮想マシンのインポート ウィザードを実行します。	2019 年 12 月のサービス リリース日以降、[仮想マシンのインポート] ウィザードは、作成プロセスの最後に、ウィザードで作成された仮想マシンを指定された Active Directory ドメインに参加させるか、仮想マシンをドメインに参加させないかのオプションを提供します。 ■ ウィザードの [ドメイン参加] トグルを有効にして仮想マシンが作成された場合、指定された Active Directory ドメインのドメイン アカウントの認証情報を使用するか、ウィザードで指定されたローカル管理者アカウントを使用できます。 ■ ウィザードの [ドメイン参加] トグルをオフにして仮想マシンが作成された場合、ウィザードで指定されたローカル管理者アカウントを使用する必要があります。この場合、仮想マシンはドメインに参加していないため、ログインするためのアクセス権を持つ唯一のアカウントがローカル管理者アカウントになります。
手動による準備手順 。	通常、仮想マシンを手動で構築するときに、仮想マシンを Active Directory ドメインに加える必要はありません。その仮想マシンにログインするには、次のいずれかの方法を使用します。 ■ 手動で構築された仮想マシンが Microsoft Azure ポータルで作成されたときに指定されたローカル管理者アカウントの認証情報。 ■ その仮想マシンを Active Directory ドメインに手動で参加させた場合、そのドメインのドメインアカウントの認証情報。

重要： ポッド マニフェスト バージョン 1230 以降では、ドメイン アカウントはエージェント ソフトウェアがインストールされているドメイン参加イメージ仮想マシンに直接接続できます。ポッド マニフェスト 1230 より前のバージョンでは、ドメインに参加した仮想マシンにインストールされたエージェント ソフトウェアにより、ドメイン アカウントをその仮想マシンに直接接続できませんでした。2298 より前のマニフェストはサポート対象外であり、ナレッジベースの記事 KB86476 の記載に従って更新する必要があります。

手順

1 Microsoft Azure ポータルで、イメージ仮想マシンを見つけて、仮想マシンの詳細ページを表示します。

仮想マシンを見つける 1 つの方法は、ポータルの検索バーを使用して仮想マシンを名前で検索することです。

2 ポータルの [管理対象ディスクの作成] ページで使用する仮想マシンのリソース グループをメモしておきます。

Horizon Cloud で使用されるイメージ仮想マシンは、パターン `vmw-hcs-podID-base-vms` という名前のリソース グループにあります。ここで *podID* はポッドの識別子です。Horizon Cloud 管理コンソールでは、ポッド ID が [キャパシティ] ページのポッドの詳細ページに一覧表示されます。

3 仮想マシンに新しいデータ ディスクを追加します。

a 仮想マシンの [ディスク] ページが表示されます。

b 表示されたアクションを実行して、新しいディスクを作成して接続します。

本書の執筆時点では、Microsoft Azure ポータルはこの選択に [新しいディスクを作成して接続する] というラベルを付けています。

c 画面上のフィールドに従って、必要な選択を行い、ディスクに名前を付けます。

d 仮想マシンの [ディスク] ページの上部で、[保存] をクリックして、新しいデータ ディスクの作成と仮想マシンへの接続を完了します。

この時点で、データ ディスクは接続されていますが、未初期化状態になります。

4 仮想マシンにログインします。

a Windows オペレーティング システムに接続するには、RDP ソフトウェアで仮想マシンの IP アドレスを使用します。

- パブリック IP アドレスを使用して仮想マシンを作成した場合は、その IP アドレスを RDP ソフトウェアで使用できます。
- 仮想マシンにプライベート IP アドレスがある場合は、次の 2 つの方法のいずれかを使用して RDP を実装する必要があります。
  - パブリック IP アドレスを持つ Microsoft Azure サブスクリプション内で別の仮想マシンを使用し、イメージ仮想マシンに対してアウトバウンド RDP を実行する。
  - VPN と RDP を企業のネットワーク経由でイメージ仮想マシン内で使用する

注： エージェントに関連するソフトウェア コンポーネントを実行している仮想マシンにアクセスする場合、リモート デスクトップ クライアントのバージョンは 8 以降である必要があります。そうでないと、接続に失敗します。最新のリモート デスクトップ クライアントを使用することをお勧めします。

b この前提条件に記述されるように、認証情報 (ユーザー名とパスワード) を使用して Windows オペレーティング システムにログインします。

仮想マシンの作成時に [イメージのインポート] ウィザードで指定したローカル管理者アカウントの認証情報を使用する場合は、ユーザー名を `\username` と入力します。

注： 仮想マシンがこの前提条件で記述されているように、ドメインに参加している仮想マシンであり、ローカル管理者アカウントではなくドメイン アカウントを使用したい場合は、ユーザー名を *ドメイン*`\username` と入力します。ここで *ドメイン* はドメイン名です。

5 仮想マシンで、Microsoft Azure ドキュメントのトピック新しいデータディスクの初期化に説明されているようにして、データ ディスクを初期化してフォーマットするための手順を実行します。

結果

この時点で、イメージ仮想マシンにはフォーマットされた空のデータ ディスクがあります。ディスクの初期構成でエンドユーザーに提供するコンテンツを含むデータ ディスクをロードする場合、イメージを公開するまではいつでもコンテンツを追加できます。

Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッド

ポッドで使用されている Microsoft Azure VNet が NSX Cloud 用に構成されている場合、それらのポッドのファームと VDI デスクトップ割り当てを使用して、NSX-T Data Center のネットワーク仮想化の機能を活用できま

す。これらの仮想マシンが同じテナント サブネットにある場合でも、NSX Cloud のマイクロセグメンテーション機能を使用して、ファーム RDSH インスタンスと VDI デスクトップ間のアクセスを制限することができます。

現在の Horizon Cloud Service バージョンの現在のポッド マニフェストとのこの統合でサポートされている NSX-T Data Center の特定のバージョンについては、ドキュメントのトピック Horizon Cloud - 環境、オペレーティング システム、および互換性を参照してください。

注： 既存のポッドを 1101 以前のマニフェスト バージョンからより新しいマニフェスト バージョンにアップデートしている場合、NSX Cloud 管理を有効にするために、ポッドをアップデートする前にポッドに存在していたファームおよび VDI デスクトップ割り当てをアップデート後に編集することはできません。

Horizon Cloud の統合は、NSX Cloud 管理コンポーネント（NSX Manager と Cloud Service Manager (CSM)）でサポートされます。これは、オンプレミスまたは NSX-T Data Center バージョン 3.1.1 以降で Microsoft Azure にネイティブでデプロイされます。NSX Cloud アーキテクチャおよびコンポーネントの概要については、VMware NSX-T Data Center のドキュメントの NSX Cloud アーキテクチャおよびコンポーネントを参照してください。

注： NSX Cloud 3.1.1 以降、検疫モードと非検疫モードの両方が Microsoft Azure の Horizon Cloud ポッドで使用できます。以前のリリースでは、非検疫モードのみがサポートされていました。

Microsoft Azure 環境で NSX Cloud を使用するための要件の 1 つとして、Microsoft Azure VNet とオンプレミスの NSX-T Data Center アプライアンス間の接続を確立する必要があります。Microsoft Azure では VNet VPN ゲートウェイにピアピアリングした後または接続した後に、VNet の CIDR ブロックを変更することが許されないので、VNet を VPN ゲートウェイに接続する前に、使用するすべての値を確認しておく必要があります。NSX Cloud をパブリック クラウドに接続するための高度な手順のワークフローについては、NSX-T Data Center ドキュメントのバージョン 3.1 のトピック Horizon Cloud Service と NSX Cloud の連携を参照してください。

次の表は、ポッドの RDSH 仮想マシンと VDI デスクトップ仮想マシンで NSX Cloud 機能を使用できるようにするためのエンド ツー エンドの手順概要を示しています。[詳細] 列の一部のリンクでは、関連する NSX-T Data Center バージョン 3.1 ドキュメントのトピックが表示されます。

手順概要	詳細
Horizon Cloud ポッドで使用するために Horizon Cloud を NSX Cloud と統合する	詳細については、NSX-T Data Center ドキュメントのトピック Horizon Cloud Service と NSX Cloud の連携を参照してください。 **重要：** ポッドで App Volumes 割り当てを作成する場合は、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 サブネットのポート 445/TCP を手動で開く必要があります。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。
仮想マシンを作成して、[マーケットプレイスからの仮想マシンのインポート] ウィザードを使用して Horizon Cloud にインポートします。	ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリングを参照してください。必要な NSX Agent を簡単にインストールできるようにするには、パブリック IP アドレスのオプションを選択するのがベストプラクティスです。 **注：** 仮想マシンをインポートするときは、仮想マシンを最適化するオプションを選択し、Windows 10 または 11 の場合は Windows ストア アプリを削除します。これらのオプションを使用すると、その後イメージのシール時に、Sysprep の問題を防止できます。
インポートされた仮想マシンに接続し、必要な NSX Tools をインストールします。	Horizon Cloud のインポートされたイメージ仮想マシンへの NSX Tools のインストール
イメージを発行します。	構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の割り当て可能なイメージに変換する
ファームおよび VDI デスクトップの割り当てを作成するには、そのイメージを使用して、ファームまたは割り当ての NSX Cloud 管理を有効にします。 RDSH 仮想マシンおよび VDI デスクトップ仮想マシンが作成されると、NSX Cloud インベントリに表示されます。	■ 第 1 世代 Horizon Cloud ポッド - ファームの作成と管理 ■ 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
RDSH 仮想マシンと VDI デスクトップ仮想マシンとの通信を許可する NSX Manager 内の分散ファイアウォール ルールを有効にします。	NSX Cloud はこれらの通信をデフォルトでブロックするため、ポッドからプロビジョニングされた NSX 管理対象の仮想マシンとの通信を許可するには、NSX Manager で一部の分散ファイアウォール ルールを有効にする必要があります。ポッドでプロビジョニングされた仮想マシンに対する NSX Manager で必要となるファイアウォールルールを参照してください。 NSX-T Data Center 2.4 を使用している場合、ファイアウォール ルールを有効にするだけでなく、NSX で管理されている仮想マシンに関するトラフィックを Microsoft Azure クラウドのネットワーク (アンダーレイ) を介してルーティングする転送ポリシーも追加する必要があります。ポッドでプロビジョニングされた仮想マシンに必要な転送ポリシーの NSX Manager への追加を参照してください。
NSX Cloud インベントリの RDSH 仮想マシンおよび VDI デスクトップ仮想マシンで NSX Cloud 機能を使用します。	『NSX-T Data Center 管理ガイド』で、この NSX Cloud のトピックとそのサブトピックを参照してください。

Horizon Cloud ワークフローと NSX Cloud

NSX Agent で構成されているゴールド イメージ仮想マシンを使用して、Horizon Cloud ポッドで RDSH ファームまたは VDI デスクトップ割り当てを作成する場合、そのファームまたは VDI デスクトップ割り当てで NSX Cloud 管理を有効にするかどうかを決定できます。ファームまたは VDI デスクトップ割り当ての NSX Cloud 管理を有効にすると、そのファームまたは VDI デスクトップの割り当ての仮想マシンのすべてが、NSX Cloud での使用にタグ付けされます。ファームまたは VDI デスクトップ割り当てを作成するときに NSX Cloud 管理を指定し

ます。ファームまたは割り当てを作成した後に、その状態を変更することはできません。ファームおよび VDI デスクトップ割り当てを作成する Horizon Cloud ワークフローには、ファームの RDSH インスタンスまたは VDI デスクトップ割り当ての仮想デスクトップで、NSX Cloud の使用を有効にするためのトグルが含まれます。これらのワークフローの詳細については、次を参照してください。

- 第 1 世代 Horizon Cloud ポッド - ファームの作成と管理
- 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

ファームまたは VDI デスクトップ割り当てを作成するときに [NSX Cloud 管理] トグルを [はい] に設定すると、結果ファームの RDSH 仮想マシンまたは VDI デスクトップ仮想マシンに `nsx.network=default` という名前のカスタム タグが付与されます。NSX Cloud の Public Cloud Gateway は、そのタグを持つすべての仮想マシンを管理します。NSX Cloud は、このタグを持つ構成済みの Microsoft Azure VNet 内の仮想マシンを自動的に検出し、パブリック クラウドのインベントリにこれらの仮想マシンを追加します。NSX-T Data Center の Cloud Service Manager コンポーネントを使用して、これらの仮想マシンをセキュアに管理できます。詳細については、『NSX-T Data Center 管理ガイド』のこの NSX Cloud のトピックとそのサブトピックを参照してください。

Horizon Cloud のポッドで NSX Cloud 管理機能を使用する場合は、いくつかの制限が適用されます。

- NSX Cloud 管理を有効にするファームまたは VDI デスクトップ割り当ての名前を編集することはできません。
- フローティング VDI デスクトップ割り当てにディスク暗号化と NSX Cloud 管理機能の両方を使用するには、最新バージョンの NSX Agent をインストールする必要があります。この組み合わせは、以前の NSX Agent のバージョンではサポートされません。

Horizon Cloud のインポートされたイメージ仮想マシンへの NSX Tools のインストール

NSX Cloud 管理が有効になっているファームまたは VDI デスクトップ割り当てを作成する場合は、そのファームまたは割り当てのために使用する公開されたイメージに、NSX Tools をインストールする必要があります。公開する前に、イメージ仮想マシンに NSX Tools をインストールする必要があります。仮想マシンが作成されたら NSX Tools をインストールします。[インポートされた仮想マシン] ページには、仮想マシンの Horizon Agent に関連したソフトウェアのステータスがアクティブとして表示されます。

このページの手順は、個々のイメージ仮想マシンに NSX ツールをダウンロードしてインストールする方法として説明されている NSX Cloud の方法に従っています。この方法には、NSX Cloud 環境の Cloud Service Manager (CSM) で特定されたダウンロード場所から PowerShell インストール スクリプト ファイルをダウンロードします。イメージ仮想マシンでは、そのインストール スクリプトを実行して NSX Tools のインストール バイナリをダウンロードし、インストールを実行します。この方法の詳細については、『NSX-T Data Center 管理ガイド 』の Windows 仮想マシンへの NSX Tools トピックを参照してください。

前提条件

[インポートされた仮想マシン] ページで、仮想マシンに対してエージェントに関連するステータスがアクティブになっていることを確認します。このステータスを取得するには、仮想マシンで [インポートされた仮想マシン] ページの [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ます。このアクションは、[詳細] ドロップダウン リストにあります。

注： Microsoft リモート デスクトップ クライアントを RDP ソフトウェアとして使用して仮想マシンに接続する場合は、それが最新のバージョンであることを確認してください。たとえば、Windows 7 オペレーティング システムのデフォルトの RDP ソフトウェアのバージョンはこの条件を満たしていません。バージョンは、バージョン 8 以降である必要があります。

仮想マシンの作成方法に応じて、仮想マシンのゲスト Windows オペレーティング システムにログインするために、認証情報（ユーザー名とパスワード）の少なくとも 1 つがあることを確認します。

仮想マシンの作成方法	ログインに使用する認証情報
[インポートされた仮想マシン] ページから、仮想マシンのインポート ウィザードを実行します。	2019 年 12 月のサービス リリース日以降、[仮想マシンのインポート] ウィザードは、作成プロセスの最後に、ウィザードで作成された仮想マシンを指定された Active Directory ドメインに参加させるか、仮想マシンをドメインに参加させないかのオプションを提供します。 ■ ウィザードの [ドメイン参加] トグルを有効にして仮想マシンが作成された場合、指定された Active Directory ドメインのドメイン アカウントの認証情報を使用するか、ウィザードで指定されたローカル管理者アカウントを使用できます。 ■ ウィザードの [ドメイン参加] トグルをオフにして仮想マシンが作成された場合、ウィザードで指定されたローカル管理者アカウントを使用する必要があります。この場合、仮想マシンはドメインに参加していないため、ログインするためのアクセス権を持つ唯一のアカウントがローカル管理者アカウントになります。
手動による準備手順 。	通常、仮想マシンを手動で構築するときに、仮想マシンを Active Directory ドメインに加える必要はありません。その仮想マシンにログインするには、次のいずれかの方法を使用します。 ■ 手動で構築された仮想マシンが Microsoft Azure ポータルで作成されたときに指定されたローカル管理者アカウントの認証情報。 ■ その仮想マシンを Active Directory ドメインに手動で参加させた場合、そのドメインのドメインアカウントの認証情報。

重要： ポッド マニフェスト バージョン 1230 以降では、ドメイン アカウントはエージェント ソフトウェアがインストールされているドメイン参加イメージ仮想マシンに直接接続できます。ポッド マニフェスト 1230 より前のバージョンでは、ドメインに参加した仮想マシンにインストールされたエージェント ソフトウェアにより、ドメイン アカウントをその仮想マシンに直接接続できませんでした。2298 より前のマニフェストはサポート対象外であり、ナレッジベースの記事 KB86476 の記載に従って更新する必要があります。

ダウンロードして仮想マシンにインストールすることで NSX Tools をインストールする場合は、NSX Cloud 環境の CSM のポータルにログインするための認証情報があることを確認してください。CSM を使用して、NSX Tools をインストールする PowerShell のインストール スクリプトをダウンロードする場所を識別します。CSM は NSX Cloud のコンポーネントであり、パブリック クラウドのインベントリ用の単一画面管理エンドポイントを提供します。詳細については、NSX-T Data Center のドキュメントの CSM についての説明をお読みください。

手順

1 仮想マシンの Windows オペレーティング システムに接続するには、RDP ソフトウェアで仮想マシンの IP アドレスを使用します。

- パブリック IP アドレスを使用して仮想マシンを作成した場合は、その IP アドレスを RDP ソフトウェアで使用できます。
- 仮想マシンにプライベート IP アドレスがある場合は、次の 2 つの方法のいずれかを使用して RDP を実装する必要があります。
  - パブリック IP アドレスを持つ Microsoft Azure サブスクリプション内で別の仮想マシンを使用し、イメージ仮想マシンに対してアウトバウンド RDP を実行する。
  - VPN と RDP を企業のネットワーク経由でイメージ仮想マシン内で使用する

注： エージェントに関連するソフトウェア コンポーネントを実行している仮想マシンにアクセスする場合、リモート デスクトップ クライアントのバージョンは 8 以降である必要があります。そうでないと、接続に失敗します。最新のリモート デスクトップ クライアントを使用することをお勧めします。

2 この前提条件に記述されるようにして、認証情報 (ユーザー名とパスワード) を使用して Windows オペレーティング システムにログインします。

仮想マシンの作成時に [イメージのインポート] ウィザードで指定したローカル管理者アカウントの認証情報を使用する場合は、ユーザー名を `\username` と入力します。

注： 仮想マシンがドメインに参加している仮想マシンであり、この の前提条件で説明しているように、ローカル管理者アカウントではなく、ドメインアカウントを使用する場合は、ユーザー名を *ドメイン*`\username` とします。ここで、*ドメイン*はドメイン名です。

3 Windows 仮想マシンから CSM にログインし、[クラウド] - [Azure] - [VNet] の順に移動し、ポッドの適切な VNet に移動します。

4 画面の [NSX Tools のダウンロードとインストール] を見つけて、Windows 用のダウンロード場所とインストール コマンドを取得します。

その領域内で、表示されている Windows のインストール スクリプトのダウンロード場所を特定します。シンプルで基本的なインストール コマンドもダウンロード場所にあります。

- 表示されるダウンロード場所には、パターン `http://filepath/nsx_install.ps1` があります。このパターンでは、`nsx_install.ps1` が PowerShell スクリプト ファイルであり、`filepath` がファイルをダウンロードするためのパスです。

- 表示される基本インストール コマンドには、`-dnsSuffix DNS-suffix` が含まれています。*DNS-suffix* は、DNS 設定に関連する動的に生成された値です。DNS 設定は、NSX Cloud 設定の一部として Microsoft Azure VNet に PCG をデプロイしたときに選択します。

重要： Horizon Cloud でイメージ仮想マシンの NSX Tools をインストールするスクリプトを実行する場合、以下を指定する必要があります。

- Microsoft Azure VNet の CSM に表示されるのと同じ *DNS-suffix*。*DNS-suffix* は、ユーザーの設定環境に対し一意である。
- `startOnDemand true` オプション。このオプションは、Horizon Cloud 公開ワークフローのために NSX Tools を最適化します。

5 表示された *DNS-suffix* をコピーし、次の手順でインストール スクリプトを実行するときに使用します。

6 ダウンロード場所を使用して、仮想マシン上の場所に `nsx_install.ps1` ファイルをダウンロードします。

7 PowerShell プロンプトを開き、nsx_install.ps1 ファイルをダウンロードした場所に移動し、*DNS-suffix* の値とオプション `-startOnDemand true` を使用してインストール コマンドを実行し、NSX Tools をインストールします。

重要： オプション -startOnDemand true が必要です。

次のコード ブロックは、`xxxxxxxxxxxxxxxxxxxxxxxx.xx.internal.cloudapp.net` の *DNS-suffix* の例を含む PowerShell プロンプト内のコマンドの例です。

```
powershell -file 'nsx_install.ps1' -operation install -dnsSuffix
xxxxxxxxxxxxxxxxxxxxxxxx.xx.internal.cloudapp.net -startOnDemand true
```

スクリプトの実行が完了すると、NSX Tools が正常にインストールされているかどうかを示すメッセージが表示されます。

8 PowerShell コマンド プロンプトを閉じます。

9 通常のコマンド プロンプトを開き、次のコマンドを実行して、NSX Tools のブートストラップ ステータスが準備完了であることを確認します。

```
schtasks /query /tn nsx_bootstrap
```

このコマンドを実行すると、nsx_bootstrap タスクが `Ready` ステータスであることが表示されます。以下に例を示します。

```

TaskName              Next Run Time       Status
--------------------- ------------------- -----------
nsx_bootstrap         N/A                 Ready
```

10 仮想マシンの Windows オペレーティング システムからログアウトします。

次のステップ

NSX Tools がインストールされ、`Ready` タスクが `nsx_bootstrap` として表示されている状態でそれ以上のカスタマイズを行わない場合、イメージを発行できます。構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の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。

ポッドでプロビジョニングされた仮想マシンに対する NSX Manager で必要となるファイアウォールルール

Microsoft Azure のポッドで NSX Cloud 機能を使用する場合は、ポッドからプロビジョニングされた NSX で管理されている仮想マシンとの通信を許可するために、NSX Manager で一部の分散ファイアウォール ルールを有効にする必要があります。これらのルールを有効にしないと、エンドユーザーはデスクトップまたはリモート アプリケーションを起動してログインできなくなります。

NSX Manager では、これらのルールを有効にして、トラフィックを指示どおりに許可します。表で、デスクトップ プールという語句は、RDSH ファームまたは VDI デスクトップ割り当てを指します。

トラフィック タイプ	ソース	送信先	サービス/プロトコル/ポート
Horizon HTML Access (Blast) トラフィック	ポッドの Unified Access Gateway 仮想マシン	デスクトップ プール	■ VMware-View-PCoIP/TCP/4172 ■ VMware-View5.x-PCoIP/UDP/4172 ■ HTTPS/TCP/443 ■ Horizon Blast UDP/UDP/22443 ■ Horizon Blast TCP/TCP/22443 ■ Horizon-USB-RedirectionIn/TCP/32111 ■ Horizon-Beat/TCP-8443 ■ Horizon-TCP-Side-Channel/TCP/9427
デスクトップ プールからポッド マネージャへのトラフィック	デスクトップ プール	ポッドのマネージャ仮想マシン	■ VMware-View5.x-JMS/TCP/4001 ■ デスクトップ メッセージング サーバ/TCP/3099 ■ VMware-View7/TCP/4002
デスクトップ プールから Active Directory ドメイン サーバへのトラフィック	デスクトップ プール	ポッドのマネージャ仮想マシン	■ 任意

ポッドでプロビジョニングされた仮想マシンに必要な転送ポリシーの NSX Manager への追加

Microsoft Azure 内のポッドで NSX-T Data Center 2.4 を使用している場合は、ファイアウォールのルールを有効にするだけでなく、Microsoft Azure クラウドのネットワーク（アンダーレイ）経由でそのポッドの NSX で管理された仮想マシンに関するトラフィックをルーティングする転送ポリシーを追加する必要があります。転送ポリシーは、NSX-T Data Center 2.4 で導入されました。

NSX-T Data Center 2.4 環境で次の手順を実行します。

手順

1 環境の NSX Manager にログインします。

2 [ネットワーク] - [転送ポリシー] の順に移動します。

3 [転送ポリシー] ページで、ポッドの使用に NSX Public Cloud Gateway (PCG) がデプロイされている VNet を示すセクションを展開します。

4 展開したセクションで、右クリックして [ルールのコピー] を選択することで、そのセクションにリストされている最後のルール（`CloudDefaultRoute` という名前）のコピーを作成します。

5 新しいコピーのアクションを [アンダーレイへのルート] に設定します。

6 [公開] をクリックします。

Horizon Universal Console でのファームと割り当ての仮想マシン タイプとサイズの管理

[仮想マシンのタイプとサイズ] ページ（[設定] - [仮想マシンのタイプとサイズ]）では、ファームと割り当てを作成するための仮想マシンのタイプとサイズを管理できます。

Horizon Cloud Service on Microsoft Azure での使用がサポートされている特定の Microsoft Azure 仮想マシンのタイプおよびサイズのリストについては、ナレッジベースの記事 Horizon Cloud Service on Microsoft Azure での Microsoft Azure 仮想マシンのタイプとサイズ (KB77120)を参照してください。この記事に記載されているように、Microsoft Azure で使用可能な一部の仮想マシンのタイプとサイズは、Horizon Cloud Service on Microsoft Azure では使用できません。

Microsoft Azure の ポッドの場合は、ファームとデスクトップ割り当ての作成ウィザードの [モデル] ドロップダウン メニューに表示される仮想マシンを選択できます。[モデル] ドロップダウン メニューで仮想マシンのフィルタに使用できるカスタム タグを追加することもできます。このリストをフィルタする方法の詳細については、第 1 世代 Horizon Cloud ポッド - ファームの作成と管理、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、または 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 のいずれかのトピックを参照してください。フィルタ オプションは、3 つのケースすべてで同じように機能するため、オプションを説明する情報はこれら 3 つのトピックで同じです。

重要： 本番環境では、ファームとデスクトップ割り当てに使用する仮想マシン モデルに少なくとも 2 個の CPU が確実に搭載されているようにします。VMware のスケール テストでは、2 個以上の 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にのみ使用する必要があります。

[仮想マシンのタイプとサイズ] ページ ([設定] - [仮想マシンのタイプとサイズ]) には、すべてのリージョンの Azure で使用可能なすべての仮想マシンのリストが表示され、毎週更新されて、追加された新しい仮想マシンが含まれます。仮想マシン リストの上部にあるドロップダウン メニューを使用して、リージョンごとにフィルタできます。

注： フィルタが適用されている間、選択したリージョンで仮想マシンのタイプとサイズがサポートされていないことを示すメッセージが表示される場合があります。メッセージが短時間だけ表示されて消える場合、そのメッセージは無視してかまいません。

[タグの追加] と [タグの削除] ボタンを使用して、仮想マシンのカスタム タグを管理できます。詳細については、次の表の [タグ] フィールドの説明を参照してください。

Horizon Cloud で動作しないために VMware がリストから削除した仮想マシン、または Microsoft がその他の理由で利用できないようにした仮想マシンがあります。使用したい Azure 仮想マシンがリストに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。

各仮想マシンについて表示される情報を次の表に示します。

フィールド	説明
表示	仮想マシンが、ファームおよびデスクトップ割り当て作成ウィザードの [モデル] ドロップダウン メニューに表示されるかどうかを示します。デフォルトでは、このオプションはすべての仮想マシンに対して選択されます。
仮想マシン名	仮想マシンの名前
タグ	仮想マシンに適用できるタグには 2 つのタイプがあります。 ■ システム タグ - これらのタグはハードコードされており、編集できません。現在、唯一のシステムレベルのタグは「VMware 推奨」です。これは VMware が推奨する仮想マシン構成に適用されます。これらの推奨される仮想マシン サイズは、VMware が一般的な Horizon Cloud RDS ファームと VDI ワークロードの価格対パフォーマンスの比率を最適化することを決定したサイズです。ただし、ビジネスのニーズによっては、この VMware 推奨リストに含まれていない仮想マシン サイズが必要になる場合があります。仮想マシン サイズがこの推奨リストに含まれていない場合でも、必ずユースケースと要件を満たす仮想マシン サイズを選択してください。 ■ カスタム タグ - これらは独自のタグであり、ユーザーが作成して仮想マシンに適用します。ファームおよびデスクトップ割り当て作成ウィザードでモデルを選択するときに、これらのタグを基準にしてフィルタすることができます。 仮想マシンにカスタム タグを追加するには： a 仮想マシンのチェック ボックスをオンにします。 b [タグの追加] をクリックします。 c タグをカンマで区切って入力し、[追加] をクリックします。 仮想マシンからカスタム タグを削除するには： a 仮想マシンのチェック ボックスをオンにします。 b [タグの削除] をクリックします。 c 削除するタグを選択し、[保存] をクリックします。
vCPU	仮想マシンの vCPU の数。
RAM	仮想マシンの RAM のサイズ。
データ ディスク	仮想マシンのデータ ディスクの数。

ネストされた Active Directory ドメイン組織単位の使用についての考慮事項

Horizon Universal Console を使用してファームまたは VDI デスクトップ割り当てを作成する場合、[コンピュータの OU] フィールドを使用し、ファームの仮想マシンまたは VDI デスクトップ仮想マシンが配置される Active Directory 組織単位 (OU) をオプションで指定できます。これらの手順を使用して、組織が [コンピュータの OU] フィールドで使用するネストされた OU 情報を特定することができます。

注： Microsoft は、個々の OU を 64 文字以内に制限します。64 文字を超える OU パスは、個々の OU が 64 文字を超えていなければ、有効です。ただし、個々の OU はそれぞれ 64 文字以内である必要があります。

その結果、コンソールの Active Directory ページの [デフォルト OU] フィールドと、ファームと VDI デスクトップ割り当ての [コンピュータの OU] フィールドに、`OU =` の部分を除き 64 文字までの OU を入力できます。

これらの手順を使用して、組織の Active Directory ドメイン サーバでネストされた OU 情報を特定します。

手順

1. お使いの Active Directory マシンで、[Active Directory ユーザーとコンピューター] を開きます。
2. [表示] > [高度な機能]（有効になっている高度な機能）を選択します。
3. デスクトップを配置する組織単位に移動します。
4. 右クリックして、[プロパティ] を選択します。
5. [属性エディター] をクリックし、distinguishedName を選択します。
6. [表示] をクリックします。
7. コンソールの [コンピュータの OU] フィールドに識別名情報を入力します。

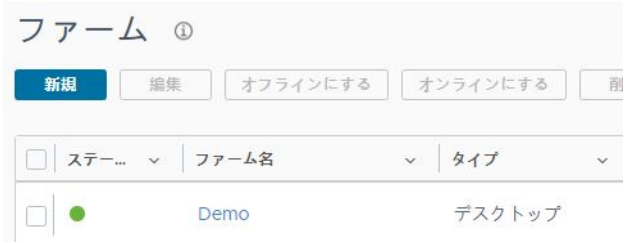
   文字列の `OU=` 部分のみが必要です。`DC=` 部分は省略できます。

Horizon Cloud のファーム

ファームは、複数のユーザーに対してセッションベースのデスクトップとアプリケーションを提供する Microsoft リモート デスクトップ サービス (RDS) ホストのコレクションです。ファームは RDS ホストの管理を簡素化します。ファームを作成して、異なるサイズ、または異なるデスクトップ要件あるいはアプリケーション要件を持つユーザー グループを処理できます。

セッションベースのデスクトップまたはリモート アプリケーションをエンド ユーザーに割り当てるには、それらのデスクトップおよびアプリケーションを提供するファームを作成する必要があります。ファームは、セッションベースのデスクトップまたはリモート アプリケーションのいずれかを提供できます。

ファームを管理するには、[ファーム] ページを使用します。テナント環境で、[インベントリ] - [ファーム] を選択して、[ファーム] ページに移動します。

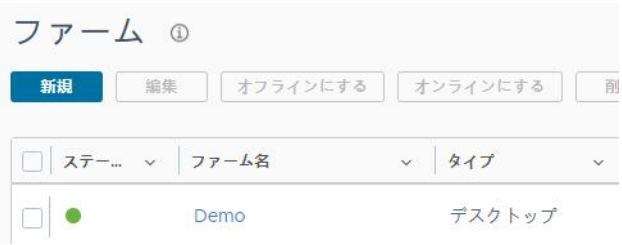


第 1 世代 Horizon Cloud ポッド - ファームの作成と管理

このドキュメント ページでは、第 1 世代 Horizon Cloud テナントでファームを作成する方法と、作成後にファームとそのマルチセッション仮想マシンのプールを管理する方法について説明します。

Horizon Cloud では、ファームを作成して、複数のユーザー セッションを同時に処理できるホストからエンド ユーザーにデスクトップ セッションまたはリモート アプリケーションをプロビジョニングできるようにします。

ファームを作成すると、複数セッション マシンのプールで構成されます。これらのマルチセッション マシンは、Microsoft Windows Server 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あるか、Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムを実行している仮想マシンです。コンソールの [ファーム] ページを使用してファームを作成します。



デフォルトでは、Horizon Cloud ファームはローリング メンテナンスで構成されています。ファームのローリング メンテナンスの実施例については、ファームのローリング メンテナンスの例を参照してください。

注： Microsoft Windows 10 または 11 マルチセッション 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をプロビジョニングし、そのデスクトップで App Volumes アプリケーションを使用できるようにするには、デスクトップ タイプのファームを作成します。App Volumes Agent をインストールしたシールドされたマルチセッション Microsoft Windows 10 または 11 イメージを指定します。

前提条件

- 少なくとも 1 つのイメージが [イメージ] ページにリストされ、そのイメージにマルチセッション Windows オペレーティング システムがあり、[イメージ] ページでそのイメージが [公開済み] の状態であり、ファームを作成する Horizon Cloud ポッドにそのイメージが配置されていることを確認します。利用できるイメージがないポッドにはファームを作成することはできません。
- このファームの仮想マシンをポッドのプライマリ仮想マシン サブネット（テナント サブネットともいいます）とは異なる仮想マシン サブネットに接続するかどうかを決定します。ポッドでマニフェスト 2298 以降が実行されていて、仮想マシン サブネットをさらに追加するためにポッドを編集してある場合は、そのサブネットをこのファームに使用するよう指定できます。このユースケースでは、使用する仮想マシン サブネットが `Ready` の

状態でポッドの詳細ページの [ネットワーク] セクションに表示されていることを確認する必要があります。これにより、そのサブネットがワークフローの手順で選択できるようになります。詳細については、ファーム用および VDI 割り当て用 Horizon Cloud ポッドでの複数のテナント サブネットの使用の概要 を参照してください。

- このファームをセッションベースのデスクトップとして使用するか、リモート アプリケーションとして使用するかを決定します。今回のリリースでは、同じファームを両方の目的で使用することはできません。

  注： エンド ユーザーが Microsoft Windows 10 または 11 マルチセッション オペレーティング システムからの App Volumes アプリケーションを使用できるようにするには、そのユーザーに App Volumes アプリケーション割り当てとセッションベースのデスクトップ割り当ての両方の使用資格を付与する必要があります。このシナリオでは、デスクトップ ファームを作成し、そのファームに基づいてセッションベースのデスクトップを提供します。そのデスクトップ ファームを作成する場合は、Microsoft Windows 10 または 11 マルチセッション オペレーティング システムで作成した公開イメージを選択します。

- ファームのマルチセッション仮想マシンで暗号化されたディスクを使用するかどうかを決定します。ファームを作成するときは、ディスクの暗号化を指定する必要があります。ファームを作成した後はディスク暗号化を追加できません。ディスクの機能の詳細については、Horizon Cloud 環境のファームと VDI デスクトップでの Microsoft Azure Disk Encryption の使用を参照してください。

- ファームの仮想マシンで NSX Cloud 機能を使用できるようにするかどうかを決定します。ファームを作成するときに、NSX Cloud 管理を有効にする必要があります。ファームの作成後に、NSX Cloud 管理のファームを有効にすることはできません。このファーム用に選択する公開イメージには、NSX Agent がインストールされていることが必要です。イメージの公開前に NSX Agent をインストールする必要があります。Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッド とそのサブトピックを参照してください。

- イメージのオペレーティング システムにユニバーサル Windows プラットフォーム (UWP) アプリケーションが含まれている場合は、エンド ユーザーがこれらの UWP アプリケーションをファームの仮想マシンから使用できるよう、使用する方法を決定します。1 つの例として、イメージに Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムがある場合があります。これらの UWP アプリケーションの使用を有効にするために選択した方法によって、ファームで使用する Active Directory の組織単位 (OU) が決まります。詳細については、Horizon Cloud での Microsoft Windows 10 または 11 Enterprise マルチセッション RDSH 仮想マシンからのユニバーサル Windows プラットフォーム (UWP) アプリケーションの実行を許可するために Horizon Agent ポリシーを有効化するを参照してください。

手順

1. 管理コンソールで、[インベントリ] - [ファーム] に移動します。
2. [新規] をクリックしてウィザードを開始します。
3. 必要に応じて選択を完了し、次の手順に進みます。

   注： 必要に応じてスクロール バーを使用して、すべての必須フィールドを表示します。

オプション	説明
名前	このファームの名前を入力します。
説明	説明を入力します（オプション）。

オプション	説明
仮想マシン名	このファーム用に作成されたすべてのマルチセッション仮想マシンの基底名。仮想マシンの基底名の末尾には数字（win2016-1、win2016-2 など）が付加されます。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。
ファーム タイプ	このファームがエンド ユーザーに提供するアセットのタイプを指定します。 ■ このファームを使用してセッションベースのデスクトップを提供するには、[デスクトップ] を選択します。 ■ このファームを使用してリモート アプリケーションへのアクセスを提供するには、[アプリケーション] を選択します。アプリケーション ファームを作成した後、新規アプリケーション ワークフローの [ファームからの自動スキャン] オプションを使用して、ファームの仮想マシンのオペレーティング システムからアプリケーション インベントリにアプリケーションをインポートできます。
場所	複数セッション イメージを持つポッドに関連付けられている場所を選択します。この選択は、[ポッド] フィールドの項目をフィルタし、選択した場所のポッドのみを表示します。
ポッド	ポッドを選択します。 **ヒント:** 選択するポッドが表示されない場合は、[場所] リストにポッドがない場所が表示されていないことを確認します。[場所] フィールドは [ポッド] リストに表示され、選択した場所に関連付けられていないポッドを除外します。すでに場所にポッドがあり、そのポッドを削除するか別の場所に移動して、表示された場所にポッドが存在しなくなると、[ポッド] リストにはエントリが表示されなくなります。場所はアルファベット順に表示されているため、画面を開くと、アルファベット順で最初の場所が自動的に選択されます。その場所にポッドが関連付けられていない場合は、場所を別のエントリに切り替える必要があります。
[仮想マシン サブネットの指定]	このトグルを有効にすると、ファームの仮想マシンの接続先とする特定のサブネットを 1 つ以上選択できます。トグルを有効にしたら、表示される一覧から特定のサブネットを選択できます。 このトグルがオフに切り替えられている場合、ファームの仮想マシンはデフォルトでポッドのプライマリ仮想マシン サブネットに接続されます。

オプション	説明
モデルのフィルタリング	1 つ以上のフィルタを設定して、[モデル] ドロップダウン メニューで使用できるモデルを制御します。モデルは、タイプ、シリーズ、CPU の数、メモリ、およびタグでフィルタできます。モデルの選択の詳細については、Horizon Universal Console でのファームと割り当ての仮想マシン タイプとサイズの管理を参照してください。ここでは、[仮想マシンのタイプとサイズ] ページ（[設定] - [仮想マシンのタイプとサイズ]）のオプションについて説明しています。 **注：** Windows 11 Enterprise オペレーティング システム ファームの場合は、[Gen1] または [Gen1、Gen2] モデルを選択してください。 フィルタを設定するには、まずドロップダウン メニューで条件を選択し、次に目的の値を入力します。デフォルトでは、条件が「タグ」、値が「VMware 推奨」の単一のフィルタがあります。この最初のフィルタを編集し、And および Or 演算子によって接続されたフィルタをさらに追加できます。 次に、フィルタに使用できる基準と、それぞれに入力できる値の説明を示します。 ■ タイプ このオプションを選択すると、2 番目のドロップダウン メニューには使用可能な値が 1 つのみ表示されます。 ■ GPU と高パフォーマンス - GPU を使用するモデル。 **注：** GPU モデルを選択した場合、表示されるイメージのリストには「GPU を含める」フラグを選択して作成されたイメージのみが含まれるため、GPU モデルを使用してファームまたはプールを作成するにはそのようなイメージが少なくとも 1 つ必要です。GPU 以外のモデルを選択した場合、表示されるイメージのリストには、「GPU を含める」フラグなしで作成されたイメージのみが含まれます。 ■ シリーズ このオプションを選択すると、2 番目のドロップダウン メニューから一連のモデルを選択できます。リストの一番上にある [フィルタ] テキスト ボックスにテキストを入力してこのリストをフィルタリングすることもできます。 ■ CPU の数 このオプションを選択すると、CPU 範囲を入力できます。 **重要：** 本番環境では、予期しないエンドユーザー接続の問題を回避するために、2 個以上の CPU を持つ仮想マシン モデルを使用します。 ■ メモリ このオプションを選択すると、メモリ範囲 (GB 単位) を入力できます。 ■ タグ このオプションを選択すると、2 番目のドロップダウン メニューからタグを選択できます。リストの一番上にある [フィルタ] テキスト ボックスにテキストを入力してこのリストをフィルタリングすることもできます。ドロップダウン メニューで使用可能なタグは、ハードコードされたシステム タグと、[仮想マシンのタイプとサイズ] ページ（[設定] - [仮想マシンのタイプとサイズ]）で作成したカスタム タグの両方です。 フィルタごとに次の手順を実行して、追加フィルタを設定できます。 a [追加] リンクをクリックします。 b 前のフィルタと作成中の新しいフィルタの間の演算子として And または Or を選択します。

オプション	説明
	c　新しいフィルタを設定するには、条件を選択して値を入力します。 **注：** ファームを作成するために選択したモデルが今後使用できなくなった場合、ファームを拡張することはできません。この制限を除けば、ファームは完全に機能します。仮想マシン タイプが使用可能かどうかを確認するには、[仮想マシンのタイプとサイズ] ページ（[設定] - [仮想マシンのタイプとサイズ]）に移動します。
モデル	ここで選択した項目は、[フィルタ モデル] で選択した条件に基づいてフィルタリングされます。ファームのマルチセッション仮想マシンに使用する仮想マシン モデルを選択します。この選択は、ファームの仮想マシンが作成されるときに使用される基盤となるリソースのセットをキャパシティ（コンピューティング、ストレージなど）の観点から定義します。使用可能な選択肢は、Microsoft Azure で使用可能な標準の仮想マシン サイズにマッピングされます。 **注：** Windows 11 Enterprise オペレーティング システム ファームの場合は、[Gen1] または [Gen1、Gen2] モデルを選択してください。 **重要：** 本番環境の場合は、2 個以上の CPU が搭載された仮想マシン モデルを選択します。第 1 世代の Horizon Cloud スケール テストでは、2 個以上の CPU を使用すると、予期しないエンド ユーザー接続の問題を回避す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、このようなモデルはテスト用または事前検証用にのみ使用する必要があります。
ディスク タイプ	利用可能なオプションからサポートされているディスク タイプを選択します。ディスク タイプのオプションは、選択したモデル、および Azure サブスクリプションとリージョンに基づいています。一般的に使用可能なディスク タイプは次のとおりです。 ■ 標準 HDD - デフォルトのディスク タイプ。 ■ 標準 SSD ■ プレミアム SSD - このオプションは、プレミアム I/O をサポートするモデルを選択した場合にのみ表示されます。 必要に応じて、後で選択内容を編集できます。
ディスク サイズ	ファームの仮想マシンの OS ディスク サイズを GiB 単位で入力します。 ■ デフォルト値は、基本イメージの OS ディスク サイズ（通常は 127 GiB）です。 ■ サイズを編集する場合、入力する値は基本イメージの OS ディスク サイズよりも大きくなければなりません。また、選択したモデルでサポートされる最大サイズ（通常は 1024 GiB）を超えることはできません。 ■ この値は、必要に応じて後で編集することもできます。 **重要：** ディスク サイズを編集する場合は、仮想マシンが予期したとおりに作成されるように、追加のアクションを実行する必要があります。詳細については、ファームまたは VDI デスクトップ割り当てのディスク サイズが増加した場合に必要な管理者のアクションを参照してください。

オプション	説明
イメージ	複数セッション イメージを選択します。 **重要：** ■ イメージのオペレーティング システムにユニバーサル Windows プラットフォーム (UWP) アプリケーションが含まれている場合は、エンド ユーザーがファームの仮想マシンからこれらの UWP アプリケーションを確実に使用できるようにするために、追加の操作を実行する必要があります。詳細については、Horizon Cloud での Microsoft Windows 10 または 11 Enterprise マルチセッション RDSH 仮想マシンからのユニバーサル Windows プラットフォーム (UWP) アプリケーションの実行を許可するために Horizon Agent ポリシーを有効化するを参照してください。 ■ [NSX Cloud 管理] を [はい] に設定する場合は、ここで選択したイメージに NSX Agent がインストールされていることを確認します。ファームの仮想マシンで NSX Cloud 管理機能を使用するには、このファーム用に選択したイメージに NSX Agent がインストールされている必要があります。システムは、ファームを作成するときに、選択したイメージに NSX Agent があるかどうかを検証しません。
優先プロトコル	エンド ユーザー セッションで使用するデフォルトの表示プロトコルを選択します。 デフォルトのプロトコルではなく、別のプロトコルが使用される状況が発生する場合があります。たとえば、クライアント デバイスがデフォルトのプロトコルをサポートしない場合や、エンド ユーザーが、選択されているデフォルト プロトコルよりも他のプロトコルを優先して使用する場合があります。
優先クライアント タイプ	エンド ユーザーが Workspace ONE Access からセッションベースのデスクトップを起動するときに使用する優先クライアント タイプを選択します。これは Horizon Client、または HTML Access 用のブラウザのいずれかになります。
ドメイン	お使いの環境に登録されている Active Directory ドメインを選択します。
ドメインへの参加	[はい] を選択し、ファームの仮想マシンが作成後に自動的にドメインに参加されるようにします。
ディスクの暗号化	ファームの仮想マシンで暗号化されたディスクを使用するように [はい] を選択します。 **重要：** ディスクを暗号化する場合は、ファームを作成するときにこれを選択する必要があります。ファームを作成した後はディスク暗号化を追加できません。
NSX Cloud 管理	ファームの仮想マシンで NSX Cloud の機能を使用できるように、[はい] を選択します。Microsoft Azure のファームでの NSX Cloud 機能の使用については、Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッドおよびそのサブトピックを参照してください。 **重要：** ■ ファームの仮想マシンで NSX Cloud を使用する場合は、ファームの作成時にこの選択を行う必要があります。NSX Cloud 管理は、ファーム作成後に有効にすることはできません。 ■ 仮想マシンで NSX Cloud 管理機能を使用するには、このファーム用に選択したイメージに NSX Agent がインストールされている必要があります。この設定を [はい] に切り替えるときは、[イメージ] で選択したイメージに NSX Agent がインストールされている必要があります。システムは、ファームを作成するときに、選択したイメージに NSX Agent があるかどうかを検証しません。

オプション	説明
仮想マシンの最小数 **仮想マシンの最大数**	このファームに含めるマルチセッション仮想マシンの最小数と最大数を指定します。ファームが最初に作成されると、システムは [仮想マシンの最大数] フィールドで指定された数の仮想マシンを展開し、次に [仮想マシンの最小数] で指定された数以外の仮想マシンをパワーオフします。 仮想マシンの最小数のみが最初にパワーオンされます。エンド ユーザーの要求が増加すると、システムは [仮想マシンの最大数] の設定を上限として追加の仮想マシンをパワーオンします。その後、エンド ユーザーの要求が減少すると、システムは [仮想マシンの最小数] の設定を下限として仮想マシンをパワーオフします。システムによって仮想マシンがパワーオフされる前に、サーバからユーザー セッションが完全になくなっている必要があります。 [仮想マシンの最小数] にゼロ (0) を指定すると、ファームに対するエンド ユーザーからのセッションの要求がなくなった時点で、システムはファームのすべての仮想マシンをパワーオフすることになります。[仮想マシンの最小数] にゼロ (0) を入力する場合は、[パワーオフ保護時間] フィールドを使用し、残りのパワーオン状態の仮想マシンにユーザー セッションがないと判断した後に、仮想マシンをパワーオフするまでシステムを待機させる時間を指定します。
パワーオフ保護時間	システムが自動的にパワーオンしているファームの仮想マシンをパワーオフするまでの待機時間（分）を指定します。1 から 60 の値を入力できます。デフォルトは 30 分です。 この保護時間は主として、システムがファームの仮想マシンを通常どおりパワーオフする状況で使用されます。この [パワーオフ保護時間] 設定を使用すると、仮想マシンのパワーオフを開始するまでに、システムを指定された時間待機させることができます。デフォルトの待機時間は 30 分です。
仮想マシン 1 台あたりのセッション数	このファームで許可される仮想マシンあたりの同時実行エンド ユーザー セッションの数を指定します。 Microsoft Azure のポッドの場合、ポッドあたりの同時接続セッションの最大数は、「第 1 世代テナント - サービス制限」ページに記載されています。 **注：** GPU 対応イメージが NVIDIA GRID テクノロジーと Microsoft Windows Server 2012 R2 を搭載した Azure 仮想マシン シリーズに基づいている場合、NVIDIA ドライバの制限により、マルチセッション仮想マシンでそのイメージを使用するファームは、仮想マシンごとに最大 20 セッションに制限されます。この特定の組み合わせ（GPU N シリーズ モデル、NVIDA ドライバ、および Microsoft Windows Server 2012 R2 に基づくイメージ）がある場合は、ここでは 20 を超える値を指定しないでください。
Windows ライセンスの質問	このウィザードでは、イメージ内にあり、ファームの仮想マシンに入ることになる Microsoft Windows オペレーティング システムを使用するための適格なライセンスがあることを確認するよう求められます。画面に表示される指示に従います。

オプションで、詳細プロパティを構成します。

オプション	説明
コンピュータの OU	ファーム仮想マシンが配置される Active Directory 組織単位。識別名（たとえば、`OU=RootOrgName,DC=DomainComponent,DC=eng` など）を使用して Active Directory 組織単位を入力します。OU およびネストされた OU 内の各パスには、文字、数字、特殊文字、および空白の任意の組み合わせを含めることができ、最大で 64 文字にすることができます。 ネストされた組織単位を使用する必要がある場合は、ネストされた Active Directory ドメイン組織単位の使用についての考慮事項を参照してください。 **注：** [コンピュータの OU] が `CN=Computers` に設定されている場合、システムは、仮想マシンのデフォルトの Active Directory `Computers` コンテナを使用します。Active Directory には、組織単位クラスのコンテナにリダイレクトされるデフォルトのコンテナがあります。
1 回実行スクリプト	（オプション）仮想マシン作成プロセス後にファーム仮想マシンで実行するスクリプトの場所。 **注：** 仮想マシンを再起動するため、スクリプトは仮想マシンを再起動する手順で終了する必要があります。再起動のための Windows コマンド ラインを以下に示します。 `shutdown /r /t 0` Microsoft Windows システムの準備 (Sysprep) プロセス後に、スクリプトが実行されます。システムがファーム仮想マシンを作成すると、仮想マシンが起動し、Windows オペレーティング システムで Sysprep プロセスを完了します。Sysprep プロセスが完了すると、仮想マシン内のエージェントはドメイン参加を実行します。同時に、エージェントはここで指定するスクリプト パスを取得します。エージェントは `Windows RunOnce` パス (`System run once`) を設定し、仮想マシンを再起動します。次の再起動時に、システムはローカル管理者アカウントを使用して Windows オペレーティング システムにログインし、スクリプトを実行します。
Azure リソース タグ	（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。 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、[追加] 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。 ■ 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。 < > % & \ ? / ■ タグの名前には、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。 ファームが作成されると、Azure リソース タグを追加したり、そのファームのタグを編集または削除することができます。

4 ウィザードの次の手順で、フィールドに情報を入力し、該当する項目を選択して、[次へ] をクリックします。

オプション	説明
ローリング メンテナンス	メンテナンスのタイプを選択します。タイム ケーデンスに基づくメンテナンス（[スケジュール]）またはこのファームの仮想マシンに対するユーザー セッションに基づくメンテナンス（[セッション]）があります。 [スケジュール] が選択されている場合は、日または週単位でのメンテナンス ケーデンスを構成します。日単位の繰り返しを選択する場合は、メンテナンスが開始する時刻を指定します。週単位の繰り返しを選択する場合は、曜日と時刻の両方を指定します。 [セッション] が選択されている場合は、ファームがローリング メンテナンスを開始するセッション数を指定します。 **注：** 15 分以内にログオフされたセッションは、ローリング メンテナンスの計算の対象になりません。これは実行時間の短いセッションの数に基づいて仮想マシンの再起動または再構築が行われるのを防ぐためです。 [同時に静止する仮想マシン数] フィールドで、同時に静止状態にすることができるファーム仮想マシンの数を指定します。仮想マシンが静止状態になると、仮想マシンではその仮想マシンにすでに接続されているユーザー セッションについては処理を継続しますが、新しいユーザー接続を受け入れません。 簡単な例については、ファームのローリング メンテナンスの例を参照してください。
仮想マシンのアクション	メンテナンス中の仮想マシンに対してシステムが実行するアクションを選択します。 ■ [再起動] を選択すると、仮想マシンが再起動されます。 ■ [再起動] により、仮想マシンはまず削除されてから、ファームの関連付けられたイメージに基づいて再プロビジョニングされます。 未使用の仮想マシンをパワーオフするように選択した場合でも、クラウド環境ではある程度の量のストレージが使用されます。

オプション	説明
電源管理	これらの電源管理設定は、セッションによる仮想マシンの使用率に応じてシステムがファーム内のパワーオンされたファーム仮想マシンの数を自動的に増やしたり減らしたりする際のしきい値に関連します。使用率が増えて上限を超えると、システムは自動的に未使用の仮想マシンを 1 台起動します。使用率が減って下限を下回ると、システムは仮想マシンを使用されなくなるまでドレインします。続いて、システムは仮想マシンをシャットダウンし、その割り当てを解除します。 電源管理の選択は、キャパシティのコストと迅速な可用性のバランスを取ります。 ■ 後からではなく、すぐに次の仮想マシンをパワーオンする場合は、[最適化されたパフォーマンス] を選択します。ユーザーが要求するよりも早く次の仮想マシンを準備することで電源の消費は増えますが、ユーザーがログインしたときにはすでに仮想マシンは起動しているので、そのようなユーザーの要求を満たすのに有効です。 ■ 次の仮想マシンをパワーオンするまで最大可能な時間待機するように設定する場合は、[最適化された電源] を選択します。仮想マシンの占有率は、システムが次の仮想マシンを起動する前に高くなります。既存の仮想マシンの使用率を高めることでキャパシティのコストは最小限に抑えられますが、この設定では新規ユーザーがログインするときに遅延が発生する可能性が高くなります。これは、システムが仮想マシンをパワーオンするまで待機が必要な場合があるためです。 ■ キャパシティのコストとユーザーに対する可用性までの時間のバランスを取るには [バランシング済み] を選択します。 各選択のしきい値の上限と下限は次のとおりです。 ■ [最適化されたパフォーマンス] ■ 低いしきい値：23% ■ 高いしきい値：50% ■ [最適化された電源] ■ 低いしきい値：38% ■ 高いしきい値：80% ■ [バランシング済み] ■ 低いしきい値：31% ■ 高いしきい値：66% 詳細については、「Horizon Cloud のファームの電源管理とロード バランシングについて」を参照してください。

オプション	説明
タイムアウト処理	システムで特定の種類のユーザー セッションを処理する方法を設定します。 **注：** これらの設定によって管理されるユーザー セッションは、RDS セッション デスクトップまたはアプリケーションの Windows オペレーティング システム セッションへのユーザー ログインです。これらのセッションは、Horizon Client、Horizon HTML Access、または Workspace ONE のユーザー ログインではありません。 ユーザーのセッションは、このファームのマルチセッション仮想マシンから提供されるセッションベースのデスクトップまたはリモート アプリケーションの基盤となる Windows オペレーティング システムに対してユーザーが認証されると開始します。 ■ [空のセッション タイムアウト] - アプリケーション ファームに対して、アイドル状態のユーザー セッションをシステムがどのように処理するか、すなわちアイドル状態のセッションをタイムアウトしないか、指定した時間（分）が経過した後でタイムアウトするかを選択します。アイドル タイムアウトは、セッションベースのデスクトップやアプリケーションではなく、エンドポイント デバイスでのアクティビティに基づきます。アイドル状態のセッションをタイムアウトするように指定した場合は、タイムアウト時間が経過したときの処理、すなわちセッションを切断するか、ユーザーをログオフするかを選択します。セッションの切断を選択した場合、セッションはネットワークから切断され、メモリに保存されます。セッションのログオフを選択した場合、セッションはメモリに保持されず、未保存のドキュメントは失われます。 ■ [切断済みセッションのログオフ] - 切断されたセッションからシステムがいつユーザーをログオフするかを選択します。 ■ [セッションの最大有効期間] - システムが単一のユーザー セッションに対して許可する最大分数を指定します。

オプション	説明
セッション タイムアウトの間隔	この間隔は、システムがこのファームによって提供されるセッションベースのデスクトップまたはアプリケーションから強制的にログオフする前に、エンド ユーザーのセッションがアイドル状態を保持する時間です。このタイムアウトは、基盤となる Windows オペレーティング システムへのログイン セッションに適用されます。ここで指定する時間は、エンド ユーザーの Horizon Client または HTML Access ログイン セッションを制御するタイムアウト設定とは別のものです。 **注意：** 基盤となる Windows オペレーティング システムのセッションでシステムが強制的にログオフすると、保存されていないデータは失われます。データが意図せずに失われるのを防ぐには、エンド ユーザーのビジネス ニーズに応じてこの間隔の値を十分に大きくします。 デフォルトの間隔は 1 日（1440 分）です。 **注：** タイムアウトの間隔に達する前にユーザー アクティビティが発生しない場合、30 秒以内に [OK] をクリックしないとログオフされることを示すメッセージがユーザーに表示されます。ログアウトが発生すると、ドキュメントやファイルなど、保存されていないユーザー データは失われます。
電源管理をスケジュール	Microsoft Azure でファームの仮想マシンの省電力とパフォーマンスを最適化するために、週単位で繰り返し、このファーム内のパワーオン状態の仮想マシンの最小数を調整するスケジュールを任意に構成することができます。次に例を示します。 ■ エンド ユーザーがデスクトップまたはリモート アプリケーションを使用していない週末や夜間の時間帯に対しては、パワーオン状態の仮想マシンの数がゼロまたは少なくなるようスケジュール設定することができます。 ■ エンド ユーザーの需要が増大することが予測できる特定の日数や特定の時間幅に対しては、その需要を満たすには利用可能になるパワーオン状態の仮想マシンの最小数が増加するスケジュールを設定できます。 ファームに対して最大 10 個のスケジュールを指定できます。期間が重複しているのに、仮想マシンの最小数の指定値が異なっているスケジュールがある場合は、システムはその重複する期間において大きい値の方の仮想マシンの最小数を使用します。 a [+] アイコンをクリックして [電源管理をスケジュール] セクションで最初の行を追加します。 b 1 番目のスケジュールの識別名を入力します。 c 1 番目のスケジュールの日数を選択します。 **注：** 行が追加されると、1 日がデフォルトで選択されます。選択した日をこのスケジュールに含めないようにするには、ドロップダウンをクリックしてその選択された日の選択を解除します。 d 指定された日数の該当する時間を指定します。次のいずれかを行います。 ■ 指定した日数のすべての時間帯でこのスケジュールを有効にするには、[全日] チェック ボックスを選択します。 ■ それぞれの日に期間の開始時間と終了時間を指定します。 **注：** 暗号化された仮想マシンは、暗号化されていない仮想マシンよりもパワーオンに時間がかかります。[ディスクの暗号化] を [はい] に設定し、暗号化された仮想マシンのエンド ユーザー接続が、一日のうちの特定の時間帯に 100% 利用できるように設定したい場合、起動時間をその時間よりも早く設定する必要があります。暗号化された仮想マシンが多数ある場合のファームと VDI デスクトップの割り当ての電源管理のスケジューリングを参照してください。

オプション	説明
	e タイムゾーンを選択します。エンド ユーザーの場所に最も近いタイムゾーンが推奨されます。選択されたタイムゾーンに適した夏時間が自動的に適用されます。 **注：** 2 つのスケジュールで同じタイム ゾーン設定が使用されていて、時間の重複がある場合、警告が表示されます。ただし、2 つのスケジュールのタイム ゾーン設定が異なっていて、重複がある場合は、この警告は表示されません。例として、全日土曜日のスケジュールが 2 つ設定されていて、1 つが [ヨーロッパ/ロンドン] タイム ゾーンを選択していてもう 1 つが [アメリカ/トロント] を選択している場合、重複についての警告は表示されません。 f [仮想マシンの最小数] フィールドに、指定した期間内にパワーオンする仮想マシンの最小数を入力します。指定された期間内に、入力した最小数の仮想マシンがパワーオンされ、その期間内でのエンド ユーザーの要求に対応するために使用できます。この数の範囲は 0 からファームの [仮想マシンの最大数] に指定された数の間になります。この数値がゼロ (0) で、スケジュールの開始時点でアクティブなエンド ユーザー セッションがない場合は、ファームの仮想マシンがパワーオフされます。このシナリオでは、その後エンド ユーザーがスケジュールされた期間内にこのファームによって提供されるデスクトップまたはアプリケーションに接続しようとすると、デスクトップまたはアプリケーションが使用可能な状態になるまで遅延が発生します。これは、基板となる仮想マシンをパワーオンする必要があるためです。

5 ウィザードの [ロード バランシング] の手順で、[ログインのしきい値] に値を入力します。この設定は、指定した期間内に許可されるログイン数を制御します。この値を超えると、仮想マシンの新しいセッションの割り当て先としての優先度が下がります。たとえば、[ログインのしきい値] に 30 秒ごとのログイン回数が 3 に設定されている場合、過去 30 秒以内に仮想マシン 1 にログインしたセッション数が 3 であれば、次のセッションは仮想マシン 2 に割り当てられる、という具合です。

注： 古い環境を使用している場合、またはファームのエージェントが最新バージョンではない場合、[ロード バランシング] の設定が表示されない、または無効になる可能性があります。

6 [セッション ホストのロード バランシングの設定] のフィールドに入力します。

- Horizon Cloud Agent は、最初の 5 つの設定（[CPU 使用率のしきい値]、[メモリ使用率のしきい値]、[ディスク キュー長のしきい値]、[ディスクの読み取り遅延のしきい値]、[ディスクの書き込み遅延のしきい値]）を使用して、仮想マシンの負荷を測定するエージェント ロード インデックス（0 ～ 100 の値）を計算します。
- 最後の設定の [ロード インデックスのしきい値] は、仮想マシンが満杯であると見なされるエージェント ロード インデックスの値です。

重要： エージェント ロード インデックスは電源管理では重要な役割を果たすため、環境内で消費電力とパフォーマンスの必要なバランスを取ることができるように、これらの設定に適切な値を選択することが重要です。

エージェント ロード インデックスが電源管理に与える影響の詳細については、Horizon Cloud のファームの電源管理とロード バランシングについてを参照してください。

オプション	説明
CPU 使用率のしきい値	CPU 使用率のしきい値 (%)。0 ～ 100 の値を設定できます。推奨値は 90 で、これはデフォルト値でもあります。
メモリ使用率のしきい値	メモリ使用率のしきい値 (%)。0 ～ 100 の値を設定できます。推奨値は 90 で、これはデフォルト値でもあります。
ディスク キュー長のしきい値	サンプリング時間中、選択されたディスクのキューに入った読み取り要求と書き込み要求の両方の平均数のしきい値。任意の正の整数を設定できます。デフォルトでは、この設定はロード バランシングで考慮されません。デフォルト値は 0 です。
ディスクの読み取り遅延のしきい値	ディスクからのデータ読み取りの平均時間のしきい値 (ミリ秒)。任意の正の整数を設定できます。デフォルトでは、この設定はロード バランシングで考慮されません。デフォルト値は 0 です。
ディスクの書き込み遅延のしきい値	ディスクへのデータ書き込みの平均時間のしきい値（ミリ秒）。任意の正の整数を設定できます。デフォルトでは、この設定はロード バランシングで考慮されません。デフォルト値は 0 です。
ロード インデックスのしきい値	仮想マシンが満杯であると見なされ、新しいセッションが割り当てられなくなるエージェント ロード インデックスの値。値は 0 ～ 100 の範囲で入力できます。デフォルト値は 90 です。 **注：** 電源管理の高しきい値よりも大きい値にする必要がある場合、システムはこの値を修正します。これで効果的な電源管理が確保されます。

7 [次へ] をクリックします。

8 ウィザードの [サマリ] の手順で、設定を確認し、[送信] をクリックしてファームの作成を開始します。

結果

システムは、ファームの作成を開始します。[アクティビティ] ページを使用して進行状況を監視できます。[ファーム] ページでファームのステータスに緑色のドットが表示されている場合は、ファームを使用する準備ができています。

注： 暗号化されたファーム仮想マシンの作成は、暗号化されていない仮想マシンの作成の約 2 倍の時間がかかります。その結果、ディスクの暗号化が有効になっているファームを作成する場合は、無効になっている場合と比べて、開始から完了までの時間が約 2 倍かかります。

また、イメージ仮想マシンにデータ ディスクがある場合は、そのイメージ仮想マシンに基づいて、暗号化されたファーム仮想マシンを作成するための追加の時間が必要になります。より大きい、テラバイト単位のサイズのデータ ディスクでは、極めて長い時間がかかります。

次のステップ

デスクトップ ファームを作成した場合は、Horizon Cloud ポッド - RDS ベースのセッション デスクトップ割り当てを作成して、エンド ユーザーのために RDS ホストからのデスクトップ セッションを提供するの手順に従ってエンド ユーザーのセッションベースのデスクトップ割り当てを作成します。

注： エンド ユーザーが Microsoft Windows 10 または 11 マルチセッション オペレーティング システムで App Volumes アプリケーションを使用できるようにデスクトップ ファームを作成した場合は、続いて次のワークフローを実行する必要があります。

1. Horizon Cloud：既存のアプリケーション パッケージをインポートして App Volumes アプリケーションを追加、App Volumes アプリケーションがアプリケーション インベントリに追加されているようにします。または、インポート ワークフローの代わりに、Windows 10 または 11 クライアント オペレーティング システムに基づいた別のイメージを使用し、作成ワークフローを使用して、App Volumes アプリケーションを Horizon Cloud テナントのインベントリに追加するを使用して、その Windows 10 または 11 クライアント システムからインベントリにアプリケーションをキャプチャできます。これらのアプリケーションの使用資格をユーザーに割り当てることができます。それらのアプリケーションは、クライアント タイプの Windows 10 または 11 オペレーティング システムからキャプチャされた場合でも、このファームに基づくセッションベースのデスクトップで使用できます。
2. Horizon Cloud：App Volumes 割り当ての作成、当該アプリケーションの使用資格をユーザーに付与します。
3. Horizon Cloud ポッド - RDS ベースのセッション デスクトップ割り当てを作成して、エンド ユーザーのために RDS ホストからのデスクトップ セッションを提供する、このファームに基づき、セッションベースのデスクトップの使用資格をユーザーに付与します。

アプリケーション ファームを作成した場合は、そのファームをスキャンしてアプリケーションを Horizon Cloud にロードし、エンド ユーザーがそのファームからリモート アプリケーションを使用できるようにアプリケーション割り当てを作成します。

詳細については、Horizon Cloud インベントリ内のアプリケーション、リモート アプリケーション - Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた RDSH ファームからのインポート、およびリモート アプリケーション - Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされたリモート アプリケーションのリモート アプリケーション割り当ての作成を参照してください。

特別なポートを開く必要があるアプリケーションがこのファームのイメージにある場合、このファームに関連付けられたネットワーク セキュリティ グループ (NSG) を Microsoft Azure で変更する必要があります。NSG の詳細については、Horizon Cloud ポッド内のネットワーク セキュリティ グループとファームについてを参照してください。

このファームに NSX Cloud 管理を指定した場合は、NSX Cloud 環境の Service Manager (CSM) を使用して、NSX Cloud でファームの仮想マシンが管理されていることを確認できます。ユーザー環境の CSM にログインし、[クラウド] - [Azure] - [インスタンス] の順に移動します。その [インスタンス] ページに、ファームの仮想マシンの管理対象のステータスが表示されたら、それらに NSX ポリシーの実装を開始できます。

Horizon Cloud での Microsoft Windows 10 または 11 Enterprise マルチセッション RDSH 仮想マシンからのユニバーサル Windows プラットフォーム (UWP) アプリケーションの実行を許可するために Horizon Agent ポリシーを有効化する

Microsoft Windows 10 または Windows 11 Enterprise マルチセッション オペレーティング システムの仮想マシンに基づいてファームを作成するときに、エンド ユーザーがオペレーティング システムによって提供されるユニバーサル Windows プラットフォーム (UWP) アプリケーションを使用できるようにするには、デフォルトで無効になっている特定の Horizon Agent ポリシーを有効にする必要があります。Horizon Agent のデフォルトのポリシー設定では、UWP アプリケーションの起動は許可されていません。そのため、エンド ユーザーがこれらの UWP アプリケーションを使用できるように、`Enable UWP support on RDSH platforms` という名前の Horizon Agent に関連したグループ ポリシー設定を有効にする手順を実行する必要があります。

必要な設定とその設定を含む Horizon ADMX テンプレートの説明については、VMware Horizon のドキュメントにある『Horizon リモート デスクトップの機能と GPO』ガイドで `Enable UWP support on RDSH platforms` を検索してください。

ファーム仮想マシン内の対応する Horizon Agent ポリシーは、デフォルトで無効になっています。したがって、エンド ユーザーがこれらのファーム仮想マシンからプロビジョニングされた UWP アプリケーション（セッションベースのデスクトップまたはリモート アプリケーション）を使用できるようにするには、このオプションを有効にする必要があります。

エージェント ポリシーが有効になっていない限り、UWP アプリケーションのステータスは、RDSH 仮想マシンにインストールされている Horizon Agent に対して `Unavailable` と表示され、その結果としてエンド ユーザーはその UWP アプリケーションにアクセスできません。

重要： ポリシーを有効にした後、ファームの既存の RDSH 仮想マシンに GPO 設定を強制する必要があります。また、それらの RDSH 仮想マシンで VMware Horizon View Agent サービス (`wsnm.exe`) を再起動するか、RDSH 仮想マシンを再起動して GPO を有効にする必要があります。

Horizon Agent 構成の ADMX テンプレート ファイル（名前付き `vdm_agent.admx`）では、[Unity Touch and Hosted Apps] フォルダ ([VMware View Agent 構成] - [Unity Touch およびホストされるアプリケーション]) にこのポリシー設定が含まれています。ファームの RDSH 仮想マシンに必要なポリシー設定を構成する 1 つの方法は、Active Directory サーバでその ADMX テンプレート ファイルを使用して、[Unity Touch およびホストされるアプリケーション] フォルダを Active Directory サーバのグループ ポリシー管理エディタに追加することです。フォルダが提示されている場合、以下のサンプルの手順に従い、ファームのターゲット OU 上の Active Directory システムで GPO を使用して、仮想マシンの UWP サポートを有効にできます。

前提条件

Active Directory サーバで、UWP グループ ポリシー設定を RDSH 仮想マシンに適用するために使用する名前付き GPO を作成します。通常、グループ ポリシー管理コンソール (GPMC) は [スタート] - [管理ツール] - [グループ ポリシー管理] によって起動されます。作成した GPO を、それらの RDSH 仮想マシンが存在する OU にリンクします。この OU は、これらの RDSH 仮想マシンをプロビジョニングするファームを作成するときに、[ファームの作成] ページで指定された OU です。[ファームの作成] ページで OU を指定しない場合、使用されるデフォルト OU は、Active Directory 登録ワークフローで、Horizon Cloud に Active Directory サーバを登録するときに指定する OU です。

注意: 最終的には、エンド ユーザーが UWP アプリケーションを起動できるようにするために、ファームの RDSH 仮想マシンで必要なエージェント ポリシーが確実に有効になっているようにすることが目標です。ここで示す手順は、RDSH 仮想マシンで必要なポリシーを有効にする方法の 1 つの例です。同じ結果となる別の方法を採用することも考えられます。どの方法を選択するかは任意です。

手順

1 VMware Horizon Service のダウンロード の VMware Customer Connect から `Horizon GPO` バンドル をダウンロードします。

その URL から、Horizon Cloud Service on Microsoft Azure ダウンロードの場所に移動します。このページには、ダウンロード可能な項目のリストが表示されます。`Horizon GPO` バンドルという名前のエントリを見つけて、その ZIP ファイルをダウンロードします。Horizon 関連コンポーネントのグループ ポリシー設定を提供するすべての ADMX ファイルは、このファイルにあります。

2 ZIP ファイルを解凍して、次のファイルを指定された場所にコピーします。

- `vdm_agent admx` ファイルを Active Directory サーバにコピーして、`%systemroot%\PolicyDefinitions` の場所に保存します。
- 必要なロケールの `vmd_agent.adml` 言語リソース ファイル（`en-US/vmd_agent.adml` など）を Active Directory サーバの `%systemroot%\PolicyDefinitions\<locale>` の場所にコピーします。*<locale>* はコピーする ADML ファイルのロケールに一致します。

3 Active Directory サーバで、[グループ ポリシー管理] を開き、UWP グループ ポリシー設定を適用するために作成した GPO の編集を選択します。

4 グループ ポリシー管理エディタで、[コンピュータの構成] - [ポリシー] - [管理テンプレート] - [VMware View Agent の構成] - [Unity Touch およびホストされるアプリケーション] を展開します。

5 その [Unity Touch およびホストされるアプリケーション] フォルダで、「RDSH プラットフォームでの UWP サポートの有効化」を見つけて編集し [有効] に設定します。

6 その GPO を、ファームの RDSH 仮想マシンが作成される OU とリンクします。

注意: ファームの仮想マシンが作成された OU に GPO をリンクすると、上記の手順を使用してその GPO に設定した UWP ポリシーが、その OU 内のすべての仮想マシンに適用されます。これは、GPO の標準の動作です。

7 GPO 設定をファームの RDSH 仮想マシンに強制します。

8 それらの RDSH 仮想マシンで VMware Horizon View Agent サービス (`wsnm.exe`) を再起動します。

Horizon Cloud でのファームの管理

管理コンソールの [ファーム] ページに表示されるファームで複数のアクションを実行できます。

[ファーム] ページで実行できるアクション

ページ レベルで、既存のファームの横にあるチェック ボックスをオンにし、いずれかのボタンをクリックしてファーム上で関連するアクションを実行できます。

[編集]

このボタンをクリックするとウィザードが起動し、ファームの電源管理設定、ファームに配置できる仮想マシンの最小数や最大数など、特定の設定を変更できます。ウィザードは、[新しいファーム] ウィザードと似ています。既存のファームでは変更できない設定の読み取り専用フィールドがあります。フィールドの詳細な説明については、ファームの作成を参照してください。

[編集] ボタンを使用する代わりに、ファームの名前をクリックしてファームの [サマリ] ページの設定を更新することもできます。

ファームを編集して [仮想マシン 1 台あたりのセッション数] の値を小さくすると、新しく指定された小さい値を超えるすべての既存セッションは自動的にログオフされません。手動で超過分のセッションをログオフするかファームの[タイムアウトを処理] の設定値（[空のセッション タイムアウト]、[切断済みセッションのログオフ]、[セッションの最大有効期間]）および [セッション タイムアウトの間隔] に従ってシステムがセッション ログオフするのを待つことができます。新しく指定された小さい値の超過分の既存セッションは自動でログオフされないため、超過分のアクティブなセッションがログオフするまで、仮想マシンとファームの使用率の値が 100% より高いものがコンソールに表示されます。

- [仮想マシン 1 台あたりのセッション数] の値を変更すると、更新された値に基づいてファームの新しい負荷に対応するために、システムはファームの仮想マシンをパワーオンまたはパワーオフします。
- ファームを作成するために選択したモデル仮想マシンが使用できなくなった場合、ファームを拡張することはできません。この制限を除き、ファームは完全に機能し続けます。仮想マシン タイプが使用可能かどうかを確認するには、[仮想マシンのタイプとサイズ] ページ（[設定] - [仮想マシンのタイプとサイズ]）に移動します。モデル仮想マシンの詳細については、Horizon Universal Console でのファームと割り当ての仮想マシン タイプとサイズの管理を参照してください。

[オフラインにする]

このボタンをクリックすると、メンテナンスのためにファームをオフラインにするウィンドウが開きます。

[オンラインにする]

このボタンをクリックすると、オフラインのファームをオンラインに戻すウィンドウが開きます。

[削除]

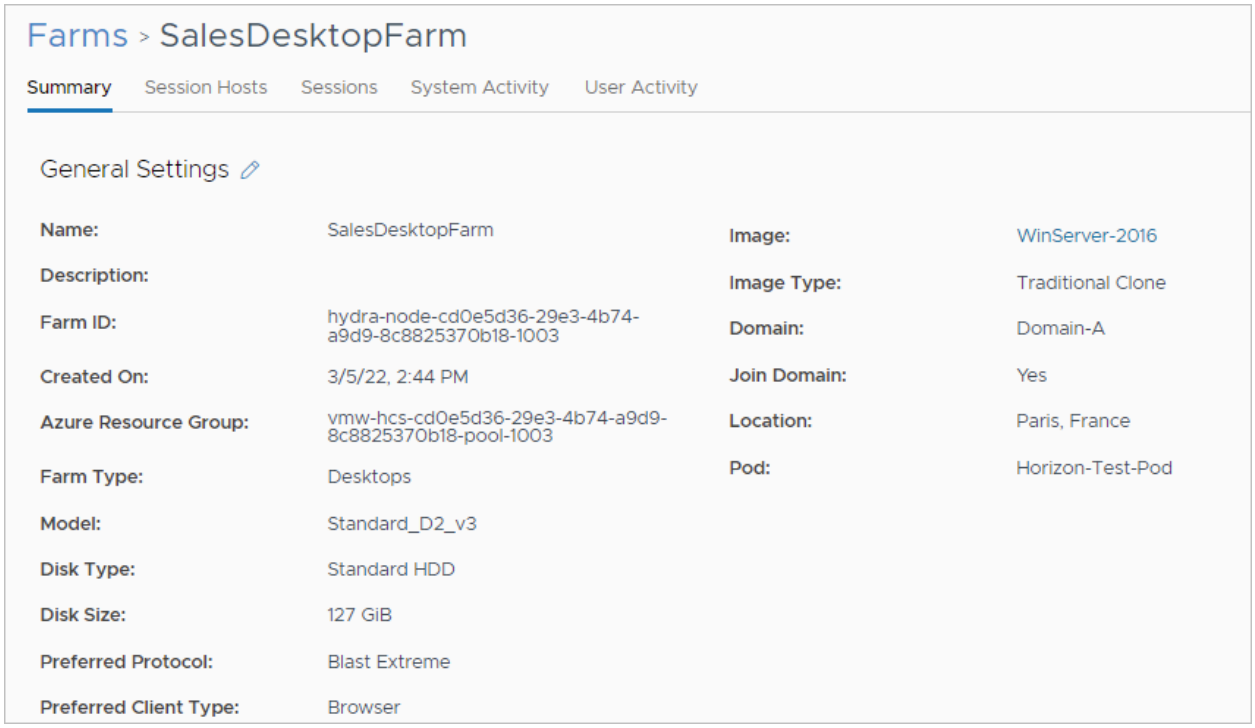
このボタンを使用して、選択したファームを削除します。ただし、このボタンを使用してファームを削除するには、そのファームを使用しているすべての割り当てを削除する必要があります。[割り当て] ページに移動し、[ファーム] 列で並べ替えることで、ファームを使用している割り当てを表示できます。

注： ファームを削除すると、ファームの基盤となる RDSH 仮想マシンがすべて削除されます。ファームが削除されると、そのファームのログに記録されたアクティビティのすべてが [アクティビティ] ページから削除されます。

ファームの詳細ページで実行できるアクション

[ファーム] ページでファームの名前をクリックして、その詳細ページを表示することができます。最初に、[サマリ] ページが表示されます。

次のスクリーンショットは、Microsoft Azure のポッドにあるファームの [サマリ] ページを示します。



[サマリ] ページ

[サマリ] ページにはファームの現在の設定が表示されます。ページのセクションごとに、鉛筆アイコンをクリックして、既存のファームに対してシステムで更新可能な設定を変更できます。ファームのポッドなど、一部の設定はファームの作成後に変更できません。

[セッション ホスト] ページ

[セッション ホスト] ページには、ファーム内の既存の RDSH インスタンスが表示されます。選択したインスタンスに対して実行できるアクションは、パワーオンまたはパワーオフ（仮想マシンの現在の状態によります）、削除、およびエージェント ペアリングのリセットです。

[セッション] ページ

[セッション] ページには、ファーム内の既存のユーザー セッションが表示されます。セッションを選択するときには、セッションを切断するか、セッションからユーザーをログオフすることができます。[切断] をクリックすると、ユーザーのセッションは強制的に切断されます。セッションが切断されたことを伝えるメッセージはユーザーに送信されません。[ログオフ] をクリックすると、セッションが終了する前にユーザーが文書を保存できる猶予期間を示すメッセージがユーザーに表示されます。

[システム アクティビティ] ページ

[システム アクティビティ] ページには、ファームの拡張など、システム アクションによって発生するファーム内のアクティビティが表示されます。[システム アクティビティ] ページでは、タスクをキャンセルしたり、レポートをエクスポートしたりできます。

割り当てに関連するタスクをキャンセルするには、そのタスクが完了する前に、リストでタスクを選択して [タスクをキャンセル] ボタンをクリックすることによってそのタスクをキャンセルできます。

- キャンセルするタスクの選択を行う前に、ビューを更新して表示されているタスクのステータスを最新の状態にします。
- タスクがシステムによってキャンセルできる状態になっている場合、そのキャンセル可能なタスクに対応しているチェック ボックスを選択できます。

次の表はキャンセルできるタスクを示しています。

タスク	タスクがキュー状態にあるときにキャンセル	タスクが実行状態にあるときにキャンセル
ファームの拡張	サポートされています **注：** システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。	サポートされています ■ システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。 ■ 仮想マシンや OS/データ ディスクなど、すでに作成されているリソースは、タスクがキャンセルされると破棄されます。仮想マシンが破棄された場合または作成されていない場合、割り当てのサイズは変わります。 ■ このオプションは、マルチクラウドの割り当てでは使用できません。
割り当ての拡張	サポートされています **注：** システムによって VDI デスクトップ割り当てに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、割り当てがオフラインになる必要があります。	サポートされています ■ システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。 ■ 仮想マシンや OS/データ ディスクなど、すでに作成されているリソースは、タスクがキャンセルされると破棄されます。仮想マシンが破棄された場合または作成されていない場合、割り当てのサイズは変わります。 ■ このオプションは、マルチクラウドの割り当てでは使用できません。
仮想マシンのイメージへの変換	サポートされています **注：** このタスクをキャンセルして再試行する場合は、まず仮想マシンが変換可能な状態であることを確認します。不明な場合は、仮想マシンをパワーオフしてからパワーオンします。	サポートされています **注：** このタスクをキャンセルして再試行する場合は、まず仮想マシンが変換可能な状態であることを確認します。不明な場合は、仮想マシンをパワーオフしてからパワーオンします。

[レポートのエクスポート] 機能で、表示されている情報をレポート ファイルとしてエクスポートできます。レポートをエクスポートすると、[レポート] ページの [エクスポートされたレポート] タブに表示されます。ここから、レポートをダウンロードできます。詳細については、第 1 世代テナント - 第 1 世代 Horizon Universal Console の [レポート] ページを参照してください。エクスポートを開始するときに、すべてのデータをエクスポートするか、現在フィルタされているデータのみをエクスポートするかを選択できます。次に、レポートが生

成中であることを示すメッセージがページの最上部に表示されます。[レポート] ページの [エクスポートされたレポート] タブで、レポートの進行状況を確認したり、エクスポートが完了したレポートをダウンロードできます。この準備はレコードの数に応じて数分間かかります。たとえば、50,000 レコードのレポートには、約 10 分かかります。

注目: Microsoft Azure のポッドのいずれかが 2552 より前のマニフェストにある場合、より大きなレポートの処理は次のようになります。

- エクスポートを開始すると、レポートがコンパイル中で、しばらく時間がかかることを知らせるメッセージが表示されます。この準備はレコードの数に応じて数分間かかります。たとえば、50,000 レコードのレポートには、約 10 分かかります。
- 準備が完了すると、「**レポートが正常に生成されました**」というメッセージおよび [ダウンロード] ボタンが表示された別のダイアログボックスが表示されます。[ダウンロード] ボタンをクリックした後、このダイアログボックスを閉じる前にダウンロードが完了するまで待機する必要があります。ダウンロードが完了する前に閉じると、ダウンロードがキャンセルされます。

このプロセスが完了するまでコンソールでその他のアクションを実行することはできないため、大量のアクティビティ レコードがある場合は、情報のエクスポートを、コンソールで他のタスクを実行するまでに最大 10 分ほど待つことができるときに計画する必要があります。

[ユーザー アクティビティ] ページ

[ユーザー アクティビティ] ページには、ファームによって提供されるセッションのログインやログオフなど、ユーザー アクションによって発生するファーム内のアクティビティが表示されます。

[レポートのエクスポート] 機能で、表示されている情報をレポート ファイルとしてエクスポートできます。

レポートをエクスポートすると、[レポート] ページの [エクスポートされたレポート] タブに表示されます。ここから、レポートをダウンロードできます。詳細については、第 1 世代テナント - 第 1 世代 Horizon Universal Console の [レポート] ページを参照してください。

エクスポートを開始するときに、すべてのデータをエクスポートするか、現在フィルタされているデータのみをエクスポートするかを選択できます。次に、レポートが生成中であることを示すメッセージがページの最上部に表示されます。[レポート] ページの [エクスポートされたレポート] タブで、レポートの進行状況を確認したり、エクスポートが完了したレポートをダウンロードできます。この準備はレコードの数に応じて数分間かかります。たとえば、50,000 レコードのレポートには、約 10 分かかります。

注目: Microsoft Azure のポッドのいずれかが 2552 より前のマニフェストにある場合、より大きなレポートの処理は次のようになります。

- エクスポートを開始すると、レポートがコンパイル中で、しばらく時間がかかることを知らせるメッセージが表示されます。この準備はレコードの数に応じて数分間かかります。たとえば、50,000 レコードのレポートには、約 10 分かかります。
- 準備が完了すると、「**レポートが正常に生成されました**」というメッセージおよび [ダウンロード] ボタンが表示された別のダイアログボックスが表示されます。[ダウンロード] ボタンをクリックした後、このダイアログボックスを閉じる前にダウンロードが完了するまで待機する必要があります。ダウンロードが完了する前に閉じると、ダウンロードがキャンセルされます。

このプロセスが完了するまでコンソールでその他のアクションを実行することはできないため、大量のアクティビティ レコードがある場合は、情報のエクスポートを、コンソールで他のタスクを実行するまでに最大 10 分ほど待つことができるときに計画する必要があります。

ファームの RDSH セッション ホストの管理

ファーム内の個々の RDSH セッション ホストに対して特定のアクションを実行できます。

手順

1 [インベントリ] - [ファーム] をクリックします。

[ファーム] ページが表示されます。

2 リストにあるファームの名前をクリックします。

ファームの詳細のページが表示されます。

3 ページ上部にある [セッション ホスト] をクリックします。

ファーム内の RDSH セッション ホスト仮想マシン (VM) のリストを示す [セッション ホスト] タブが表示されます。ページの右上にあるコントロールを使用して、リストをフィルタ、更新、およびエクスポートできます。

1 つまたは複数のセッション ホスト仮想マシンを選択し、ページ上部のいずれかのボタンをクリックして、次のアクションを実行できます。

注： 仮想マシンのステータスが緑色でなければ、これらの操作は実行できません。

オプション	説明
シャットダウン	選択した仮想マシンをシャットダウンします。 ■ 一度に複数の仮想マシンを選択できます。 ■ アクティブなユーザー セッションのない仮想マシンのみをシャットダウンできます。 **注：** Horizon Cloud ポッドで、1976.0 より前のマニフェスト バージョンが実行されている場合、コンソールには [パワーオフ] としてラベルが表示されます。
削除	選択した仮想マシンを削除します。仮想マシンが削除されたときにファームのサイズを減らすには、ダイアログ ボックスで [ファーム サイズを減らしますか] の下にある [はい] を選択します。
エージェント ペアリングをリセット	ペアリングのエラーが発生したときにエージェント ペアリングの状態を修正します。 ■ 複数の仮想マシンを選択できます。アクションは、現在パワーオン状態の選択した仮想マシンにのみ適用されます。 ■ 進行状況は、[監視] - [アクティビティ] ページ、またはファームの詳細ページの [システム アクティビティ] タブで確認できます。
ユーザー ログイン モード	メンテナンスのためにユーザー ログインを制御します。設定について以下に説明します。 **注：** この設定は、仮想マシンに最新のエージェントがある場合にのみ変更できます。 ■ [ログインを許可（アクティブ）] ■ 仮想マシンへの新しい接続を許可します。 ■ 仮想マシンへの再接続を許可します。 ■ 表示される [エージェントのステータス] が [有効] です。 ■ [新規ログインと再接続を禁止（無効）] ■ 仮想マシンに対して新しい接続要求を送信しません。 ■ ファームで利用可能な他の仮想マシンに新しい接続をルーティングします。 ■ 仮想マシンへの再接続を拒否します。 ■ 表示される [エージェントのステータス] が [無効] です。 **注：** このオプションを選択する前に、仮想マシンにログインするか、再接続する必要があります。 ■ [新規ログインのみを禁止（ドレイン）] ■ 仮想マシンに対して新しい接続要求を送信しません。 ■ ファームで利用可能な他の仮想マシンに新しい接続をルーティングします。 ■ 仮想マシンへの再接続を許可します。 ■ 表示される [エージェントのステータス] が [ドレイン中] です。 **注：** このオプションを選択する前に、仮想マシンに既存のセッションが必要です。 ■ [再起動するまで新規ログインを禁止（ドレイン）] ■ 仮想マシンが再起動されるまで、新しい接続要求を仮想マシンに送信しません。 ■ 仮想マシンが再起動されるまで、ファーム内の他の使用可能な仮想マシンに新しい接続をルーティングします。 ■ 仮想マシンへの再接続を許可します。 ■ 表示される [エージェントのステータス] が [再起動するまでドレイン] です。 ■ 仮想マシンの再起動後に [ログインを許可] の設定に戻します。 **注：** このオプションを選択する前に、仮想マシンに既存のセッションが必要です。

ファームのローリング メンテナンスの例

この例では、Horizon Cloud が新しいファームの RDSH 仮想マシン (VM) をどのようにプロビジョニングし、ローリング メンテナンス用に管理するのかについて説明します。

[新規] ファーム ウィザードでは、このファームの規模は次のように設定されます。

- [仮想マシンの最小数] = 1
- [仮想マシンの最大数] = 3
- [仮想マシン 1 台あたりのセッション数] = 20

作成ワークフローでは、

1 3 つのすべての RDSH 仮想マシンは、Microsoft Azure で完全に構成されています (パワーオンされドメインに参加している状態)。

2 稼動コストを節約するために、仮想マシン 2 と 3 がパワーオフされます。

仮想マシン 1 はパワーオンのままで、ユーザー セッションを提供できる状態です。

ユーザーがログインすると、仮想マシン 1 でセッションが与えられます。利用可能な仮想マシン（ここでは仮想マシン 1）の占有率が電源管理のしきい値に達すると、別の仮想マシン（仮想マシン 2）がパワーオンされます。2 台の仮想マシンがパワーオンされると、新しいユーザー セッションは負荷の少ない仮想マシンに配置され、パワーオンされた 2 台の仮想マシン間でセッションの負荷が分散されます。パワーオンされた両方の仮想マシンでユーザー セッションの合計数が 1 つ上の占有率しきい値に達すると、次の仮想マシン（仮想マシン 3）がパワーオンされます。

ユーザーのそのセッションから ログオフする場合、次のようになります。

1 占有率がしきい値の下限を下回ると、仮想マシンの 1 つが静止中としてマークされます。通常、システムは負荷が最小の仮想マシンを静止中としてマークします。

2 マークされると、仮想マシン上の既存のセッションはそのまま残りますが、その仮想マシンに対する新しいユーザー セッションは受け付けられません。この時点で、新しいセッションは実行中の仮想マシンにのみ配置されます。

3 マークされた仮想マシン上に既存のセッションを持つすべてのユーザーが自分のセッションからログオフすると、Horizon Cloud はその仮想マシンをパワーオフします。

上記の手順は、実行中の仮想マシンの数が [仮想マシンの最小数] の値に達するまで繰り返されます。

ローリング メンテナンス

仮想マシンのメンテナンスのベスト プラクティスは、仮想マシンを定期的に再起動し、キャッシュされたリソースや、仮想マシン内のサードパーティ アプリケーションからのメモリ リークを消去することです。Horizon Cloud のローリング メンテナンス機能は、ファーム全体で正常な健全性を自動的に復元します。通常のアクションは、仮想マシンの再起動です。Horizon Cloud は、仮想マシンを削除し、そのファームで使用されている最新の公開イメージに基づいて再プロビジョニングすることにより、ファームの仮想マシンを再構築する追加のオプションを提供します。再構築のオプションは、ファームのすべての仮想マシンに対してイメージの更新を自動的かつ定期的に適用する便利な方法です。再構築のオプションには、手動による操作を日常のメンテナンスの一部として行う必要がありません。

システムは、ファームの [同時に静止する仮想マシン数] の値に設定した数の仮想マシン数のみを一度に静止させます。ファームのローリング メンテナンス用に設定された [メンテナンスのタイプ] で設定されているように、システムは各仮想マシンに対して指定されたメンテナンス アクションを実行します。このアクションは、アクティブなユーザー セッションを持つ仮想マシンに対しても、[同時の静止サーバ] で設定した数を超える仮想マシンに対しても実行されません。

Horizon Cloud のファームの電源管理とロード バランシングについて

このトピックでは、Horizon Cloud の RDSH ファームで、ロード バランシングの設定に基づいて、エージェント ロード インデックスを電源管理に使用する方法について説明します。

このドキュメントの記事に記載されている設定の詳細については、第 1 世代 Horizon Cloud ポッド - ファームの作成と管理を参照し、その記事内で設定を検索してください。

Horizon Cloud Agent は、5 つの設定（[CPU 使用率のしきい値]、[メモリ使用率のしきい値]、[ディスク キュー長のしきい値]、[ディスクの読み取り遅延のしきい値]、[ディスクの書き込み遅延のしきい値]）を使用して、各仮想マシンの負荷を測定するエージェント ロード インデックス（0 ～ 100 の値）を計算します。

重要： エージェント ロード インデックスは電源管理では重要な役割を果たすため、環境内で消費電力とパフォーマンスの必要なバランスを取ることができるように、これらの設定に適切な値を選択することが重要です。

システムによるファームの使用量の決定

システムは、次の 2 つの割合値のうちの高い方を選択することによって、特定のファームの使用量を決定します。

セッション占有率

ファーム内のパワーオン状態の仮想マシンで可能なセッションの合計数で割ったファーム内のアクティブなセッションの数。可能なセッション数は、ファーム内のパワーオン状態の仮想マシンの数に、ファームに設定した [仮想マシン 1 台あたりのセッション数] の値を掛けて計算されます。

平均ロード インデックス

ファーム内のパワーオン状態の仮想マシンの平均エージェント ロード インデックス。

ファームを拡張する場合、システムは、選択した値をファームで選択した [電源管理] 設定の高しきい値と比較します。

次のいずれの例でも、ファームの [電源管理] 設定は [最適化されたパフォーマンス] です。最適化されたパフォーマンス設定の高しきい値は 50% です。つまり、使用率が 50% に到達すると、システムは未使用の仮想マシンの 1 つをパワーオンします。

注： 次の例では、ファームの [仮想マシンの最大数] 設定は 1 より大きい値にする必要があります。そうしないと、拡張は実行されません。

例：セッション占有量が高しきい値を超えたためにファームを拡張

この例では、設定は次のとおりです。

- 仮想マシン 1 台あたりのセッション数 = 20
- 電源管理の高しきい値 = 50%

拡張前	拡張後
パワーオン状態の仮想マシン 仮想マシン 1 ■ 実行中のセッション数 = 10 ■ エージェント ロード インデックス = 25% **使用量値** ■ セッション占有率 = 実行中のセッション数 10 / （仮想マシン 1 台あたり 20 セッション x 1 台の仮想マシン） = 50% ■ 平均ロード インデックス = エージェント ロード インデックス 25% / 1 台の仮想マシン = 25% 2 つの値の高い方は 50% で、これは、電源管理の最適なパフォーマンス設定の高しきい値に一致します。その結果、システムは 2 台目の仮想マシンをパワーオンします。	**パワーオン状態の仮想マシン** 仮想マシン 1 ■ 実行中のセッション数 = 10 ■ エージェント ロード インデックス = 25% 仮想マシン 2 ■ 実行中のセッション数 = 0 ■ エージェント ロード インデックス = 0% **使用量値** ■ セッション占有率 =（実行中のセッション数 10 + 0）/（仮想マシン 1 台あたり 20 セッション x 2 台の仮想マシン）= 25% ■ 平均ロード インデックス =（エージェント ロード インデックス 25% + 0%）/ 2 台の仮想マシン = 12.5% 2 つの値のうちの高い方は 25% で、これは、電源管理の最適なパフォーマンス設定の高しきい値を下回っています。このため、システムは何もアクションを実行しません。

例：平均ロード インデックスが高しきい値を超えたためにファームを拡張

この例では、設定は次のとおりです。

- 仮想マシン 1 台あたりのセッション数 = 20
- 電源管理の高しきい値 = 50%

拡張前	拡張後
パワーオン状態の仮想マシン 仮想マシン 1 ■ 実行中のセッション数 = 5 ■ エージェント ロード インデックス = 50% **使用量値** ■ セッション占有率 = 実行中のセッション数 5 /（仮想マシン 1 台あたり 20 セッション x 1 台の仮想マシン） = 25% ■ 平均ロード インデックス = エージェント ロード インデックス 50% / 1 台の仮想マシン = 50% 2 つの値の高い方は 50% で、これは、電源管理の最適なパフォーマンス設定の高しきい値に一致します。その結果、システムは 2 台目の仮想マシンをパワーオンします。	**パワーオン状態の仮想マシン** 仮想マシン 1 ■ 実行中のセッション数 = 5 ■ エージェント ロード インデックス = 50% 仮想マシン 2 ■ 実行中のセッション数 = 0 ■ エージェント ロード インデックス = 0% **使用量値** ■ セッション占有率 =（実行中のセッション数 5 + 0）/（仮想マシン 1 台あたり 20 セッション x 2 台の仮想マシン） = 12.5% ■ 平均ロード インデックス =（エージェント ロード インデックス 50% + 0%）/ 2 台の仮想マシン = 25% 2 つの値のうちの高い方は 25% で、これは、電源管理の最適なパフォーマンス設定の高しきい値を下回っています。このため、システムは何もアクションを実行しません。

Horizon Cloud ポッド内のネットワーク セキュリティ グループとファームについて

Microsoft Azure サブスクリプションにデプロイされた Horizon Cloud ポッドごとに、ポッドのリソース グループにはテンプレートとして機能するネットワーク セキュリティ グループ (NSG) も作成されます。このテンプレートを使用して、ファームによって提供されるリモート アプリケーションまたは RDS デスクトップに必要となる可能性がある追加のポートを確実に開くことができます。

Microsoft Azure では、ネットワーク セキュリティ グループ (NSG) は Azure Virtual Network (VNet) に接続されたリソースへのネットワーク トラフィックを管理します。NSG は、そのネットワーク トラフィックを許可または拒否するセキュリティ ルールを定義します。NSG によるネットワーク トラフィックのフィルタ方法の詳細については、Microsoft Azure のドキュメントで「Filter network traffic with network security groups」のトピックを参照してください。

Horizon Cloud ポッドが Microsoft Azure にデプロイされると、`vmw-hcs-podID-nsg-template` という名前の NSG がポッドの `vmw-hcs-podID` という同じ名前のリソース グループに作成されます。*podID* はポッド ID です。ポッドの詳細ページ（Horizon Universal Console の [キャパシティ] ページからアクセスする）からポッドの ID を取得できます。

デフォルトでは：

- Microsoft Azure は、各 NSG が作成されると自動的にいくつかのデフォルトのルールを作成します。作成されるすべての NSG で、Microsoft Azure はいくつかのインバウンド ルールとアウトバウンド ルールを 65000 以上の優先度で作成します。このような Microsoft Azure のデフォルトのルールは、ユーザーまたはシステムが Microsoft Azure で NSG を作成すると、Microsoft Azure によって自動的に作成されるので、このドキュメントのトピックでは説明されません。これらのルールは Horizon Cloud によって作成されるものではありません。これらのデフォルトのルールの詳細については、Microsoft Azure ドキュメントの「デフォルトのセキュリティ ルール」トピックを参照してください。
- Horizon Cloud ポッド デプロイヤは、ポッドのテンプレート NSG に次のインバウンド セキュリティ ルールを作成します。これらのデフォルトのインバウンド セキュリティ ルールは、Blast、PCOIP および USB リダイレクトのためのエンド ユーザー クライアントによる RDS セッション デスクトップおよびリモート アプリケーションへのアクセスをサポートします。

表 6-3. ポッドのテンプレート NSG で Horizon Cloud ポッド デプロイヤによって作成されたインバウンド セキュリティ ルール

優先順位	名前	ポート	プロトコル	ソース	送信先	アクション
1000	AllowBlastUdpIn	22443	UDP	インターネット	任意	許可
1100	AllowBlastTcpIn	22443	TCP	インターネット	任意	許可
1200	AllowPcoipTcpIn	4172	TCP	インターネット	任意	許可
1300	AllowPcoipUdpIn	4172	UDP	インターネット	任意	許可

表 6-3. ポッドのテンプレート NSG で Horizon Cloud ポッド デプロイヤによって作成されたインバウンド セキュリティ ルール （続き）

優先順位	名前	ポート	プロトコル	ソース	送信先	アクション
1400	AllowTcpSideChannelIn	9427	TCP	インターネット	任意	許可
1500	AllowUsbRedirectionIn	32111	TCP	インターネット	任意	許可

このテンプレート NSG に加えて、ファームが作成されるときに、システムはテンプレート NSG をコピーすることによってそのファームの NSG を作成します。各ファームには、テンプレート NSG のコピーである独自の NSG があります。ファームの NSG は、そのファームの仮想マシンの NIC に割り当てられます。デフォルトでは、すべてのファームは、ポッドのテンプレート NSG で設定されているのと同じデフォルトのセキュリティ ルールを使用します。

テンプレート NSG とファームごとの NSG の両方を変更できます。たとえば、追加のポートを開いておく必要があるアプリケーションがファームにある場合は、ポートでネットワーク トラフィックを許可するようにファームの NSG を変更します。同じポートを開く必要がある複数のファームを作成する場合、テンプレート NSG をあらかじめ編集しておくと、ファームの作成が容易になります。

重要： 基本テンプレートを変更する計画の場合は、変更前にコピーを作成します。元のデフォルト設定に戻す必要がある場合に、コピーをバックアップとして使用することができます。

Horizon Cloud インベントリ内のアプリケーション

Horizon Universal Console の [アプリケーション] ページを使用して、Horizon Cloud 環境のインベントリにあるアプリケーションを操作し、新しいアプリケーションをインベントリに追加します。これらのアプリケーションは、エンド ユーザーが使用するために提供するものです。コンソールで、[アプリケーション] ページを開くには、[インベントリ] - [アプリケーション] をクリックします。

システムは、アプリケーションのソースに応じて、このインベントリ内のアプリケーションを分類します。

- App Volumes のアプリケーションには、App Volumes を使用して作成されたアプリケーション パッケージが含まれます。Microsoft Azure にデプロイされたポッドで App Volumes の機能を使用するように Horizon Cloud テナントが構成されている場合に、コンソールはそのアプリケーションをインベントリに追加するために使用します。Microsoft Azure 上の Horizon Cloud の App Volumes アプリケーション - 概要および前提条件を参照してください。
- リモート アプリケーションとは、アプリケーションの種類の RDSH ファームからインベントリに追加されたものです（コンソールの [ファーム] ページに表示）。インベントリに追加するときに、これらのリモート アプリケーションをユーザーに割り当てることができます。リモート アプリケーション - Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた RDSH ファームからのインポートを参照してください。

新しいアプリケーションをインベントリに追加することに加えて、このページでは、アプリケーションを編集したり、インベントリから削除したりすることもできます。

Microsoft Azure 上の Horizon Cloud の App Volumes アプリケーション - 概要および前提条件

App Volumes アプリケーション機能を使用して、アプリケーションのライフサイクル全体を管理できます。これには、アプリケーションのパッケージ作成、更新、およびリタイアが含まれます。アプリケーションの割り当てをカスタマイズして、特定のバージョンのアプリケーションをエンド ユーザーに提供することもできます。

重要： 第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアーに記載されているように、クラウドベースのコンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。機能へのアクセスは、テナントのリージョン クラウド プレーン、クラウドに接続されたポッドが最新レベルのソフトウェアを実行しているかどうか、機能が特定のライセンスに基づいているかどうかなどの要因によって異なります。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。使用したい機能が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て、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。

Horizon Cloud の VMware App Volumes 機能の概要

次の表は、Horizon Cloud の VMware App Volumes 機能の概要を示しています。

機能領域	説明
デプロイ	■ 完全に自動化されたデプロイ。App Volumes マネージャ、App Volumes データベース、ストレージなどの App Volumes インフラストラクチャ コンポーネントの自動プロビジョニング。 ■ データベースのニーズに合わせて Microsoft Azure PostgreSQL マネージド サービスを利用します。追加のデータベース管理は不要です。 ■ ポッドのセットアップ時に、アプリケーションを保存および配信するための Microsoft Azure ファイル共有の自動プロビジョニング。
管理コンソール	■ App Volumes コンソールは、Horizon Universal Console にシームレスに統合されます。デスクトップとアプリケーションを同じコンソールで管理します。 ■ App Volumes Agent のインストール エクスペリエンスは、Horizon Cloud イメージ作成ワークフローにシームレスに統合されています。
App Volumes 4 Agent	オンプレミスおよび Microsoft Azure デプロイの両方に使用される統合され、パフォーマンス最適化されたエージェント。
パッケージ作成	■ Microsoft Azure ファイル共有を使用して提供される VHD ベースのパッケージをサポートしています。 ■ アプリケーション パッケージの作成は Horizon Cloud 内でネイティブに実行されます。コマンドライン ツールは不要です。 ■ ユーザーは、App Volumes を使用して、MSIX アプリケーション添付の VHD をインポートし、この新しいパッケージ形式を提供できます。
アプリケーション ライフサイクル管理	すでに App Volumes 4 オンプレミスの一部となっている SAM (Simplified Application Management) 機能をサポートします。管理者は、アプリケーションのライフサイクル全体（パッケージ作成、更新、リタイアなど）を管理できるようになりました。

機能領域	説明
アプリケーション割り当て	■ 管理者は、アプリケーションの割り当てをカスタマイズして、特定のバージョンのアプリケーションをエンド ユーザーに提供することができます。 ■ マルチポッド アプリケーションの提供をサポートします。
ハイブリッド クラウドのサービス	オンプレミスの App Volumes ユーザーが、オンプレミスのデプロイから Microsoft Azure 上の Horizon Cloud にアプリケーション パッケージをインポートできるようになりました。オンプレミス パッケージを再利用します。Microsoft Azure 用にパッケージを作成し直す必要はありません。

App Volumes アプリケーション プロセスの概要

ユーザーが App Volumes アプリケーションを使用できるようにするには、次の 2 段階のプロセスがあります。

- Horizon Universal Console で App Volumes アプリケーションを追加します。これを行うには、次の 2 つの方法があります。
  - 新しいアプリケーション パッケージを作成してインポートすることにより、App Volumes アプリケーションを追加します。

    アプリケーション パッケージがまだ作成されていない場合は、[作成] オプションを使用して作成できます。これにより、App Volumes を使用してアプリケーション パッケージが作成され、自動的にインポートされます。作成ワークフローを使用して、App Volumes アプリケーションを Horizon Cloud テナントのインベントリに追加するを参照してください。
  - 既存のアプリケーション パッケージをインポートすることにより、App Volumes アプリケーションを追加します。

    以前に App Volumes で作成されているアプリケーション パッケージがある場合は、[インポート] オプションを使用してインポートできます。これは、アプリケーション パッケージを作成し直すことなく、オンプレミスのデプロイからアプリケーション パッケージを再利用できることを意味します。Horizon Cloud：既存のアプリケーション パッケージをインポートして App Volumes アプリケーションを追加を参照してください。
- App Volumes アプリケーションをユーザーに割り当てる App Volumes 割り当てを作成します。Horizon Cloud：App Volumes 割り当ての作成を参照してください。

Horizon Cloud on Microsoft Azure 環境で App Volumes を使用するための要件と前提条件

重要： App Volumes アプリケーションにアクセスできなくなり、Horizon Cloud on Microsoft Azure 環境の App Volumes 機能のサポートが無効になるのを防ぐには、App Volumes 関連のストレージ アカウントのストレージ アカウント キーを、そのキーの有効期限切れ、変更、ローテーションを引き起こすような方法で操作しないようにする必要があります。

ストレージ アカウント キーが手動または Azure ポリシーを介してローテーションされると、App Volumes が依存するストレージ アカウントとファイル共有にアクセスできなくなります。この問題が発生した場合、環境内に保存されているストレージ キーが無効なため、App Volumes はエンド ユーザーにアプリケーションを配信できません。

Horizon Cloud on Microsoft Azure 環境は指定された Azure サブスクリプションに存在しますが、環境の App Volumes 関連ストレージ アカウントは、ポッド マネージャ マシン、Unified Access Gateway マシン、および Azure サブスクリプションにプロビジョニングされるその他のサービスによってデプロイされたその他のリソースと同じ VMware 管理コンポーネントです。すべての Horizon Cloud on Microsoft Azure 環境には、App Volumes 関連のストレージ アカウントのデプロイが含まれます。

サービスがポッド マネージャ マシンをデプロイすると、サービスはこの App Volumes 関連のストレージ アカウントを Azure サブスクリプションにプロビジョニングします。このストレージ アカウントの目的は、App Volumes アプリケーション ファイルがプロビジョニングされるファイル共有を提供することです。

このストレージ アカウントのデータは、Microsoft 管理のキーを使用して Azure Storage によって自動的に暗号化されます。ユーザーまたは組織がこのストレージ アカウント キーの期限切れ、変更、ローテーションを行うと、ストレージ キーが無効になります。この問題が発生すると、App Volumes はファイル共有にアクセスできず、エンド ユーザーにアプリケーションを配布できなくなります。

App Volumes アプリケーションをインベントリに追加する前に、環境が次の前提条件を満たしていることを確認します。

ポッド関連の前提条件

- 単一セッション タイプの Microsoft Windows オペレーティング システムで App Volumes 機能を使用するには、Horizon Cloud Service on Microsoft Azure 環境がマニフェスト 2298.x 以降を実行している必要があります。
- Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムで App Volumes 機能を使用するには、環境がマニフェスト 2747.x 以降を実行している必要があります。
- 環境にはゲートウェイ構成（Unified Access Gateway インスタンス）が必要です。また、Unified Access Gateway インスタンスで構成された Horizon Cloud on Microsoft Azure 環境の場合と同様に、Unified Access Gateway の FQDN マッピング手順を完了している必要があります。
- 各ポッドの詳細ページを確認し、ページに各ポッドにマウントされたファイル共有があることを確認してください。コンソールでは、Active Directory ドメイン登録ワークフローを完了した後に、ポッドの詳細ページに移動できます。これらのファイル共有はサービスによって生成され、App Volumes 機能の使用はその存在に依存します。

ポッドの詳細ページを表示するには、[キャパシティ] ページ（[設定] - [キャパシティ]）に移動して、ポッドをクリックします。ここで次のことを確認します。

- [プロパティ] の [FileShare] フィールドの値が 2 で、数字にカーソルを合わせると、両方のファイル共有が表示されます。
- ページの下部にある [ゲートウェイ] 設定が入力されている。これは、Unified Access Gateway が構成されていることを示します。

構成要件

- 1 章 第 1 世代テナント - Horizon Cloud 環境の使用を開始するの説明に従って、Active Directory ドメイン登録ワークフローを完了したこと。
- Horizon Universal Console を使用してドメインを登録した後、Active Directory ドメインのドメイン コントローラ ポリシーの [ドメイン コントローラ: LDAP サーバ署名要件] を [署名が必要] に設定している場合、次の手順を実行する必要があります。
  a [設定] - [Active Directory] ページで、[ドメイン バインド] の横にある編集（鉛筆）アイコンをクリックします。
  b [バインド パスワード] テキスト ボックスにプライマリ バインド アカウントのパスワードを入力します。その他の変更は行わないでください。
  c [ドメイン バインド] をクリックします。
- Horizon Cloud の第 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満たすだけでなく、TCP プロトコル トラフィック用のポート 445 を開く必要があります。ポート 445 は、Microsoft Windows の SMB ファイル共有にアクセスするための標準の SMB ポートです。AppStack は、Microsoft Azure サブスクリプションのポッドのリソース グループにある SMB ファイル共有に保存されます。

イメージの要件

コンソールで作成ワークフローを使用して、アプリケーション パッケージを作成して App Volumes アプリケーションを追加するには、コンソールのインベントリに次の条件を満たす公開イメージが必要です。

- クライアント タイプの Microsoft Windows 10 または Windows 11 オペレーティング システムを実行している。このクライアント タイプは、VDI タイプのオペレーティング システムと呼ばれる場合があります。クラウド内キャプチャ ワークフローは、VDI タイプのオペレーティング システムでのみ使用できます。クラウド内キャプチャ ワークフローは、マルチセッションまたは RDS タイプのオペレーティング システムでは使用できません。
- App Volumes Agent がインストールされている。

Microsoft Azure の Horizon Cloud ポッド内の App Volumes アプリケーションで Microsoft Windows 10 または 11 Enterprise マルチセッション イメージを使用するためのベスト プラクティス

次のベスト プラクティスにより、ユーザーと管理者の使用環境の向上につながります。Microsoft Azure の Horizon Cloud ポッド内の App Volumes アプリケーションで Microsoft Windows 10 または 11 Enterprise マルチセッション イメージを設定するも参照してください。

- 基本イメージに、プリンタ ドライバを使用してハードウェア プリンタをインストールします。関連する既知の問題の情報（特に既知の問題のトピック）については『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』ガイドを参照してください。
- Microsoft のドキュメント FAQ で説明されているように、Microsoft Windows 10 Enterprise マルチセッションは、以前は Microsoft Windows Server オペレーティング システムでのみ提供された複数の同時対話型セッションを許可する Remote Desktop Session Host (RDSH) タイプの仮想マシンです。Microsoft Windows 10 Enterprise マルチセッションは RDSH タイプのオペレーティング システムであるため、VDI 関連のワークフローではなく、Horizon Cloud RDSH に該当するワークフローが適用されます。したがって、これらのマルチセッション システムに基づいてエンド ユーザーにセッション デスクトップを提供するには、ファームの作成の説明に従ってファームを作成します。ファームに基づいたセッション デスクトップで App Volumes アプリケーションの使用をサポートするには、次のすべてのファーム設定が必要です。これらの設定によりファーム仮想マシンのオペレーティング システム ディスクが定期的に初期状態に更新され、この定期的な更新は、そのような仮想マシンでの App Volumes アプリケーションの使用をサポートするために必要です。

  必要なローリング メンテナンスの設定

  - メンテナンス タイプ：[セッション]
  - セッション数：仮想マシン 1 台あたりのセッション数と同じ
  - [仮想マシン アクション]：[再構築]
  - [同時に静止する仮想マシン数]：ファーム サイズの 40%

  必要なタイムアウト処理の設定

  - [切断済みセッションのログオフ]：90 分後のタイムアウト
  - [セッション タイムアウト間隔]：90 分
- Microsoft Windows 10 マルチセッションでアプリケーション パッケージとしてプロビジョニングする各アプリケーションの自動更新サービスを無効にする必要があります。このタイプの Microsoft Windows 10 マルチセッション環境では、自動更新の動作に問題があります。
  - アプリケーションに自動更新サービスがある場合は、アプリケーションのプロビジョニング プロセス中に、Windows Services Manager などのサービスを無効にします。
  - アプリケーション プロビジョニング プロセス中に自動更新サービスを無効にできない場合や無効にしない場合は、未割り当てのアプリケーションの不完全なバージョンをユーザーが受け取るなどの問題が発生した後で、レジストリを構成して基本イメージを変更します。このように構成することで、アプリケーション パッケージがユーザー仮想マシンにデプロイされるときに、目的のサービスが確実に開始されなくなります。

具体的には、アプリケーション サービス名を svservice レジストリ構成 [DisableAppServicesList] に追加してレジストリを構成します。関連する既知の問題の情報（特に既知の問題のトピック）については『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』ガイドを参照してください。

- アプリケーションをインストールしたり、同じ仮想マシン上のすべてのユーザー セッション間で共有しないファイルを作成したりするときに、ファイルをユーザー自身のプロファイルの場所に配置できることをユーザーに通知します。

Microsoft Azure の Horizon Cloud ポッド内の App Volumes アプリケーションで Microsoft Windows 10 または 11 Enterprise マルチセッション イメージを設定する

Microsoft Azure の Horizon Cloud の App Volumes で Microsoft Windows 10 または 11 Enterprise マルチセッション イメージを使用することを選択した場合は、処理中に特定のアクションを実行する必要があります。この処理は、以下の高度な手順に示すように、まず基盤となる Microsoft Windows Enterprise マルチセッション オペレーティング システムの作成から始まり、App Volumes 割り当てを作成してユーザーにアプリケーションを提供することで終わります。

その後に続く手順の背景情報については、Microsoft Azure 上の Horizon Cloud の App Volumes アプリケーション - 概要および前提条件を参照してください。

Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムで App Volumes 機能を使用するには、ポッドのマニフェストが 2747.x 以降である必要があります。

次のリストにリンクされている手順を実行する場合は、Microsoft Azure の Horizon Cloud ポッドの App Volumes 機能で使用する Microsoft Windows 10 または 11 Enterprise マルチセッション イメージの構成に固有の手順を確認してください。

重要：

- マルチセッションのマシンでは、アプリケーション パッケージの分離は、そのパッケージを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ます。ボリュームを接続解除するために、対応する仮想マシンをシャットダウンする必要はありません。
- システムのクラウド内キャプチャ ワークフローは、マルチセッションまたは RDS タイプのオペレーティング システムでは使用できません。このクラウド内キャプチャ ワークフローは、コンソールで [App Volumes] - [作成] を選択して実行されます。

  したがって、クラウド内キャプチャ ワークフローを使用して App Volumes アプリケーションをテナント インベントリに追加するには、クライアント タイプの Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムに基づくイメージを使用する必要があります。これは VDI タイプのオペレーティング システムと呼ばれることもあり、これをクラウド内キャプチャ ワークフローに使用します。次に、これらのアプリケーションがインベントリにある場合、Microsoft Windows 10 または 11 Enterprise マルチセッション イメージを使用してファームによってプロビジョニングされたセッションベースのデスクトップで使用できます。セッションベースのデスクトップを基盤となるデスクトップのエンド ユーザーに割り当てたら、それらのキャプチャした App Volumes アプリケーションを同じエンド ユーザーに割り当て、そのセッションベースのデスクトップ内で使用できるようにします。

---

1. App Volumes アプリケーションを Horizon Cloud インベントリに追加する

セッションベースのデスクトップの資格を付与したエンド ユーザーに App Volumes アプリケーションを割り当てる前に、テナントのインベントリにその App Volumes アプリケーションが含まれている必要があります。コンソールの作成ワークフローまたはインポート ワークフローを使用して、テナントのインベントリに App Volumes アプリケーションを追加できます。

ただし、作成ワークフローは、マルチセッション タイプのオペレーティング システムでは使用できません。作成ワークフローを使用してアプリケーションをインベントリに追加する場合は、そのワークフローで使用し、その VDI タイプのオペレーティング システムからアプリケーションをキャプチャするために、クライアント タイプ、VDI タイプの Microsoft Windows 10 または 11 オペレーティング システムが必要です。

- コンソールの作成ワークフローを使用して、VDI タイプの Microsoft Windows 10 または 11 オペレーティング システムからインベントリにアプリケーションを追加します。手順については、作成ワークフローを使用して、App Volumes アプリケーションを Horizon Cloud テナントのインベントリに追加するを参照してください。
- コンソールのインポート ワークフローを使用して、Horizon Cloud テナントの外部で手動でキャプチャし、Microsoft Azure ポータルを使用してポッドのステージング ファイル共有に手動でアップロードした App Volumes アプリケーションをインベントリに追加します。このワークフローは、主に一部のオンプレミスの App Volumes インストールからの App Volumes パッケージがすでにあり、それらのパッケージを Horizon Cloud インベントリで再利用する場合に使用されます。詳細については、Horizon Cloud：既存のアプリケーション パッケージをインポートして App Volumes アプリケーションを追加

2. App Volumes アプリケーションの資格を新しいユーザーに付与する

作成したばかりの 1 つ以上の App Volumes アプリケーションを含む、新しいユーザーの App Volumes 割り当てを作成します。Horizon Cloud：App Volumes 割り当ての作成を参照してください。

重要： 管理者権限を必要とするサービスが Microsoft Windows 10 または 11 Enterprise マルチセッション アプリケーション パッケージにキャプチャされている場合、そのアプリケーション パッケージに割り当てられているすべてのユーザーにも管理者権限が必要です。

3. Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムの基盤となるデスクトップを作成し、ユーザーに資格を割り当てる

このプロセスの最初の部分には、次の手順が含まれています。

1 Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システムのデスクトップ イメージを作成します。Microsoft Azure でのデスクトップ イメージと Horizon Cloud ポッドの作成を参照してください。

   注： イメージのベース仮想マシンを作成するときに、App Volumes Agent をインストールします。

2 新しい Microsoft Windows 10 または 11 Enterprise マルチセッション オペレーティング システム デスクトップ イメージを使用してファームを作成します。第 1 世代 Horizon Cloud ポッド - ファームの作成と管理を参照してください。

3 新しいファームに基づいて、エンド ユーザーに新しい Microsoft Windows 10 または 11 Enterprise マルチセッション セッション デスクトップの資格を付与します。Horizon Cloud ポッド - RDS ベースのセッション デスクトップ割り当てを作成して、エンド ユーザーのために RDS ホストからのデスクトップ セッションを提供するを参照してください。

作成ワークフローを使用して、App Volumes アプリケーションを Horizon Cloud テナントのインベントリに追加する

Horizon Universal Console の作成ワークフローを使用して、App Volumes アプリケーションをテナントのインベントリに追加します。この作成ワークフロー内で、システムは Horizon Cloud 内でネイティブにアプリケーション パッケージをキャプチャします。

背景情報については、VMware Digital Workspace Tech Zone にアクセスして、Horizon Cloud Service on Microsoft Azure の App Volumes のビデオ デモ ウォークスルーをご覧ください。

- [作成] オプションを初めて使用した後、キャプチャ デスクトップ仮想マシンでアプリケーション パッケージをキャプチャする手順を完了するまでは、同じユーザーが同じイメージに対してそのオプションの 2 回目の使用を試みることはできません。アプリケーション パッケージのキャプチャ手順を完了する前に、同じイメージに対して [作成] オプションを再度使用しようとすると、パッケージを作成する要求がすでに開始されていることを示すメッセージが表示されます。ただし、同じテナント内の別のユーザーは、最初のユーザーが完了したかどうかにかかわらず、そのイメージに対してパッケージの作成を開始できます。

  注： 同じポッドまたは別のポッドで異なるイメージを選択すると、同じユーザーが複数のキャプチャを同時に実行できます。同じイメージで複数のキャプチャを同時に実行することはできません。

- 初めて [作成] オプションをクリックしてキャプチャ プロセスを開始する場合、システムではキャプチャ デスクトップ仮想マシンの準備が完了してから `Desktop ready for application capture` に変更されるまで、最大で 20 分かかることがあります。この初めてのときの 20 分という時間は、システムがキャプチャ処理をサポートするためにデスクトップ割り当てと 2 台のデスクトップ仮想マシンを作成しているためです。最初のアプリケーション パッケージのキャプチャを完了してから新しいキャプチャ プロセスを開始すると、[作成] オプションをクリックしてから、ステータスが `Desktop ready for application capture` に変更されるまでの時間が 10 分ほど短くなります。初回のようにキャプチャ デスクトップ割り当てを作成する必要がないので、初回以降の時間は短くなります。2 回目は、以前に使用されたキャプチャ デスクトップ仮想マシンが削除され、新しい仮想マシンが使用されます。

前提条件

この手順を実行する前に、環境が次の前提条件を満たしていることを確認します。

- 環境が Microsoft Azure 上の Horizon Cloud の App Volumes アプリケーション - 概要および前提条件に記載されているすべての前提条件を満たしていることを確認します。

- 環境用に構成されたすべての Active Directory ドメインに、各構成でドメイン参加アカウントが構成されていることを確認します。構成を調べ、それぞれにドメイン参加アカウントが構成されていることを確認するには、コンソールで [設定] - [Active Directory] の順に移動し、構成された各ドメインの [ドメイン参加] セクションを見て、ドメイン参加アカウント名が存在することを確認します。

  重要： システムで作成された App Capture デスクトップ割り当ては、パッケージャ管理者ユーザーの Active Directory ドメインと、Horizon Cloud 環境用に構成された Active Directory ドメイン内で構成されたドメイン参加アカウント認証情報の使用に依存するため、ドメイン参加アカウントは App Capture 操作の必須の前提条件です。App Capture 操作では、そのドメイン参加アカウントを使用して、App Capture デスクトップをそのドメインに参加させます。パッケージャ管理者ユーザーは、Horizon Universal Console にログインし、以下で説明する App Capture の手順を実行する管理者として定義されます。

- **重要：** この作成ワークフローは、単一ユーザー、クライアント、または VDI タイプの Microsoft Windows オペレーティング システムのイメージでのみ使用でき、マルチセッション タイプのオペレーティング システムでは使用できません。以下のタスクの手順を開始する前に、App Volumes Agent がインストールされた使用可能なイメージが必要です。このようなイメージを作成するには、次の手順を実行します。
  - App Volumes Agent がインストールされ、クライアント タイプ、VDI タイプ、または単一セッション タイプのオペレーティング システム（Microsoft Windows 10、Microsoft Windows 11、または Microsoft Windows 7 など）を実行している仮想マシンをインポートします。ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリング のトピックのインポート手順を実行し、[詳細オプション] の下にある [App Volumes Agent] トグルを選択します。
  - インポートされた仮想マシンからイメージを作成します。これは、次の手順で新しいアプリケーション パッケージを作成するために使用するイメージです。

手順

1 コンソールで、[インベントリ] - [アプリケーション] を選択します。

[アプリケーション] ページの [App Volumes] タブが表示されます。

2 [新規] - [作成] をクリックします。

3 [新しいアプリケーション パッケージ] ウィンドウの [定義] の下に、以下に示す値を入力します。

オプション	説明
アプリケーション	[新規] ラジオ ボタンを選択し、アプリケーションの一意の名前を入力します。名前は英字 (a ～ Z) で開始し、英字 (a ～ Z)、ハイフン (-)、および数字のみで構成する必要があります。
説明	（オプション）アプリケーションの説明を入力します。
パッケージ	パッケージの一意の名前を入力します。
説明	（オプション）パッケージの説明を入力します。

4 [新しいアプリケーション パッケージ] ウィンドウの [アプリケーション パッケージのデスクトップ] の下に、以下に示す値を入力します。

オプション	説明
場所	[ポッド] ドロップダウン メニューに表示されるポッドのセットをフィルタする場所を選択します。
ポッド	[イメージ] ドロップダウン メニューに表示されるポッドのセットをフィルタするポッドを選択します。ドロップダウン メニューには、App Volumes が有効で、App Volumes Agent がインストールされたイメージを少なくとも 1 つ持ち、Unified Access Gateway が有効になっている[ポッド]のみが表示されます。
イメージ	[イメージ] ドロップダウン メニューからイメージを選択します。 **注：** メニューには、App Volumes Agent がインストールされ、単一ユーザー タイプまたはクライアント タイプのオペレーティング システムを実行しているイメージのみが表示されます。このようなイメージの作成の詳細については、上記の前提条件を参照してください。

5 アプリケーションのリストの下で、アプリケーションをオンデマンドで配信するか、次回のログインまたは起動時に配信するかを選択します。

- [オンデマンド] : ユーザーがパッケージのショートカットをクリックした後にのみパッケージを配信するには、このオプションを選択します。
- [ログイン時] : ログインまたは起動時にパッケージを配信するには、このオプションを選択します。これはデフォルトです。

6 [保存] をクリックします。

ユーザーがキャプチャ プロセスを初めて開始するときは、キャプチャ デスクトップ仮想マシンがアプリケーションのキャプチャに使用できるようになるまで、最大で 20 分かかります。この 20 分間に、システムは、キャプチャ デスクトップ仮想マシンに使用されるキャプチャ プロセスの VDI デスクトップ割り当てを 1 つ以上作成しています。システムが基盤となる割り当てと仮想マシンを作成するには、最大で 20 分かかる場合があります。

- システムは、ポッドごとに 1 つのイメージにつき割り当てを 1 つ作成します。このため、1 つまたは複数の割り当てを作成する場合があります。
- 各割り当ては、キャプチャを実行している同時ユーザー数に合わせて拡張され、常にパワーオフ状態の余分な仮想マシンが 1 台あります。最初のユーザーがキャプチャ プロセスを開始すると、2 台の仮想マシンが作成されます。1 台はキャプチャのためにそのユーザーに割り当てられ、もう 1 台はパワーオフされます。2 つ目のユーザーがキャプチャを開始すると、割り当ては 3 台の仮想マシンに拡張され、最終的には割り当てのキャパシティの上限まで拡張されます。各キャプチャが完了すると、キャプチャで使用された仮想マシンが削除され、割り当てのキャパシティが減少します。通常、キャプチャが実行されていないときの割り当てのデフォルト サイズは、1 台の仮想マシンです。ただし、割り当ての仮想マシンの数を一時的にゼロにすることは可能です。いずれの場合でも、最初のユーザーがキャプチャを開始すると、上記のようにサイズが 2 台の仮想マシンに増加します。
- これらの割り当ては `appcaptureXXX` パターンに従って名前が付けられます。ここで、`XXX` はランダムに生成された番号になります。

- 次に説明するように、割り当ての場所は異なります。
  - コンソールの [ブローカ] ページのテナントの構成に応じて、またその構成を反映するコンソールの動的な性質により、割り当て用のコンソールの左側のナビゲーションには、たとえば、[割り当て] - [VDI デスクトップとアプリ] または [割り当て] - [RDSH デスクトップとアプリ] のような [デスクトップ] と [アプリケーション] のラベルの組み合わせが表示されたり、それらの行に沿っていくつかの組み合わせが表示されたりします。[アプリケーション] ラベルが付いているコンソールのパスのタイプの場合は、これらの割り当てが表示されます。
  - コンソールの [ブローカ] ページで、Horizon Cloud ポッドの Universal Broker が有効になっていることが示され、割り当てが非マルチクラウド割り当てに基づいている場合、それらは [割り当て] - [RDSH デスクトップとアプリ] に表示されます。

    注： 2020 年 12 月 9 日の更新前に実行したキャプチャからの割り当てがあり、Horizon Cloud ポッドの Universal Broker が有効になっている場合は、それらの割り当てを [RDSH デスクトップとアプリ] コンソール ページから削除することをお勧めします。Universal Broker を有効にすると、キャプチャ プロセスで作成されたすべての新しい割り当てがマルチクラウド割り当てになり、以下で説明するように、[VDI デスクトップとアプリ] と [RDSH デスクトップとアプリ] の両方に表示されます。
  - コンソールの [ブローカ] ページで、Horizon Cloud ポッドの Universal Broker が有効になっていることが示され、割り当てがマルチクラウド割り当てに基づいている場合、それらは [割り当て] - [VDI デスクトップとアプリ] と [割り当て] - [RDSH デスクトップとアプリ] の両方の場所に表示されます。

    注： 割り当てが両方の場所に表示される場合、名前は少し異なります。[RDSH デスクトップとアプリ] での割り当ての名前には英数字文字列が追加されています。たとえば、[VDI デスクトップとアプリ] の `appcapture1234` という名前の割り当ては、[RDSH デスクトップとアプリ] では `appcapture1234-5ab6c789` という名前になります。

    重要： これらの割り当てのいずれかを削除する前に、割り当ての削除に関する以下の情報を確認してください。
- 割り当ての削除について：
  - 近い将来に追加のキャプチャを実行する予定がない場合は、これらの割り当てを削除して、理由もなく環境内に存在しないようにすることができます。削除した場合、次回キャプチャを実行したときに、システムは新しいものを作成するまでに最大で 20 分かかります。

- パッケージ プロセスに使用されるイメージを更新する場合は、更新する前にこれらの割り当てを削除する必要があります。

注目: 上記のように、[割り当て] - [VDI デスクトップとアプリ] と [割り当て] - [RDSH デスクトップとアプリ] の両方で表示される割り当てを削除する場合、[割り当て] - [RDSH デスクトップとアプリ] ページでは割り当てを削除しないでください。ここで削除するとエラーが発生します。代わりに、[割り当て] - [VDI デスクトップとアプリ] ページから割り当てを削除してください。これにより、両方のページから割り当てが削除されます。

割り当てが両方の場所に表示される場合、名前は少し異なることに注意してください。[割り当て] - [RDSH デスクトップとアプリ] での割り当ての名前には英数字文字列が追加されています。たとえば、[割り当て] - [VDI デスクトップとアプリ] の `appcapture1234` という名前の割り当ては、[割り当て] - [RDSH デスクトップとアプリ] では `appcapture1234-5ab6c789` という名前になります。

ヒント: [監視] - [通知] に移動して、キャプチャの進行状況に関する有用な情報と、手順の各ポイントでの次のステップを表示できます。パッケージの作成、割り当ての作成、割り当てのステータスに関する通知があります。通知では、割り当て名、パッケージ名、各キャプチャを実行するユーザーの ID も確認できます。何らかの理由でキャプチャに失敗した場合は、通知を確認して、報告されたエラーを表示できます。

これで、[アプリケーション] ページのリストにアプリケーション パッケージのエントリが作成されます。このリスト エントリの [ステータス] をポイントすると、キャプチャ仮想マシンのステータスが示されます。ステータスが `Desktop ready for application capture` の場合は、手順に従ってキャプチャ デスクトップ仮想マシンにログインし、アプリケーション パッケージのアプリケーションのインストールを開始できます。

7 [アプリケーション] ページで、アプリケーションの名前をクリックします。

アプリケーションの [アプリケーションの詳細] ページが表示されます。

8 新しいアプリケーション パッケージを選択し、[キャプチャの開始] をクリックします。

新しいブラウザ タブで、Horizon HTML Access（ブラスト）ログイン フォームが開きます。

9 Horizon Universal Console へのログインに使用したものと同じ認証情報を使用してログインします。

10 Horizon HTML Access クライアントで、キャプチャ デスクトップ仮想マシンを起動します。

注意: キャプチャ仮想マシンにログインするために使用されるユーザー名にはローカル管理者権限が必要です。そうでないと、ユーザーには [パッケージング中] ダイアログ ボックスが表示されません。

Windows デスクトップに、[VMware App Volumes - パッケージの進行中] ダイアログ ボックスが、[パッケージング中...] のメッセージとともに表示されます。

重要： このダイアログ ボックスを閉じないでください。必要に応じて、アプリケーション パッケージに必要なアプリケーションのインストールが完了するまで、邪魔にならない場所に移動します。

11 アプリケーション パッケージにパッケージ化するアプリケーションをインストールします。

注： キャプチャ セッションごとに 1 つのアプリケーションのみをキャプチャすることがベスト プラクティスです。1 つのアプリケーションをインストールして、キャプチャ プロセスを終了します。アプリケーションのアプリケーション パッケージがコンソールの [アプリケーション] ページに表示されている場合は、新しいパッケージに別のアプリケーションをキャプチャできます。Horizon Cloud：既存の App Volumes アプリケーションへの新しいアプリケーション パッケージの追加を参照してください。

12 [VMware App Volumes - パッケージの進行中] ダイアログ ボックスで [OK] をクリックします。アプリケーションのインストールが終了したら、[App Volumes – パッケージの進行中] ウィンドウで OK をクリックします。次の [App Volumes –パッケージの進行中] ウィンドウが表示されます。

[VMware App Volumes - パッケージの進行中] ダイアログ ボックスに、[インストールが完了しましたか?] というメッセージが表示されます。

13 [はい] をクリックします。

[VMware App Volumes - パッケージの完了] ダイアログ ボックスが表示されます。

14 名前とバージョンに必要な変更を加え、必要に応じて説明を追加します。

15 [完了] をクリックします。

仮想マシンの再起動を求めるメッセージが表示されます。

16 [OK] をクリックして、仮想マシンの再起動を許可します。

キャプチャ デスクトップ仮想マシンが再起動すると、HTML Access クライアント セッションによって切断されたことを示すメッセージが表示されます。

17 キャプチャ デスクトップ仮想マシンがオンラインに戻ったら、再度ログインして、[パッケージ化に成功しました!]というメッセージを確認します。

18 キャプチャ デスクトップ仮想マシンからログアウトします。

結果

[アプリケーションの詳細] ページに、`Application capture in progress` のステータスで新しいアプリケーション パッケージ表示されます。アプリケーション パッケージのインポートが完了すると、ステータスは `Success` に変わります。

Horizon Cloud：既存のアプリケーション パッケージをインポートして App Volumes アプリケーションを追加

Horizon Universal Console で、これらの手順に従い、Microsoft Azure ストレージにすでにあるアプリケーション パッケージをインポートして、App Volumes アプリケーションを作成します。

このタスクには次のような背景があります。

- Microsoft Azure Storage Explorer の操作の詳細については、Storage Explorer のドキュメントを参照してください。

- [プラットフォームでプロビジョニングされたファイル共有]：プラットフォームは、次のように、オンボーディングされた Microsoft Azure ポッドごとに顧客サブスクリプションで 2 つのファイル共有をプロビジョニングします。
  - [Staging] は、インポートする必要があるアプリケーション パッケージをステージングする場所であり、アプリケーション パッケージをエンド ユーザーに配信する場所でもあります。
  - [Delivery] は、アプリケーション パッケージをエンド ユーザーに配信する場合にのみ使用されます。

前提条件

- 環境が Microsoft Azure 上の Horizon Cloud の App Volumes アプリケーション - 概要および前提条件に記載されているすべての前提条件を満たしていることを確認します。
- ファイアウォールを介してステージング ファイル共有にアクセスできるアドレスの許可リストに、クライアント IP アドレスを追加します。Microsoft Azure ポータルで、ストレージ アカウントのネットワーク セキュリティ設定を含むページに移動します。[ファイアウォール] セクションで、クライアント IP アドレスを追加するオプションを有効にします。
- インポートするアプリケーション パッケージの JSON ファイルと VHD ファイルは、`cloudvolumes/パッケージ` の下にあるポッドのステージング ファイル共有に含まれている必要があります。Microsoft Azure Storage Explorer で適切なファイル共有に移動すると、このファイル共有の場所を確認できます。ポッドのステージング ファイル共有を特定するには、[設定] - [キャパシティ] の順に移動し、ポッドの名前をクリックして、[ファイル共有] の値にポインタを置きます。表示されるツール チップには、ステージング ファイル共有が含まれています。

  ヒント: アプリケーション パッケージのインポートに必要な JSON ファイルと VHD ファイルは、次のようになります。

  - `7Zip.json`
  - `7Zip.vhd`

  JSON および VHD ファイルには、スタンドアローン キャプチャ、App Volumes 移行ユーティリティの出力、別の Horizon Cloud ポッドのファイル共有など、複数の可能なソースが存在します。

注： ファイル共有のファイルにアクセスするには、Microsoft Azure ポータルでストレージ アカウントのファイアウォール ルールの更新が必要になる場合があります。

手順

1 コンソールで、[インベントリ] - [アプリケーション] を選択します。

[アプリケーション] ページの [App Volumes] タブが表示されます。

2 [新規] - [インポート] をクリックします。

[ネイティブ アプリケーションのインポート] ダイアログ ボックスが表示されます。

3 場所とポッドを選択し、[保存] をクリックします。

結果

- アプリケーションのインポートが開始されたことを示すメッセージが表示されます。
- インポートが完了すると、[アプリケーション] ページのリストに新しい App Volumes アプリケーションが表示されます。新しいアプリケーションを表示するには、ページの更新が必要になる場合があります。
- インポートされると、JSON データは Horizon Universal Console で更新されます。

  重要： Staging および Delivery ファイル共有から JSON または VHD ファイルを直接削除しないでください。アプリケーション パッケージを削除するには、常に Horizon Universal Console を使用します。

- [ポッド] 列に、選択したポッドが表示され、そのポッドでアプリケーションが使用可能であることが示されます。追加のポッドに対して再度インポートを実行する場合（VHD および JSON ファイルをインポートする必要がある各ポッドにコピー/転送した後）、アプリケーションは複数のポッドで使用可能になります。この場合、この列には、アプリケーションを使用できるポッドの数が表示されます。その番号にポインタを置くと、ポッドの名前が表示されます。

別のポッドからの App Volumes アプリケーション パッケージの手動複製

複数のポッドがある場合、キャプチャまたはインポートされたアプリケーション パッケージをポッド間で複製するには、次の手順を実行します。

前提条件

複製するキャプチャまたはインポートされたアプリケーション パッケージを特定します。

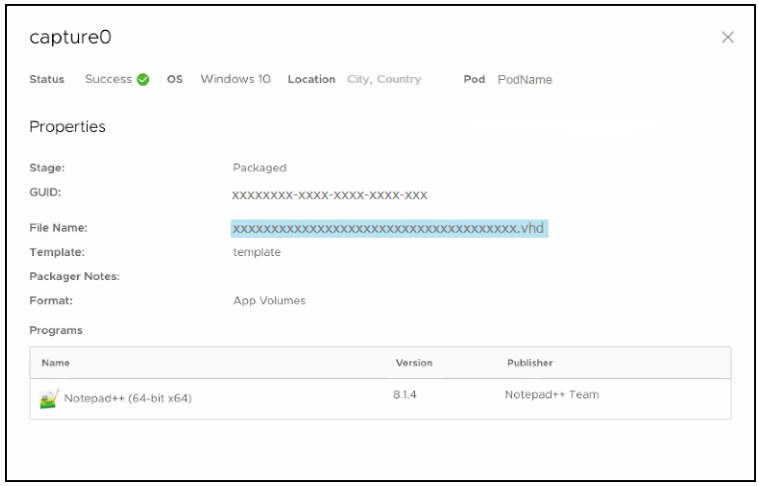
手順

1 複製するアプリケーション パッケージのファイル名を取得します。

a Horizon Universal Console で、[インベントリ] - [アプリケーション] の順に選択して、[アプリケーション] ページを開きます。

b アプリケーション パッケージのリストを表示するには、レプリケートするパッケージが存在するアプリケーションの名前をクリックします。

c [アプリケーション] ページの [ファイル名] テキストボックスからファイル名をコピーするには、アプリケーション パッケージ名をクリックします。



2 Microsoft Azure ポータルで、[アプリケーション] ページに一覧表示されているファイル名に対応するファイル（VHD および JSON）を、`cloudvolumes/packages` フォルダのソース ポッドに対応するステージング ファイル共有からコピーします。

3 コピーしたファイルを、`cloudvolumes/packages` フォルダの宛先ポッドのステージング ファイル共有にアップロードします。

Horizon Cloud：既存の App Volumes アプリケーションへの新しいアプリケーション パッケージの追加

Horizon Universal Console を使用して、アプリケーション パッケージを作成して、既存の App Volumes アプリケーションに追加できます。

手順

1 コンソールで、[インベントリ] - [アプリケーション] を選択します。

[アプリケーション] ページの [App Volumes] タブが表示されます。

2 [新規] - [作成] をクリックします。

3 [新しいアプリケーション パッケージ] ウィンドウの [定義] の下に、以下に示す値を入力します。

オプション	説明
アプリケーション	[既存] ラジオ ボタンを選択し、ドロップダウン メニューからアプリケーションを選択します。
説明	上で [既存] が選択されている場合は編集できません。
パッケージ	パッケージの一意の名前を入力します。
説明	（オプション）パッケージの説明を入力します。

4 アプリケーションのリストの下で、アプリケーションをオンデマンドで配信するか、次回のログインまたは起動時に配信するかを選択します。

- [オンデマンド] : ユーザーがパッケージのショートカットをクリックした後にのみパッケージを配信するには、このオプションを選択します。
- [ログイン時] : ログインまたは起動時にパッケージを配信するには、このオプションを選択します。これはデフォルトです。

5 [新しいアプリケーション パッケージ] ウィンドウの [アプリケーション パッケージのデスクトップ] の下に、以下に示す値を入力します。

オプション	説明
場所	[ポッド] ドロップダウン メニューに表示されるポッドのセットをフィルタする場所を選択します。
ポッド	[イメージ] ドロップダウン メニューに表示されるポッドのセットをフィルタするポッドを選択します。ドロップダウン メニューには、App Volumes が有効で、App Volumes Agent がインストールされたイメージを少なくとも 1 つ持ち、Unified Access Gateway が有効になっている[ポッド]のみが表示されます。
イメージ	イメージを選択します。[イメージ] ドロップダウン メニューには、App Volumes Agent がインストールされているイメージのみが表示されます。

6 [保存] をクリックします。

キャプチャ プロセスを初めて開始するときは、キャプチャ デスクトップ仮想マシンがアプリケーションのキャプチャに使用できるようになるまで、最大で 20 分かかります。この 20 分間に、システムがキャプチャ プロセス VDI デスクトップ割り当てと、キャプチャ デスクトップ仮想マシンに使用される 2 台のデスクトップ仮想マシンを作成しています。システムが基盤となる割り当てと仮想マシンを作成するには、最大で 20 分かかる場合があります。

- システムは、ポッドごとに 1 つのユーザー、1 つのイメージにつき割り当てを 1 つ作成します。このため、1 つまたは複数の割り当てを作成する場合があります。
- 各割り当てに 2 台のデスクトップがあるため、1 つ目の完了後に 2 つ目のキャプチャをすばやく開始できます。
- これらの割り当ては `appcaptureXXX` パターンに従って名前が付けられます。ここで、`XXX` はランダムに生成された番号になります。
- コンソールの [ブローカ] ページのテナントの構成に応じて、またその構成を反映するコンソールの動的な性質により、割り当て用のコンソールの左側のナビゲーションには、たとえば、[割り当て] - [VDI デスクト

ップとアプリ] または [割り当て] - [RDSH デスクトップとアプリ] のような [デスクトップ] と [アプリケーション] のラベルの組み合わせが表示されたり、それらの行に沿っていくつかの組み合わせが表示されたりします。[アプリケーション] ラベルが付いているコンソールのパスのタイプの場合は、これらの割り当てが表示されます。

- パッケージ プロセスに使用されるイメージを更新する場合は、更新する前にこれらの割り当てを削除する必要があります。
- 近い将来に追加のキャプチャを実行する予定がない場合は、これらの割り当てを削除して、理由もなく環境内に存在しないようにすることができます。削除した場合、次回キャプチャを実行したときに、システムは新しいものを作成するまでに最大で 20 分かかります。

注： キャプチャに失敗した場合は、[監視] - [通知] を確認して、報告されたエラーを表示できます。

これで、[アプリケーション] ページのリストにアプリケーション パッケージのエントリが作成されます。このリスト エントリの [ステータス] をポイントすると、キャプチャ仮想マシンのステータスが示されます。ステータスが `Desktop ready for application capture` の場合は、手順に従ってキャプチャ デスクトップ仮想マシンにログインし、アプリケーション パッケージのアプリケーションのインストールを開始できます。

注： キャプチャ仮想マシンがアプリケーション キャプチャの準備ができてから 6 時間以内に以下の手順を開始する必要があります。そうしないと、キャプチャ仮想マシンをアプリケーション キャプチャに使用できなくなります。また、最初の手順を実行してから 6 時間以内に以下の手順を完了する必要があります。これを行わない場合、システムは警告を表示し、30 分後にキャプチャ プロセスをキャンセルしてキャプチャ仮想マシンをシャットダウンし、アプリケーション パッケージのステータスを `Error` に変更します。`Error` 状態にあるアプリケーション パッケージを削除して、[アプリケーション] ページで、[新規] - [作成] を再度クリックすると、再試行できます。

7 [アプリケーション] ページで、アプリケーションの名前をクリックします。

アプリケーションの [アプリケーションの詳細] ページが表示されます。

8 新しいアプリケーション パッケージを選択し、[キャプチャの開始] をクリックします。

新しいブラウザ タブで、Horizon HTML Access（ブラスト）ログイン フォームが開きます。

9 この手順の開始時点でコンソールにログインするために使用したのと同じ認証情報を使用してログインします。

10 Horizon HTML Access クライアントで、キャプチャ デスクトップ仮想マシンを起動します。

注： キャプチャ仮想マシンへのログインに使用するユーザー名には、ユーザー アクセス コントロール (UAC) プロンプトを回避するためのローカル管理者権限が必要です。

Windows デスクトップに、[VMware App Volumes - パッケージの進行中] ダイアログ ボックスが、[パッケージング中...] のメッセージとともに表示されます。

重要： このダイアログ ボックスを閉じないでください。必要に応じて、アプリケーション パッケージに必要なアプリケーションのインストールが完了するまで、邪魔にならない場所に移動します。

11 アプリケーション パッケージにパッケージ化するアプリケーションをインストールします。

注： キャプチャ セッションごとに 1 つのアプリケーションのみをキャプチャすることがベスト プラクティスです。1 つのアプリケーションをインストールして、キャプチャ プロセスを終了します。アプリケーションのアプリケーション パッケージがコンソールの [アプリケーション] ページに表示されている場合は、新しいパッケージに別のアプリケーションをキャプチャできます。Horizon Cloud：既存の App Volumes アプリケーションへの新しいアプリケーション パッケージの追加を参照してください。

12 [VMware App Volumes - パッケージの進行中] ダイアログ ボックスで [OK] をクリックします。アプリケーションのインストールが終了したら、[App Volumes – パッケージの進行中] ウィンドウで OK をクリックします。次の [App Volumes –パッケージの進行中] ウィンドウが表示されます。

[VMware App Volumes - パッケージの進行中] ダイアログ ボックスに、[インストールが完了しましたか?] というメッセージが表示されます。

13 [はい] をクリックします。

[VMware App Volumes - パッケージの完了] ダイアログ ボックスが表示されます。

14 名前とバージョンに必要な変更を加え、必要に応じて説明を追加します。

15 [完了] をクリックします。

仮想マシンの再起動を求めるメッセージが表示されます。

16 [OK] をクリックして、仮想マシンの再起動を許可します。

キャプチャ デスクトップ仮想マシンが再起動すると、HTML Access クライアント セッションによって切断されたことを示すメッセージが表示されます。

17 キャプチャ デスクトップ仮想マシンがオンラインに戻ったら、再度ログインして、[パッケージ化に成功しました!]というメッセージを確認します。

18 キャプチャ デスクトップ仮想マシンからログアウトします。

結果

[アプリケーションの詳細] ページに、`Application capture in progress` のステータスで新しいアプリケーション パッケージ表示されます。アプリケーション パッケージのインポートが完了すると、ステータスは `Success` に変わります。

Horizon Cloud：App Volumes アプリケーションでのアプリケーション パッケージの管理

Horizon Universal Console 内の App Volumes アプリケーションのアプリケーション詳細ページで、アプリケーション パッケージの追加、削除、その他の変更を行えます。

重要： App Volumes アプリケーションを編集する前に、Microsoft Azure のすべてのポッドが健全な状態であることを確認します。App Volumes アプリケーションはテナントレベルのリソースであるため、変更はすべてのポッドに伝達されます。この場合、いずれかのポッドが非健全な状態になると、動作によってアプリケーションがエラー状態になる可能性があります。

App Volumes アプリケーションのアプリケーション詳細ページを表示するには、[アプリケーション] ページの [App Volumes] タブに移動し、[アプリケーション] 列でそのアプリケーションをクリックします。

次の表は、アプリケーションの詳細ページで実行できるアクションを示しています。

アクション	説明
アプリケーションへのアプリケーション パッケージの追加	1 [新規] をクリックします。 [アプリケーション パッケージの追加] ダイアログ ボックスが表示されます。[アプリケーション] と [説明] には、現在のアプリケーションの情報が事前入力されています。 2 [新しいアプリケーション パッケージ] ウィンドウの [定義] の下に、以下に示す値を入力します。 ■ [パッケージ] : パッケージの一意の名前を入力します。 ■ [説明] : (オプション) パッケージの説明を入力します。 3 アプリケーションのリストの下で、アプリケーションをオンデマンドで配信するか、次回のログインまたは起動時に配信するかを選択します。 ■ [オンデマンド] : ユーザーがパッケージのショートカットをクリックした後にのみパッケージを配信するには、このオプションを選択します。 ■ [ログイン時] : ログインまたは起動時にパッケージを配信するには、このオプションを選択します。このオプションがデフォルトになります。 4 [新しいアプリケーション パッケージ] ウィンドウの [アプリケーション パッケージのデスクトップ] の下に、以下に示す値を入力します。 ■ [場所] : [ポッド] ドロップダウン メニューに表示される一連のポッドをフィルタする場所を選択します。 ■ [ポッド] : [イメージ] ドロップダウン メニューに表示される一連のポッドをフィルタするポッドを選択します。ドロップダウン メニューには、App Volumes が有効になっており、App Volumes Agent がインストールされたイメージが少なくとも 1 つあり、Unified Access Gateway が有効になっているポッドのみが表示されます。 ■ [イメージ] : イメージを選択します。ドロップダウン メニューには、App Volumes Agent がインストールされているイメージのみが表示されます。 5 [保存] をクリックします。 新しいアプリケーション パッケージは、アプリケーションの詳細ページの一覧に表示されます。
アプリケーション パッケージのライフサイクル ステータスの変更	パッケージを作成した際には、システムによってステータスが `New` に設定され、パッケージに含めるアプリケーションのキャプチャが完了すると、システムによってステータスが `Packaged` に変更されます。 この時点から、ステータスを `Tested`、`Published`、または `Retired` に更新できるようになり、アプリケーション パッケージのインベントリを追跡する助けとなります。

アクション	説明
アプリケーション パッケージに含めるアプリケーションのキャプチャ	ステータスが New のアプリケーション パッケージがある場合は、アプリケーションをキャプチャして、そのパッケージに含めることができます。 1 新しいアプリケーション パッケージを選択し、[キャプチャの開始] をクリックします。 新しいブラウザ タブで、Horizon HTML Access（ブラスト）ログイン フォームが開きます。 2 Horizon Universal Console へのログインに使用したものと同じ認証情報を使用してログインします。 3 Horizon HTML Access クライアントで、キャプチャ デスクトップ仮想マシンを起動します。 4 コンソールへのログインに使用したのと同じ認証情報を使用して、Windows 10 または 11 オペレーティング システムにログインします。 Windows 10 または 11 デスクトップに、[VMware App Volumes - パッケージの進行中] ダイアログ ボックスが、[パッケージング中...] のメッセージとともに表示されます。 **重要：** このダイアログ ボックスを閉じないでください。必要に応じて、アプリケーション パッケージに必要なアプリケーションのインストールが完了するまで、邪魔にならない場所に移動します。 5 アプリケーション パッケージにパッケージ化するアプリケーションをインストールします。 **注：** キャプチャ セッションごとに 1 つのアプリケーションのみをキャプチャすることがベスト プラクティスです。1 つのアプリケーションをインストールして、キャプチャ プロセスを終了します。アプリケーションのアプリケーション パッケージがコンソールの [アプリケーション] ページに表示されている場合は、新しいパッケージに別のアプリケーションをキャプチャできます。Horizon Cloud：既存の App Volumes アプリケーションへの新しいアプリケーション パッケージの追加を参照してください。 6 [VMware App Volumes - パッケージの進行中] ダイアログ ボックスで [OK] をクリックします。アプリケーションのインストールが終了したら、[App Volumes – パッケージの進行中] ウィンドウで OK をクリックします。次の [App Volumes –パッケージの進行中] ウィンドウが表示されます。 [VMware App Volumes - パッケージの進行中] ダイアログ ボックスに、[インストールが完了しましたか?] というメッセージが表示されます。 7 [はい] をクリックします。 [VMware App Volumes - パッケージの完了] ダイアログ ボックスが表示されます。 8 名前とバージョンに必要な変更を加え、必要に応じて説明を追加します。[名前] に表示される値は、コンソールの [アプリケーション] ページに表示される値です。 9 [完了] をクリックします。 仮想マシンの再起動を求めるメッセージが表示されます。 10 [OK] をクリックして、仮想マシンの再起動を許可します。

アクション	説明
	キャプチャ デスクトップ仮想マシンが再起動すると、HTML Access クライアント セッションによって切断されたことを示すメッセージが表示されます。 11 キャプチャ デスクトップ仮想マシンがオンラインに戻ったら、再度ログインして、[パッケージ化に成功しました!]というメッセージを確認します。 12 キャプチャ デスクトップ仮想マシンからログアウトします。 [アプリケーションの詳細] ページに、`Application capture in progress` のステータスで新しいアプリケーション パッケージ表示されます。アプリケーション パッケージのインポートが完了すると、ステータスは `Success` に変わります。
アプリケーション パッケージの移動	アプリケーション間でパッケージを移動できます。アプリケーション間で同様のパッケージ要件が存在する場合は、移動機能を使用できます。割り当てのあるパッケージを移動すると、対応する割り当ても更新され、移動したアプリケーション パッケージが反映されます。 **注：** ■ パッケージを移動すると、デスクトップ接続のためのパッケージの実現に最大 30 分かかる場合があります。そのため、ユーザーは、パッケージがポッドで実現されるまで、デスクトップでアプリケーションを受信しない場合があります。 ■ 単一の割り当てでは、1 つのパッケージは 1 つのアプリケーションでのみサポートされます。あるアプリケーションから同じ割り当て内の別のアプリケーションにパッケージを移動すると、競合が発生し、移動されたパッケージは接続されません。 移動するパッケージに [CURRENT] のマーカーが設定されている場合は、パッケージを移動する前にマーカーの設定を解除します。アプリケーション パッケージからマーカーを削除する方法については、次の情報を参照してください。 1 [...] - [移動] を選択します。 2 ドロップダウン リストからターゲットのアプリケーションを選択します。 3 [保存] をクリックします。 移動されたアプリケーションに割り当てがあるかどうか、アプリケーションにマーカーがあるかどうか、移動が成功したかどうかによって、次の結果が発生する可能性があります。 ■ 同じページ（ソース アプリケーション ページ）の上部に成功メッセージが表示されます。 ■ ターゲット アプリケーション ページに、移動したアプリケーション パッケージが表示されます。また、パッケージに 1 つ以上の割り当てがある場合、移動の成功または失敗についてのメッセージが表示されます。 移動が成功すると、割り当てが正常に更新されたことを示す別のメッセージが表示されます。 移動が失敗すると、次に何をすべきかのメッセージが表示されます。 ■ パッケージに 1 つ以上の割り当てがある場合、影響を受ける各割り当ての割り当てページには、移動したアプリケーション パッケージが新しいアプリケーション名で表示されます。

アクション	説明
アプリケーション パッケージへのマーカーの追加	マーカーを追加するには、[マーカー] をクリックし、ドロップダウン メニューからマーカーを選択します。アプリケーション パッケージに追加するマーカーはいずれも、割り当ての作成プロセス時、そのアプリケーション パッケージに関連付けられます。詳細については、Horizon Cloud：App Volumes 割り当ての作成を参照してください。
アプリケーション パッケージからのマーカーの削除	マーカーを削除または設定解除するには、[マーカー] をクリックし、削除するマーカーの [設定解除] オプションを選択します。
アプリケーション パッケージの編集	1 [...] - [編集] をクリックします。 2 必要に応じて名前と説明を変更します。 3 アプリケーションのリストの下で、アプリケーションをオンデマンドで配信するか、次回のログインまたは起動時に配信するかを選択します。 ■ [オンデマンド]：ユーザーがパッケージのショートカットをクリックした後にのみパッケージを配信するには、このオプションを選択します。 ■ [ログイン時]：ログインまたは起動時にパッケージを配信するには、このオプションを選択します。これはデフォルトです。 4 [保存] をクリックします。 [...] - [編集] をクリックし、変更を加え、[保存] をクリックします。
アプリケーションからのアプリケーション パッケージの削除	[...] - [削除] をクリックします。 **注：** 割り当てに関連付けられているアプリケーション パッケージを削除することはできません。
アプリケーション パッケージのイメージの更新	[...] - [更新] をクリックし、変更を加え、[保存] をクリックします。

Horizon Cloud：App Volumes 割り当ての作成

コンソールの [割り当て] メニューを使用して、Horizon Cloud テナントの App Volumes 割り当てを作成します。

前提条件

App Volumes 割り当てを作成する前に、まずフローティング VDI デスクトップ割り当てを作成する必要があります。Microsoft Windows 10 および Windows 11 オペレーティング システムの処理が必要になるため、この割り当てには、少なくとも 2 基の vCPU と 4 GB の RAM を提供する VMware 推奨のデスクトップ モデルが必要です。

手順

1 コンソールで、[割り当て] をクリックし、App Volumes または VDI を含むオプションを選択します。

2 メインの割り当てページで [新規] - [App Volumes] をクリックします。

3 ウィザードの [定義] の手順で、次の値を入力します。

オプション	説明
割り当ての名前	新しい割り当ての一意の名前を入力します。
説明	（オプション）割り当ての説明を入力します。

4 [次へ] をクリックします。

5 ウィザードの [アプリケーション] の手順で、ユーザーに提供するアプリケーションを選択します。

- 表示されたアプリケーションをフィルタリングするには、[アプリケーション] 列のヘッダーにあるフィルタ アイコンをクリックして、フィルタ値を入力します。
- 選択したアプリケーションのみを表示するには、リストの右上の [選択したアプリケーション] をクリックします。

アプリケーションを選択するには、最初にチェック ボックスを選択し、[パッケージ] 列でアプリケーション パッケージを選択します。パッケージは、マーカー（「最新」など）またはパッケージの実際の名前（Notepad++ v7.7.1 など）で選択できます。

注： 最良の結果を得るには、アプリケーション パッケージがキャプチャされた OS ファミリとしてアプリケーションが割り当てられている VDI デスクトップに同じ OS ファミリ イメージを使用します。

6 [次へ] をクリックします。

7 [ユーザー] の手順で、登録済みの Active Directory ドメイン内のユーザーとグループを検索し、この割り当てからアプリケーションを使用する資格を付与するユーザーとグループを選択し、[次へ] をクリックします。

8 ウィザードの [サマリ] の手順で、表示されている情報が正しいことを確認し、[終了] をクリックします。

結果

[割り当て] ページのリストに、新しい割り当てが表示されます。

注： App Volumes 割り当てを作成または編集するときに Microsoft Azure の Horizon Cloud ポッドのいずれかがオフラインの場合、構成の変更はオンライン ポッドにのみ伝達され、割り当てには保留状態が表示されます。割り当ての [サマリ] ページに移動して、割り当てが完了していない状態を確認し、各ポッドのステータスを表示できます。問題のあるポッドがオンラインに戻ると、構成の変更がそれらのポッドに伝達され、割り当ては完了状態に達します。

問題のあるポッドが 35 分以上オフラインのままの場合、割り当てはエラー状態に切り離されます。割り当てを完了状態に戻すには、まず、問題のあるすべてのポッドがオンラインに戻るのを待ちます。次に、必要に応じて割り当てを再度編集し、構成の変更を保存します。

Horizon Cloud での App Volumes の既知の制限

このトピックでは、Horizon Cloud での App Volumes 機能に関する既知の制限について説明します。

- [割り当て] ページ（[割り当て] - [デスクトップとアプリ] または [割り当て] - [RDSH デスクトップとアプリ]）で App Volumes 割り当てを削除した場合、[インベントリ] - [アプリケーション] - [新規] - [作成] を使用して新しいアプリケーション パッケージを作成するには、アプリケーションの詳細ページでまだ「新規」ステージにある既存のアプリケーション パッケージを削除する必要があります。
- 1 つのポッドで使用可能なアプリケーション パッケージは、他のポッドに自動的に複製されることはありません。他のポッドで使用できるようにするには、そのポッドへ手動でインポートする必要があります。手順については、Horizon Cloud：既存のアプリケーション パッケージをインポートして App Volumes アプリケーションを追加を参照してください。

仮想化が無効であることを示す App Volumes エラーがデスクトップに表示される場合

フローティング VDI デスクトップが App Volumes Agent がインストールされたマルチポッド イメージに基づいている場合、App Volumes アプリケーションの使用資格を持つエンドユーザーがデスクトップにログインすると、「仮想化が無効です」という文を含むエラー メッセージが表示されます。

問題

フローティング VDI デスクトップにログインすると、「接続エラーです。App Volumes Manager に接続できません。仮想化が無効になっています」または、「マネージャのエラーです（エラー コード：400）。仮想化が無効になっています」というエラー メッセージが表示されます。

注： Horizon Cloud on Microsoft Azure 環境で使用される App Volumes は、フローティング VDI デスクトップでの使用のみがサポートされています。専用 VDI デスクトップは現在、これらの Horizon Cloud ポッドを持つ App Volumes での使用がサポートされていないため、このドキュメント ページではフローティング VDI デスクトップのシナリオについて説明します。

原因

この問題は、次のシナリオで発生します。

- テナントのフリートに複数の Horizon Cloud on Microsoft Azure ポッドがある。
- フローティング VDI デスクトップが、コンソールの [インベントリ] - [イメージ - マルチポッド] ページの公開ワークフローを介してマルチポッド イメージを使用して作成された。
- 公開ワークフローで、[Horizon Agent のインストール] トグルがオフにされた。これは、公開ワークフロー中に Image Management Service によってエージェントをインストールするオプションがオフであったことを意味します。

第 1 世代 Horizon Cloud Service では、その設計上、各ポッドに独自の App Volumes Manager IP アドレスがあります。

マルチポッド イメージの公開ワークフローでは、各宛先ポッドにコピーが公開されます。

マルチポッド イメージの各ポッドのコピーは、そのポッドの特定の App Volumes Manager IP アドレスを認識している必要があります。

各コピーが関連付けられたポッドの App Volumes Manager IP アドレスを認識するのは、Image Management Service (IMS) が Horizon Agent をインストールするときです。

[Horizon Agent のインストール] トグルが公開ワークフローに対してオンになっている場合のみ、IMS はポッドの特定の App Volumes Manager IP アドレスで各コピーを構成するように設計されたアクションを実行します。

[Horizon Agent のインストール] トグルが公開ワークフローでオフになっている場合、IMS はこれらのアクションをスキップし、その結果、すべてのコピーはポッドに固有の個々の IP アドレスではなく、同じ App Volumes Manager IP アドレスで構成されます。

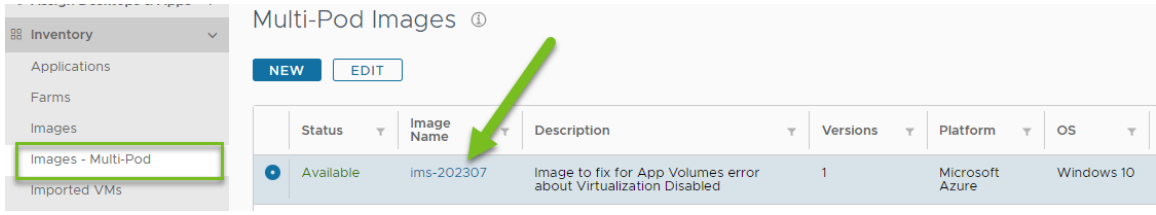
したがって、この問題が発生しないようにするには、IMS が公開ワークフローの一部としてエージェントのインストールを実行するようにします。公開ワークフローで [Horizon Agent のインストール] トグルがオンになっていることを確認します。

注： この問題は、インポートされたイメージをコンソールの [インポートされた仮想マシン] ページから [イメージ - マルチポッド] ページに移動する [マルチポッド イメージに移動] アクションを使用して公開イメージを作成し、最初のイメージ バージョンを公開して、そのイメージをデスクトップ割り当てに使用した場合にも発生します。[マルチポッド イメージに移動] アクションの使用事例では、[インポートされた仮想マシン] からのイメージにエージェントがすでにインストールされているため、コンソールでは [Horizon Agent のインストール] トグルを有効にできません。この特定のシナリオでの回避策として、以下の最初の解決策を使用してください。

解決方法

既存のデスクトップおよび公開されたマルチポッド イメージでこの問題を解決するには

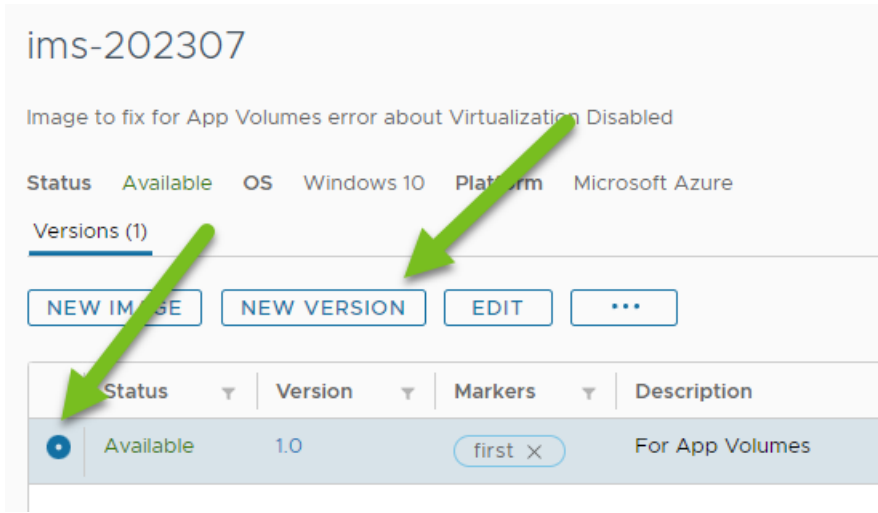
1 コンソールの [イメージ - マルチポッド] ページ（[インベントリ] - [イメージ - マルチポッド]）でイメージを見つけます。



2 イメージの名前をクリックして、[イメージ バージョン] ユーザー インターフェイス画面に移動します。

前のスクリーンショットの緑色の矢印が示すイメージの名前をクリックします。

次に、その [イメージ バージョン] 画面でラジオ ボタンをクリックして、[新しいバージョン] アクションを使用できるようにします。

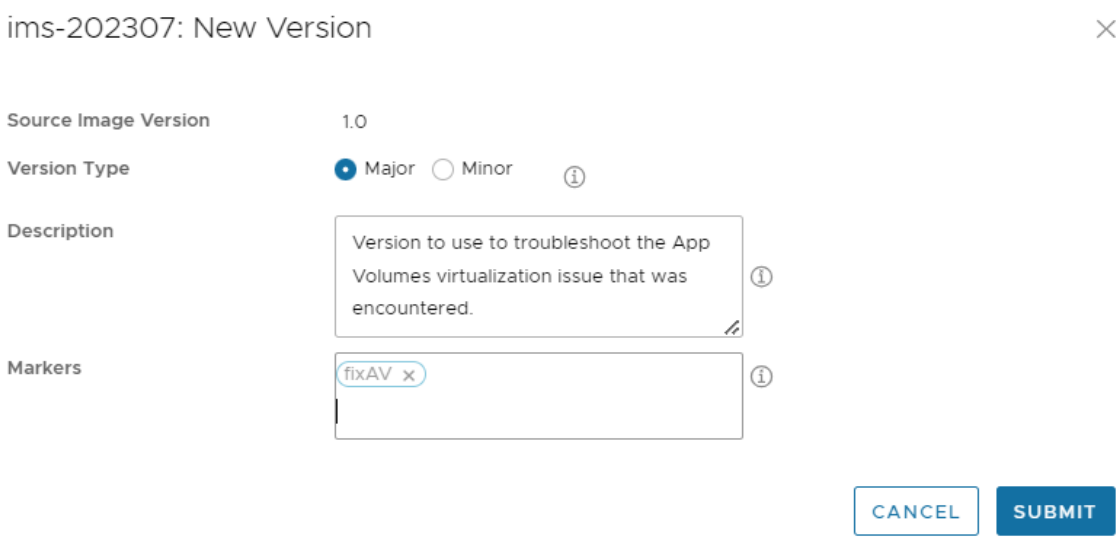


3 [新しいバージョン] をクリックして、イメージの新しいバージョンを作成します。

この新しいイメージ バージョンに Horizon Agent をインストールするオプションを使用して、この新しいバージョンを公開します。

次のスクリーンショットは、[新しいバージョン] をクリックして情報を入力した後のユーザー インターフェイスを示しています。

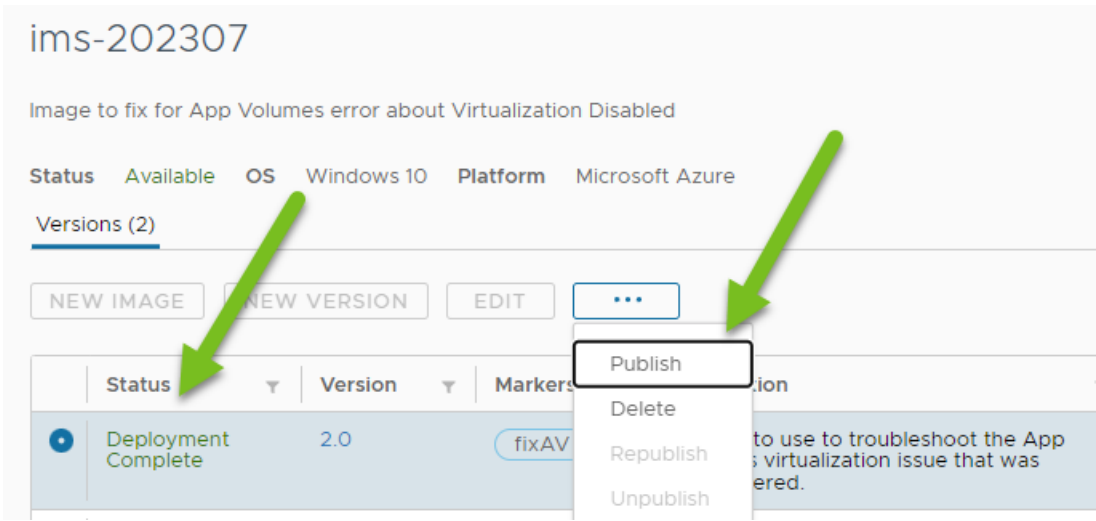
重要： マーカーを入力し、[Enter] をクリックして、マーカーが [マーカー] フィールドに表示されていることを確認してから、このウィンドウを送信します。バージョンにマーカーが存在しない場合、この新しいイメージ バージョンを使用するようにフローティング VDI デスクトップ割り当てを更新する最後の手順を正常に完了できません。



[送信] をクリックして、この新しいイメージ バージョンの作成を完了します。

システムは、新しいイメージ バージョンの基盤となる仮想マシンをデプロイします。

4 新しいイメージ バージョンが [イメージ バージョン] ページで [展開の完了] であることがユーザー インターフェイスに表示されたら、そのイメージ バージョンを選択して [公開] をクリックします。



5 [公開] ワークフローで、[Horizon Agent のインストール] オプションがオンになっていることを確認します。

注目: この新しいイメージ バージョンで [Horizon Agent のインストール] オプションをオンに切り替えるには、これらのトラブルシューティング手順を完了したときに「仮想化が無効」の問題が発生していないことが重要です。

6 次に、新しいイメージ バージョンの準備ができたら、フローティング VDI デスクトップ割り当てを更新して、そのバージョンを使用します。

新しいイメージでこの問題を回避するには

常にコンソールの [イメージ - マルチポッド] ページの [イメージのインポート] ワークフローを使用し、[Horizon Agent のインストール] をオンにして、標準のワークフローを使用してイメージを公開します。

リモート アプリケーション - Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた RDSH ファームからのインポート

Horizon Cloud で、リモート アプリケーションを RDSH アプリケーション ファームからインポートして、ユーザー割り当てに使用できるようにします。これらの手順は管理コンソールの [アプリケーション] ページを使用して実行します。複数のアプリケーション ファームを使用し、ファームによってアプリケーションが異なる場合は、エンドユーザーに割り当てるためにインベントリ内に必要な一連のアプリケーションを持つファームごとに、これらの手順を繰り返します。

システムがインベントリにインポートするリモート アプリケーションを特定するには、次の 2 つの選択肢があります。

- [ファームからの自動スキャン]：システムは、アプリケーション ファームのベースとなる仮想マシンの Windows オペレーティング システムをスキャンし、自動的にインポートできるアプリケーションを特定します。選択と確認のために、それらのアプリケーションのリストが表示されます。
- [ファームから手動で]：システムがファームの仮想マシンの Windows オペレーティング システムをスキャンする自動化された方法がベストですが、コマンド プロンプトから起動されるアプリケーションの追加や、Windows オペレーティング システムでは自動検出されないアプリケーションの追加など、特定の状況では手動による方法が役に立ちます。この方法では、一度に 1 つのアプリケーションを特定し、アプリケーションが存在する正確なパスを提供する必要があります。

ヒント: コンソールの [アプリケーション] ページに [リモート] タブが表示されている場合は、[リモート] タブで次の手順を実行します。コンソールは動的であり、Horizon Cloud テナント環境における最新の状況に適したワークフローを反映しています。Horizon Cloud テナントで App Volumes アプリケーションを使用できるようになっている場合は、[アプリケーション] ページに 2 つのタブ（[App Volumes] と [リモート]）が表示されます。

前提条件

[インベントリ] - [ファーム] に移動して、インベントリに少なくとも 1 つのアプリケーション ファームがあることを確認します。

手順

1 [新規] をクリックして、インポートするそれらのアプリケーションをシステムが特定する方法を選択します。

- [ファームからの自動スキャン]
- [ファームから手動で]

2 選択した方法に応じて、画面の指示に従います。

オプション	説明
[ファームからの自動スキャン]	この方法を選択すると、この方法のウィザードが開始されます。 a 場所、ポッド、およびアプリケーション ファームを選択し、[次へ] をクリックして次の手順に進みます。 b システムは選択されたファームからアプリケーションをスキャンして表示し、選択できるようにします。システムは、ファームの RDSH 仮想マシンに使用されている Windows オペレーティング システムでシステムの自動スキャン処理によって検出されたアプリケーションを表示します。 c アプリケーション インベントリに追加するアプリケーションを選択して、[次へ] をクリックします。 d オプションで、選択したアプリケーションの構成可能なオプションの一部をカスタマイズし、[次へ] をクリックします。 e サマリを確認し、[終了] をクリックします。
[ファームから手動で]	この方法を選択すると、インポートするアプリケーションを特定するための詳細を指定するウィンドウが開きます。 a 次の主要なプロパティを指定します。 ■ [名前] : インベントリに一覧表示されるアプリケーションの名前を指定します。名前を指定すると、コンソールに表示されるアプリケーションのリストでこのアプリケーションを特定するのに役立ちます。 ■ [表示名] : エンド ユーザーが Horizon Client や Workspace ONE などのクライアントからアプリケーションを表示して起動したときに表示されるアプリケーションの名前。 ■ [場所] : [ポッド] ドロップダウン リストに表示されるポッドのセットをフィルタする場所を選択します。この選択された場所に関連付けられているポッドのみが、次の [ポッド] リストに表示されます。 ■ [ポッド] : [ファーム] リストに表示されるファームのセットをフィルタするポッドを選択します。選択したポッドのプロビジョニングされたファームのみが、次の [ファーム] リストに表示されます。 ■ [ファーム] : 追加するアプリケーションが含まれる RDSH 仮想マシンを持つファームを選択します。 ■ [アプリケーション パス] : RDSH 仮想マシンのオペレーティング システム内のアプリケーションへのパスを指定します。 ■ [アイコン ファイル] : オプションで、アプリケーションのアイコンとして使用する PNG ファイル（32 x 32 ピクセル）をアップロードします。 b [詳細プロパティ] セクションで、以下のオプション設定を指定します。 ■ [ファームで利用可能なアプリケーション] : システムがアプリケーションのパスを検証するようにするには [はい] を選択します。アプリケーションがそのパスのファームの仮想マシンに存在しない場合は、[いいえ] を選択して、システムがアプリケーションを検索しないようにします。たとえば、アプリケーションが仮想マシンのローカル ディレクトリに格納されている場合は、[いいえ] を選択して、システムがその場所のアプリケーションを検索しないようにします。 ■ [バージョン] : アプリケーションのバージョン番号 ■ [公開者] : アプリケーションの公開者 ■ [開始フォルダ] : RDSH 仮想マシンの Windows オペレーティング システム内で、リモート アプリケーションがその開始フォルダとして使用する場所を指定します。 **注：** [アプリケーション パス] に独自の開始ディレクトリを指定する LNK ファイルを指定すると、システムはここで指定した場所を使用しません。

オプション	説明
	■ [パラメータ]：リモート アプリケーションを起動するときに使用するコマンドライン パラメータを指定します。 c [送信] をクリックします。

結果

システムは、指定したアプリケーションをインベントリのアプリケーション カタログに追加します。

次のステップ

上記の手順を繰り返して、他のファームから必要なアプリケーションをインポートします。

リモート アプリケーション - Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされたリモート アプリケーションのリモート アプリケーション割り当ての作成

Horizon Cloud では、エンド ユーザーが Microsoft Azure のポッドにある RDSH ファームからプロビジョニングされたリモート アプリケーションにアクセスして使用できるようにするために、リモート アプリケーションの割り当てを作成します。このリリースでは、リモート アプリケーションは Microsoft Azure のポッドによってプロビジョニングされたアプリケーション ファームから提供されます。

前提条件

[アプリケーション] ページを使用して、エンド ユーザーに資格を付与するリモート アプリケーションがインベントリで使用可能であることを確認します。例については、リモート アプリケーション - Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた RDSH ファームからのインポートを参照してください。

手順

1 管理コンソールで、[割り当て] をクリックして、Microsoft Azure のポッドからプロビジョニングされた RDSH ベースのアプリケーション（リモート アプリケーションとも呼ばれる）の割り当てを作成するためのページに移動します。

ヒント: コンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。コンソールの割り当て関連ページに表示されるラベルは、テナントの設定済みのブローカ設定、フリート内のクラウド接続されたポッドのタイプ、テナントの地域別クラウド プレーン、および特定のライセンスに基づく機能などの要因によって異なります。

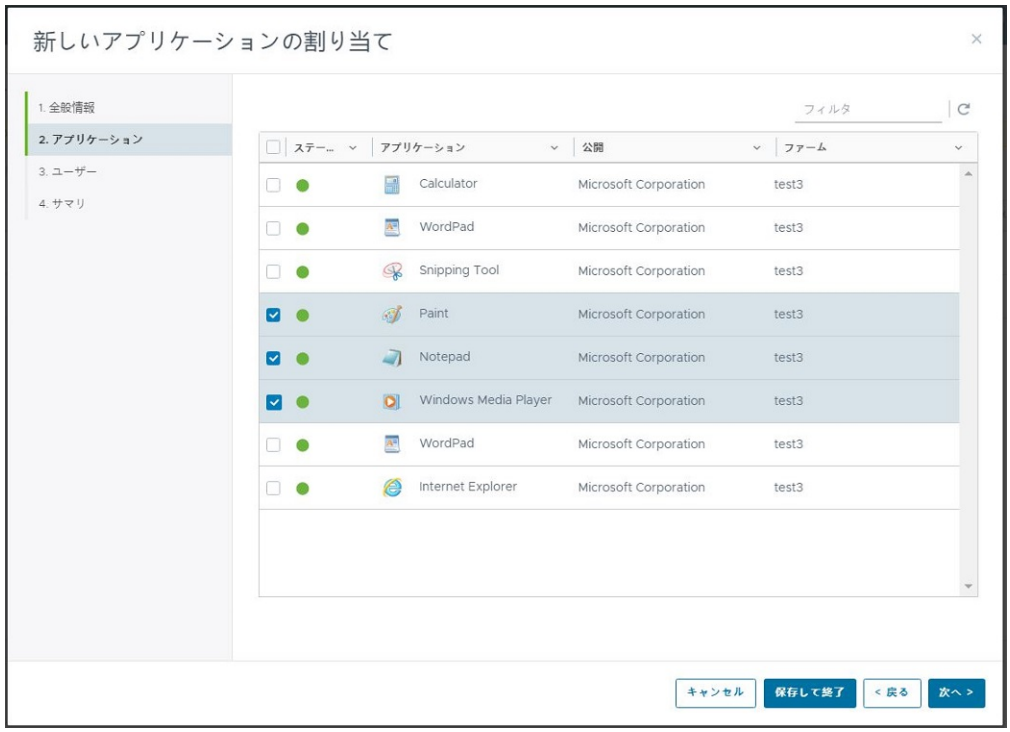
2 そのページで、[新規] をクリックします。

3 [新しい割り当て] の開始画面で、[アプリケーション] アイコンをクリックします。

4 ウィザードの [定義] の手順で場所とポッドを選択し、この割り当ての名前を指定して [次へ] をクリックします。

5 [アプリケーション] の手順でリモート アプリケーションを選択し、[次へ] をクリックします。

注： 表示されたアプリケーションは、すべて同じ Horizon Cloud ポッド内のファームから Horizon Cloud アプリケーション カタログにインポートされたアプリケーションです。割り当て内の同じポッドにある別のファームのアプリケーションも使用できます。



6 [ユーザー] の手順でこの割り当てのユーザーおよびグループを検索して選択し、[次へ] をクリックします。

7 [サマリ] の手順で情報を確認し、[送信] をクリックします。

結果

システムは割り当てを作成し、[割り当て] ページに一覧表示します。

Microsoft Azure の Horizon Cloud ポッドに基づくテナントのデスクトップ割り当ての概要

この記事では、テナントのポッド フリートにある Horizon Cloud ポッドのリソースを使用してテナントで作成できるデスクトップ割り当てのタイプについて簡単に説明します。割り当ては、Horizon Universal Console 内の概念的なエンティティです。コンソールを使用して行うデスクトップの割り当ては、エンド ユーザーの仮想デスクトップのプールを定義し、それらの使用資格をエンド ユーザーに付与する方法です。

Microsoft Azure 環境の Horizon Cloud ポッドは、次のタイプのデスクトップ割り当てを提供します。

セッション デスクトップ割り当て

セッション デスクトップ割り当てでは、リモート デスクトップ サービス (RDS) のデスクトップ エクスペリエンスが複数ユーザー間で共有されます。これらのデスクトップは、ポッドの RDSH ファームで実行している RDSH 対応仮想マシンへのセッションベースの接続です。RDSH セッション デスクトップ割り当てを作成する前に、公開されたイメージに基づいて作成されたデスクトップ ファームを少なくとも 1 つ用意する必要があります。第 1 世代 Horizon Cloud ポッド - ファームの作成と管理を参照してください。

専用の VDI デスクトップ割り当て

専用の VDI デスクトップ割り当てでは、各仮想デスクトップが特定のユーザーにマッピングされます。マッピングされた各ユーザーは、ログインするたびに同じデスクトップに戻ります。特定の専用の VDI デスクトップが特定のユーザーにマッピングされると、そのデスクトップはそのユーザーに割り当てられたということになります。特定の専用の VDI デスクトップは、次の 2 つの方法のいずれかで特定のユーザーにマッピングされます。

- 管理者は、[割り当て] アクションを使用して、特定のユーザーに特定のデスクトップを明示的に割り当てます。
- ユーザーは、([ユーザー] タブの）割り当てに対する資格が付与されていて、割り当てからデスクトップの最初の起動を行います。その時点では、そのユーザーは、割り当てによって定義されたすべての専用の VDI デスクトップのセットから、該当する専用の VDI デスクトップに対する資格を獲得したことになります。ユーザーがこのような方法で専用の VDI デスクトップの資格を獲得した場合、システムによってその特定のデスクトップが特定のユーザーにマッピングされ、専用の VDI デスクトップは [割り当て済み] 状態になります。その特定の専用の VDI デスクトップは、管理者が明示的に （[割り当て解除] アクションを使用して）デスクトップの割り当てを解除するまで、または、該当するユーザーの Active Directory アカウントが資格のあるユーザーの割り当てのセットから削除されるまで、[割り当て済み] 状態のままになります。

専用割り当てでは、デスクトップとユーザーの関係が 1 対 1 になる必要があり、ユーザーの総数を基準にしてサイジングする必要があります。たとえば、100 ユーザーのグループについては 100 台のデスクトップの割り当てが必要となります。このような専用デスクトップ割り当ての主な使用例は、各ユーザーのデスクトップ仮想マシンのホスト名がセッション間でそのまま確実に残るようにすることです。特定のソフトウェア パッケージでは、ライセンス上、専用デスクトップを使用することが必要となる場合があります。

フローティング VDI デスクトップ割り当て

フローティング VDI デスクトップ割り当てでは、ユーザーはログインするたびにマシン名が異なる別の仮想マシンを受け取ります。フローティング デスクトップ割り当てでは、ユーザーのシフトに合わせてデスクトップを作成できます。この場合、同時実行ユーザーの最大数を基準としてサイジングする必要があります。たとえば、ユーザーがシフトして作業しており、1 度に 100 ユーザーが作業している場合は、300 ユーザーが 100 台のデ

スクトップ割り当てを使用できます。フローティング デスクトップ割り当てでは、ユーザーに各デスクトップ セッションで異なるホスト名が表示される場合があります。

専用 VDI デスクトップ割り当てとフローティング VDI デスクトップ割り当てのどちらかを選択する場合は、フローティング VDI デスクトップ割り当てがベスト プラクティスです。理由は、専用 VDI デスクトップ割り当てよりも柔軟性の高いプール管理機能を備え、仮想マシン リソースが各ユーザー専用になることを回避できるためです。その結果、フローティング VDI デスクトップ割り当ては、通常、専用 VDI デスクトップ割り当てよりも低コストになります。

デスクトップの割り当てを作成するには、エンドユーザーのデスクトップの基礎となる設定済みオペレーティング システムとしてシステムが使用する、1 つ以上の公開状態のイメージ仮想マシンが存在する必要があります。

注： セッション ベースのデスクトップまたはフローティング VDI デスクトップのどちらも、ユーザー データ、設定、プロファイルの永続性を提供しません。ユーザーがフローティング VDI デスクトップからログオフすると、そのフローティング VDI デスクトップはユーザーがログインする前の状態にリセットされます。VMware Dynamic Environment Manager を設定し、ご使用の環境に応じてそれを構成することによって、ユーザー データ、設定、およびプロファイルの永続性を提供することができます。自動化された [デスクトップのインポート] ウィザードを使用して作成されたイメージには、デフォルトで VMware Dynamic Environment Manager エージェントがインストールされています。これらの項目の永続性の構成については、次のリソースを参照してください。

- http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-user-environment-manager-deployment-considerations.pdf にある『VMware User Environment Manager Deployment Considerations』ドキュメント。VMware User Environment Manager™ は以前の名前です。
- Dynamic Environment Manager の製品ドキュメント。

これらのデスクトップ割り当ての作成について

デスクトップ割り当ての作成ワークフローは、テナントの Horizon Cloud ポッドの現在のブローカ構成によって異なります。この構成を表示するには、コンソールで [設定] - [ブローカ] に移動します。

[ブローカ] ページに Universal Broker が示されている

VDI デスクトップの場合は、Microsoft Azure の Horizon Cloud ポッド - 第 1 世代環境での VDI マルチクラウド割り当ての作成と表示で説明されているワークフローを実行します。

セッションベースのデスクトップの場合は、Horizon Cloud ポッド - RDS ベースのセッション デスクトップ割り当てを作成して、エンド ユーザーのために RDS ホストからのデスクトップ セッションを提供するで説明されているワークフローを実行します。

[ブローカ] ページにシングルポッド ブローカが示されている

VDI デスクトップの場合は、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および 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で説明されているワークフローを実行します。

セッションベースのデスクトップの場合は、Horizon Cloud ポッド - RDS ベースのセッション デスクトップ割り当てを作成して、エンド ユーザーのために RDS ホストからのデスクトップ セッションを提供するで説明されているワークフローを実行します。

Horizon Cloud Service on Microsoft Azure を使用した Carbon Black Cloud のデプロイ

Horizon Cloud Service on Microsoft Azure VDI デスクトップ割り当ておよびファームを使用して VMware Carbon Black Cloud をデプロイする方法については、VMware ナレッジベースの記事 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。

Horizon Cloud ポッド - RDS ベースのセッション デスクトップ割り当てを作成して、エンド ユーザーのために RDS ホストからのデスクトップ セッションを提供する

Horizon Cloud では、セッション デスクトップ割り当てと呼ばれるものを作成して、エンド ユーザーにマルチセッション オペレーティング システムへのアクセスを提供します。セッション デスクトップ割り当てを作成した後、指定したエンド ユーザーはファームの RDS ホストから同時にデスクトップ セッションを取得できます。Microsoft Azure の Horizon Cloud ポッドの場合、ファーム ホストは、Windows Server オペレーティング システムを実行している仮想マシン、あるいは Windows 10 または 11 Enterprise マルチセッション オペレーティング システムを実行している仮想マシンです。

Horizon Cloud でのデスクトップ割り当ての全般的な情報については、Microsoft Azure の Horizon Cloud ポッドに基づくテナントのデスクトップ割り当ての概要を参照してください。Horizon オンプレミス製品に精通している場合、このタイプのセッション デスクトップはその製品ドキュメントで公開デスクトップと呼ばれます。

前提条件

以下の項目を確認します。

- デプロイによっては、ブローカを設定しないとポッドに関連する割り当てを作成できないというメッセージが、コンソールの割り当て関連ページに表示されることがあります。このメッセージが表示された場合は、画面上の手順を実行します。
- [ファーム] ページにはリモート デスクトップ タイプのファームが少なくとも 1 つ表示され、そのファームはセッション デスクトップに使用する公開イメージに基づきます。セッション デスクトップの割り当てに使用できるのは、リモート デスクトップを提供するように構成されたファームのみです。
- ファームがまだ割り当てに使用されていない。リモート デスクトップを提供するように構成されたファームを複数のセッション デスクトップ割り当てに使用することはできません。使用したいファームがセッション デスクトップ割り当てで既に使用されているかどうかを確認するには、セッションベースのデスクトップ割り当てが一覧表示されているコンソール ページで、[ファーム] 列を確認します。使用したいファームが一覧にある場合は既にセッション デスクトップ割り当てに使用されているため、新しいファームを作成する必要があります。

手順

1 割り当て関連のコンソール ページに移動して、RDSH デスクトップ割り当てが作成されていることを確認し、[新規] をクリックしてワークフローを開始します。

ヒント: コンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。コンソールの割り当て関連ページに表示されるラベルは、テナントの設定済みのブローカ設定、フリート内のクラウド接続されたポッドのタイプ、テナントの地域別クラウド プレーン、および特定のライセンスに基づく機能などの要因によって異なります。

2 表示される画面で、[デスクトップ] アイコンをクリックします。

[新しいデスクトップ割り当て] ウィンドウが開き、最初のウィザードの手順が表示されます。

3 [セッション] タイプを選択します。

4 選択を行い、次の手順に進みます。

オプション	説明
場所	セッション デスクトップを提供するポッドの場所を選択します。
ポッド	ポッドを選択します。 **ヒント:** 選択するポッドが表示されない場合は、[場所] リストにポッドがない場所が表示されていないことを確認します。[場所] フィールドは [ポッド] リストに表示され、選択した場所に関連付けられていないポッドを除外します。すでに場所にポッドがあり、そのポッドを削除するか別の場所に移動して、表示された場所にポッドが存在しなくなると、[ポッド] リストにはエントリが表示されなくなります。場所はアルファベット順に表示されているため、画面を開くと、アルファベット順で最初の場所が自動的に選択されます。その場所にポッドが関連付けられていない場合は、場所を別のエントリに切り替える必要があります。
ファーム	デスクトップ セッションのソースとなることを希望する、ホスト仮想マシンを持つファームを選択します。 選択されたポッドにあり、既存のセッション デスクトップ割り当てにまだ含まれていないファームのみを選択できます。
割り当ての名前	この割り当てにわかりやすい名前を入力します。エンド ユーザーが自分に割り当てられたデスクトップにアクセスするときにこの名前が表示されます。たとえば、エンド ユーザーが Horizon Client を起動して割り当てられたデスクトップに移動すると、この名前は Horizon Client に表示されます。 名前には文字、ハイフン、数字のみを含める必要があります。スペースは使用できません。名前を英字以外の文字で始めることはできません。

5 登録済みの Active Directory ドメイン内のユーザーとグループを検索し、この割り当てを使用してデスクトップ セッションにアクセスするユーザーとグループを選択して、次の手順に進みます。

6 構成を確認し、ウィザードを完了します。

結果

システムは、ファームの仮想マシンを構成するプロセスを開始し、選択したユーザーにセッション デスクトップを提供します。割り当てが一覧表示されているページでは、[ステータス] 列に現在の進行状況が反映されます。

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

Horizon Cloud では、デスクトップ割り当てを作成して、仮想デスクトップをエンド ユーザーにプロビジョニングします。Horizon Universal Console の [割り当て] 領域を使用してフローティング VDI デスクトップ割り当てを作成します。Horizon Cloud テナントが Microsoft Azure のポッドでシングルポッド タイプの仲介を使用するように構成されている場合、ここの手順に従って、シングル ポッドから仮想デスクトップを仲介するデスクトップ割り当てを作成します。

注： テナントが Microsoft Azure のポッドで Universal Broker を使用するように構成されている場合は、ここで説明する手順に従うのではなく、マルチクラウド割り当てという、同じ割り当て内にある複数のポッドからリソースをプロビジョニングできるものを構成します。Microsoft Azure の Horizon Cloud ポッド - 第 1 世代環境での VDI マルチクラウド割り当ての作成と表示を参照してください。

デスクトップ割り当ての全般的な情報については、Microsoft Azure の Horizon Cloud ポッドに基づくテナントのデスクトップ割り当ての概要を参照してください。

次の手順を使用して、エンド ユーザーにフローティング VDI デスクトップを割り当てます。別のタイプのデスクトップを割り当てる方法については、Microsoft Azure の Horizon Cloud ポッドに基づくテナントのデスクトップ割り当ての概要に記載されているサブトピックを参照してください。

前提条件

- デプロイによっては、ブローカを設定しないとポッドに関連する割り当てを作成できないというメッセージが、コンソールの割り当て関連ページに表示されることがあります。このメッセージが表示された場合は、画面上の手順を実行します。
- Microsoft Windows クライアント オペレーティング システムを持つ少なくとも 1 つの公開イメージがあることを確認します。このようなイメージがない場合、VDI デスクトップ割り当てを作成することはできません。確認するには、[イメージ] ページに移動し、該当するイメージが一覧表示されているかを確認します。公開イメージの作成手順については、構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の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。

  注： テナントがシングル ポッド ブローカ用に構成されている場合、フローティング VDI デスクトップ割り当てにマルチポッド イメージを使用することはサポートされていません。次の手順で説明するユーザー インターフェイスを使用すると、[イメージ] リストにこのようなマルチポッド イメージは表示されません。それらはこのユースケースではサポートされていないためです。

- デスクトップに暗号化されたディスクを使用するかどうかを決定します。VDI デスクトップ割り当てを作成するときに、ディスクの暗号化を指定する必要があります。割り当ての作成後にディスクの暗号化を追加することはできません。ディスク機能の説明については、Horizon Cloud 環境のファームおよび VDI デスクトップでの Microsoft Azure ディスク暗号化の使用を参照してください。

  重要： このリリースでは、データ ディスクが接続されたイメージ仮想マシンを使用するフローティング VDI 割り当てのディスク暗号化をサポートしていません。割り当てで使用する予定のイメージにデータ ディスクがないことを確認してください。

- デスクトップ仮想マシンで NSX Cloud 機能を使用できるようにするかどうかを決定します。VDI デスクトップ割り当てを作成するときは、NSX Cloud 管理を有効にする必要があります。NSX Cloud 管理の割り当ては、作成後に有効にすることはできません。この割り当て用に選択する公開済みイメージには、NSX エージェントがインストールされていることが必要です。イメージの公開前に NSX Agent をインストールする必要があります。Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッド とそのサブトピックを参照してください。

  重要： NSX Cloud の機能とディスク暗号化の両方を使用するには、イメージにインストールされている NSX エージェントが最新のエージェント バージョンであることを確認します。以前のバージョンの NSX エージェントでディスク暗号化を使用することはサポートされていません。

- この割り当てのデスクトップ仮想マシンをポッドのプライマリ仮想マシン サブネット（テナント サブネットともいいます）とは異なる仮想マシン サブネットに接続するかどうかを決定します。ポッドでマニフェスト 2298 以降が実行されていて、仮想マシン サブネットをさらに追加するためにポッドを編集してある場合は、そのサブネットをこのデスクトップ割り当てに使用するよう指定できます。このユースケースでは、使用する仮想マシン サブネットが `Ready` の状態でポッドの詳細ページの [ネットワーク] セクションに表示されていることを確認する必要があります。これにより、そのサブネットがワークフローの手順で選択できるようになります。詳細については、ファーム用および VDI 割り当て用 Horizon Cloud ポッドでの複数のテナント サブネットの使用の概要 を参照してください。

手順

1 割り当て関連のコンソール ページに移動して、VDI デスクトップ割り当ての作成先を探し、新しい割り当てワークフローを開始します。

  ヒント: コンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。コンソールの割り当て関連ページに表示されるラベルは、テナントの設定済みのブローカ設定、フリート内のクラウド接続されたポッドのタイプ、テナントの地域別クラウド プレーン、および特定のライセンスに基づく機能などの要因によって異なります。

2 [新しい割り当て] の開始画面で、[デスクトップ] アイコンをクリックします。

[新しいデスクトップ割り当て] ウィンドウが開き、最初のウィザードの手順が表示されます。

3 [フローティング] を選択します。

4 [定義] の手順での選択を完了し、[次へ] をクリックします。

注： 必要に応じてスクロール バーを使用し、すべての内容を表示します。

オプション	説明
場所	デスクトップを提供するポッドの場所を選択します。
ポッド	ポッドを選択します。 **ヒント:** 選択するポッドが表示されない場合は、[場所] リストにポッドがない場所が表示されていないことを確認します。[場所] フィールドは [ポッド] リストに表示され、選択した場所に関連付けられていないポッドを除外します。すでに場所にポッドがあり、そのポッドを削除するか別の場所に移動して、表示された場所にポッドが存在しなくなると、[ポッド] リストにはエントリが表示されなくなります。場所はアルファベット順に表示されているため、画面を開くと、アルファベット順で最初の場所が自動的に選択されます。その場所にポッドが関連付けられていない場合は、場所を別のエントリに切り替える必要があります。
仮想マシン サブネットの指定	このトグルを有効にすると、割り当てのデスクトップ仮想マシンの接続先とする特定のサブネットを 1 つ以上選択できます。トグルを有効にしたら、表示される一覧から特定のサブネットを選択できます。 このトグルがオフに切り替えられている場合、割り当てのデスクトップ仮想マシンはデフォルトでポッドのプライマリ仮想マシン サブネットに接続されます。

オプション	説明
モデルのフィルタリング	1 つ以上のフィルタを設定して、[モデル] ドロップダウン メニューで使用できるモデルを制御します。モデルは、タイプ、シリーズ、CPU の数、メモリ、およびタグでフィルタできます。モデルの選択の詳細については、Horizon Universal Console でのファームと割り当ての仮想マシン タイプとサイズの管理を参照してください。ここでは、[仮想マシンのタイプとサイズ] ページ（[設定] - [仮想マシンのタイプとサイズ]）のオプションについて説明しています。  フィルタを設定するには、まずドロップダウン メニューで条件を選択し、次に目的の値を入力します。デフォルトでは、条件が「タグ」、値が「VMware 推奨」の単一のフィルタがあります。この最初のフィルタを編集し、And および Or 演算子によって接続されたフィルタをさらに追加できます。 次に、フィルタに使用できる基準と、それぞれに入力できる値の説明を示します。 **[タイプ]**  このオプションを選択すると、2 番目のドロップダウン メニューはデフォルトで [GPU と高パフォーマンス - GPU を使用するモデル] に設定されます。 **注：** GPU モデルを選択した場合、表示されるイメージのリストには「GPU を含める」フラグを選択して作成されたイメージのみが含まれるため、GPU モデルを使用してファームまたはプールを作成するにはそのようなイメージが少なくとも 1 つ必要です。GPU 以外のモデルを選択した場合、表示されるイメージのリストには、「GPU を含める」フラグなしで作成されたイメージのみが含まれます。 **[シリーズ]**  このオプションを選択すると、2 番目のドロップダウン メニューから一連のモデルを選択できます。リストの一番上にある [フィルタ] テキスト ボックスにテキストを入力してこのリストをフィルタリングすることもできます。 **[CPU の数]**  このオプションを選択すると、CPU 範囲を入力できます。 **重要：** 本番環境では、予期しないエンドユーザー接続の問題を回避するために、2 個以上の CPU を持つ仮想マシン モデルを使用します。 **[メモリ]** 

オプション	説明
	このオプションを選択すると、メモリ範囲（GB 単位）を入力できます。 **[タグ]**  このオプションを選択すると、2 番目のドロップダウン メニューからタグを選択できます。リストの一番上にある [フィルタ] テキスト ボックスにテキストを入力してこのリストをフィルタリングすることもできます。ドロップダウン メニューで使用可能なタグは、ハードコードされたシステム タグと、[仮想マシンのタイプとサイズ] ページ ([設定] - [仮想マシンのタイプとサイズ]) で作成したカスタム タグの両方です。 フィルタごとに次の手順を実行して、追加フィルタを設定できます。 a [追加] リンクをクリックします。 b 前のフィルタと作成中の新しいフィルタの間の演算子として And または Or を選択します。 c 新しいフィルタを設定するには、条件を選択して値を入力します。
モデル	デスクトップ インスタンスに使用するモデルを選択します。この選択では、デスクトップ インスタンスが作成されるときに使用される基盤となるリソースのセットを、キャパシティ（コンピューティング、ストレージなど）の観点から定義します。使用可能な選択肢は、Microsoft Azure で使用可能な標準の仮想マシン サイズにマッピングされます。 **重要：** 本番環境の場合は、2 個以上の CPU が搭載された仮想マシン モデルを選択します。第 1 世代の Horizon Cloud スケール テストでは、2 個以上の CPU を使用すると、予期しないエンド ユーザー接続の問題を回避す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、このようなモデルはテスト用または事前検証用にのみ使用する必要があります。
ディスク タイプ	利用可能なオプションからサポートされているディスク タイプを選択します。ディスク タイプのオプションは、選択したモデル、および Azure サブスクリプションとリージョンに基づいています。一般的に使用可能なディスク タイプは次のとおりです。 ■ 標準 HDD - デフォルトのディスク タイプ。 ■ 標準 SSD ■ プレミアム SSD - このオプションは、プレミアム I/O をサポートするモデルを選択した場合にのみ表示されます。 必要に応じて、割り当てを作成した後に選択内容を編集できます。
ディスク サイズ	この割り当ての仮想マシンの OS ディスク サイズを GB 単位で入力します。 ■ デフォルト値は、基本イメージの OS ディスク サイズ（通常は 128 GB）です。 ■ サイズを編集する場合、入力する値は基本イメージの OS ディスク サイズよりも大きくなければなりません。また、選択したモデルでサポートされる最大サイズ（通常は 1024 GB）を超えることはできません。 ■ この値は、必要に応じて後で編集することもできます。 **重要：** ディスク サイズを編集する場合は、仮想マシンが予期したとおりに作成されるように、追加のアクションを実行する必要があります。詳細については、ファームまたは VDI デスクトップ割り当てのディスク サイズが増加した場合に必要な管理者のアクションを参照してください。
ドメイン	お使いの環境に登録されている Active Directory ドメインを選択します。

オプション	説明
ドメインへの参加	[はい] を選択し、デスクトップ インスタンスが作成後に自動的にドメインに参加されるようにします。
ディスクの暗号化	デスクトップ インスタンスが暗号化されたディスクを持つようにするため [はい] を選択します。 **重要：** ■ ディスクを暗号化する場合は、VDI デスクトップ割り当てを作成するときにこの選択を行う必要があります。割り当ての作成後にディスクの暗号化を追加することはできません。 ■ NSX Cloud の機能とディスク暗号化の両方を使用するには、イメージにインストールされている NSX エージェントが最新のエージェント バージョンである必要があります。以前のバージョンの NSX エージェントでディスク暗号化を使用することはサポートされていません。
NSX Cloud 管理	割り当てのデスクトップ インスタンスを持つ NSX Cloud の機能を使用できるように、[はい] を選択します。Microsoft Azure のデスクトップでの NSX Cloud 機能の使用については、Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッドおよびそのサブトピックを参照してください。 **重要：** ■ デスクトップ インスタンスを持つ NSX Cloud を使用する場合、VDI デスクトップ割り当ての作成時にこの選択を行う必要があります。NSX Cloud 管理は、割り当て作成後に有効にすることはできません。 ■ 割り当てのデスクトップ インスタンスで NSX Cloud 管理機能を使用するには、この割り当て用に選択したイメージに NSX エージェントがインストールされている必要があります。この設定を [はい] に切り替えるときは、[イメージ] で選択したイメージに NSX Agent がインストールされている必要があります。システムは、VDI デスクトップ割り当てを作成するときに、選択したイメージに NSX エージェントがあるかどうかを検証しません。 ■ NSX Cloud の機能とディスク暗号化の両方を使用するには、イメージにインストールされている NSX エージェントが最新のエージェント バージョンである必要があります。以前のバージョンの NSX エージェントでディスク暗号化を使用することはサポートされていません。

オプション	説明
イメージ	エンド ユーザーに割り当てるイメージを選択します。 選択したポッドの公開イメージのうち、VDI デスクトップに適しているものだけがここに一覧表示されます。公開イメージは、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も呼ばれ、基本イメージまたはゴールド イメージをデスクトップに変換してシステムに公開したものです。 **重要：** ■ [ディスクを暗号化] を [はい] に設定する場合、ここで選択したイメージにデータ ディスクが接続されていないことを確認してください。フローティング VDI 割り当てにデータ ディスクを使用した仮想マシンのディスク暗号化の使用は、このリリースではサポートされていません。 ■ [NSX Cloud 管理] を [はい] に設定する場合は、ここで選択したイメージに NSX Agent がインストールされていることを確認します。割り当てのデスクトップ インスタンスで NSX Cloud 管理機能を使用するには、この割り当て用に選択したイメージに NSX エージェントがインストールされている必要があります。システムは、VDI デスクトップ割り当てを作成するときに、選択したイメージに NSX エージェントがあるかどうかを検証しません。 ■ テナントがシングル ポッド ブローカ用に構成されている場合、[イメージ] にはマルチポッド イメージが一覧表示されません。そのようなイメージはこのユースケースではサポートされていないためです。
割り当ての名前	このフローティング VDI デスクトップ割り当てのわかりやすい名前を入力します。資格のあるエンド ユーザーが、クライアントでデスクトップにアクセスする際に、この形式の割り当ての名前が表示されます。 名前には文字、ハイフン、数字のみを含める必要があります。スペースは使用できません。名前を英字以外の文字で始めることはできません。
仮想マシン名	この割り当てで作成されたデスクトップ仮想マシンの基底名。仮想マシン名はこの基底名に数値を加えたもの、たとえば、win10-1、win10-2 などになります。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。この名前は、エンド ユーザーがこの割り当てからデスクトップにアクセスするときに表示されます。たとえば、エンド ユーザーが Horizon Client を起動してデスクトップの 1 つを使用すると、この名前は Horizon Client に表示されます。
既定のプロトコル	エンド ユーザー セッションで使用するデフォルトの表示プロトコルを選択します。 デフォルトのプロトコルではなく、別のプロトコルが使用される状況が発生する場合があります。たとえば、クライアント デバイスがデフォルトのプロトコルをサポートしない場合や、エンド ユーザーが、選択されているデフォルト プロトコルよりも他のプロトコルを優先して使用する場合があります。 **注：** Microsoft Windows 7 Enterprise オペレーティング システムのイメージの場合、サポートされている選択肢は RDP のみです。
優先クライアント タイプ	エンド ユーザーが Workspace™ ONE™ Access からデスクトップを起動するときに使用する優先クライアント タイプを選択します。これは Horizon Client、または HTML Access 用のブラウザのいずれかになります。 **注：** Microsoft Windows 7 Enterprise オペレーティング システムのイメージの場合、サポートされている選択肢は Horizon Client のみです。

オプション	説明
デスクトップの最小数 **デスクトップの最大数**	このフローティング VDI デスクトップ割り当てに含めるデスクトップの最小数と最大数を指定します。割り当てが最初に作成されると、システムは [デスクトップの最大数] フィールドで指定された数のデスクトップを展開し、次に [デスクトップの最小数] で指定された数以外のデスクトップをパワーオフします。 最小数のデスクトップ インスタンスのみが最初にパワーオンされます。エンド ユーザーの要求が増加すると、システムは [デスクトップの最大数] の設定を上限として追加のデスクトップをパワーオンします。その後、エンド ユーザーの要求が減少すると、システムは [デスクトップの最小数] の設定を下限としてデスクトップをパワーオフします。システムによってデスクトップがパワーオフされる前に、デスクトップからログイン済みユーザー セッションがなくなっている必要があります。 [デスクトップの最小数] にゼロ (0) を指定すると、デスクトップに対するエンド ユーザーからの要求が発生するまで、システムは割り当てのすべてのデスクトップをパワーオフすることになります。
パワーオフ保護時間	パワーオンしているデスクトップをシステムが自動的にパワーオフするまでの待機時間（分）を指定します。1 から 60 の値を入力できます。デフォルトは 30 分です。 この保護時間は主として、システムが自動的にデスクトップ仮想マシンをパワーオフする状況で使用されます。この [パワーオフ保護時間] を使用して、[電源管理] フィールドのしきい値設定を満たすように、仮想マシンのパワーオフを開始する前にシステムが指定した時間の間待機するように設定できます。システムは、[パワーオフ保護時間] に指定した時間の間待機した後に、構成されたスケジュールどおりに仮想マシンをパワーオフします。デフォルトの待機時間は 30 分です。
Windows ライセンスの質問	このウィザードでは、イメージ内にあり、デスクトップ仮想マシンに入ることになる Microsoft Windows オペレーティング システムを使用するための適格なライセンスがあることを確認するよう求められます。画面に表示される指示に従います。 クライアント オペレーティング システムの場合、Horizon Cloud はデフォルトで Windows クライアント ライセンス タイプを使用するように VDI 割り当てのデスクトップ仮想マシンを設定します。この設定は変更できません。

オプションで、詳細プロパティを構成します。

オプション	説明
コンピュータの OU	デスクトップ仮想マシンが配置される Active Directory 組織単位。識別名（たとえば、`OU=RootOrgName,DC=DomainComponent,DC=eng` など）を使用して Active Directory 組織単位を入力します。OU およびネストされた OU 内の各パスには、文字、数字、特殊文字、および空白の任意の組み合わせを含めることができ、最大で 64 文字にすることができます。 ネストされた組織単位を使用する必要がある場合は、ネストされた Active Directory ドメイン組織単位の使用についての考慮事項を参照してください。 **注：** [コンピュータの OU] が `CN=Computers` に設定されている場合、システムは、仮想マシンのデフォルトの Active Directory `Computers` コンテナを使用します。Active Directory には、組織単位クラスのコンテナにリダイレクトされるデフォルトのコンテナがあります。
1 回実行スクリプト	（オプション）仮想マシンの作成プロセスの後に、割り当てのデスクトップ仮想マシンで実行するスクリプトの場所。 **注：** スクリプトは、仮想マシンを再起動するための再起動ステップで終了する必要があります。そうしないと、エンド ユーザーは手動で再起動を実行するまで、デスクトップにログインすることができません。再起動のための Windows コマンド ラインを以下に示します。 `shutdown /r /t 0` スクリプトが再起動ステップで終了する必要がある理由は、sysprep プロセス後にスクリプトが実行されるときのシーケンスのためです。システムが割り当てのデスクトップ仮想マシンを作成すると、仮想マシンが起動し、Windows オペレーティング システムの `sysprep` プロセスを完了します。`sysprep` プロセスが完了したら、デスクトップ仮想マシンのエージェントがドメイン参加を行おうとします。同時に、エージェントはここで指定するスクリプト パスを取得します。エージェントは `Windows RunOnce` パス (`System run once`) を設定し、デスクトップ仮想マシンを再起動します。次の再起動時に、システムはローカル管理者アカウントを使用して Windows オペレーティング システムにログインし、スクリプトを実行します。デスクトップ仮想マシンが、ユーザーのログインに対応できるようになるのは、スクリプトに指定されているように、次回以降の再起動後になります。

オプション	説明
セッション タイムアウトの間隔	この間隔は、システムがデスクトップから強制的にログオフする前に、エンド ユーザーのセッションがアイドル状態を保持する時間です。このタイムアウトは、基盤となる Windows オペレーティング システムへのログイン セッションに適用されます。ここで指定する時間は、エンド ユーザーの Horizon Client または HTML Access ログイン セッションを制御するタイムアウト設定とは別のものです。 **注意：** 基盤となる Windows オペレーティング システムのセッションでシステムが強制的にログオフすると、保存されていないデータは失われます。データが意図せずに失われるのを防ぐには、エンド ユーザーのビジネス ニーズに応じてこの間隔の値を十分に大きくします。 デフォルトの間隔は 1 週間（10080 分）です。 **注：** タイムアウトの間隔に達する前にユーザー アクティビティが発生しない場合、30 秒以内に [OK] をクリックしないとログオフされることを示すメッセージがデスクトップに表示されます。ログアウトが発生すると、ドキュメントやファイルなど、保存されていないユーザー データは失われます。
Azure リソース タグ	（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。 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、[追加] 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。 ■ 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。 割り当てが作成されると、Azure リソース タグを追加したり、その割り当てのタグを編集または削除できます。

5 ウィザードの [管理] の手順で、フィールドに情報を入力し、該当する項目を選択して、[次へ] をクリックします。

オプション	説明
イメージの更新	[同時の静止デスクトップ] 設定は、このフローティング VDI デスクトップ割り当ての中で、割り当てのイメージの更新中に同時に静止することができる、パワーオン状態のデスクトップ仮想マシンの数を制御します。 たとえば、このフローティング VDI デスクトップ割り当てを後で編集して別のイメージを使用すると、システムは、セッションのない仮想マシンがあるパワーオン状態のデスクトップを同時にこの数だけパワーオフします (パワーオン状態のデスクトップにセッションがある場合、システムはセッションが終了するまで、そのデスクトップをパワーオフしません)。 パワーオフ状態のデスクトップ仮想マシンのセットに対して、システムは新しいイメージをそのセットにプロビジョニングするために必要なアクションを実行します。一般的なユースケースでは、この数は、この割り当てに対して定義されているデスクトップの最大数のサブセットに設定されます。ただし、必要に応じて、ここでは [デスクトップの最大数] の設定に等しい数を指定できます。このシナリオでは、新しいイメージを使用するように割り当てを編集するときに、システムは割り当てのパワーオン状態のデスクトップを同時にパワーオフすることができます。 **注：** この設定は、パワーオフ状態のデスクトップ仮想マシンには関係ありません。フローティング VDI デスクトップ割り当てのイメージが変更されると、システムはすぐにパワーオフ状態のデスクトップ仮想マシンを削除して、新しいイメージに更新します。
電源管理	これらの電源管理設定は、使用率に応じてフローティング VDI デスクトップ割り当てのパワーオンされたデスクトップ インスタンスの数を自動的に増やしたり減らしたりする際のしきい値に関連します。使用率が増えて上限を超えると、システムは自動的に新しいデスクトップ インスタンスを起動します。使用率が下限を下回ると、システムは、エンド ユーザーがデスクトップからログオフすると、デスクトップ仮想マシンをシャットダウンし、その割り当てを解除します。 電源管理の選択は、キャパシティのコストと迅速な可用性のバランスを取ります。 ■ 後からではなく、すぐに次のデスクトップ インスタンスをパワーオンする場合は、[最適化されたパフォーマンス] を選択します。ユーザーが要求するよりも早く次のデスクトップを準備することで電源の消費は増えますが、ユーザーが割り当てからデスクトップを起動しようとするときにはすでにデスクトップは起動しているので、そのようなユーザーの要求を満たすのに有効です。 ■ 次のデスクトップ インスタンスをパワーオンする時間をできるだけ遅らせる場合は、[最適化された電源] を選択します。割り当てのデスクトップ セットの占有率は、システムが次のデスクトップ インスタンスを起動する前に高くなります。既存のデスクトップの使用率を高めることでキャパシティのコストは最小限に抑えられますが、この設定では新規ユーザーがログインするときに遅延が発生する可能性が高くなります。これは、システムがデスクトップをパワーオンするまで待機が必要な場合があるためです。 ■ キャパシティのコストとユーザーに対する可用性までの時間のバランスを取るには [バランシング済み] を選択します。 各選択のしきい値の上限と下限は次のとおりです。 ■ [最適化されたパフォーマンス] ■ 低いしきい値：23% ■ 高いしきい値：50% ■ [最適化された電源] ■ 低いしきい値：38% ■ 高いしきい値：80%

オプション	説明
	■ [バランシング済み] ■ 低いしきい値：31% ■ 高いしきい値：66%

オプション	説明
タイムアウト処理	システムでデスクトップのユーザー セッションを処理する方法を設定します。 **注：** これらの設定によって管理されるユーザー セッションは、デスクトップの Windows オペレーティング システムへのユーザー ログインです。これらのセッションは、Horizon Client、Horizon HTML Access、または Workspace ONE のユーザー ログインではありません。 ユーザーのセッションは、ユーザーがデスクトップの Windows オペレーティング システムに対して認証されると開始します。 ■ [切断済みセッションのログオフ] - 切断されたセッションからシステムがいつユーザーをログオフするかを選択します。 ■ [セッションの最大有効期間] - システムが単一のユーザー セッションに対して許可する最大分数を指定します。
電源管理をスケジュール	Microsoft Azure でデスクトップ仮想マシンの省電力とパフォーマンスを最適化するため、パワーオン状態のデスクトップ インスタンスの最小数を週単位で繰り返し調整するスケジュールを設定するオプションがあります。次に例を示します。 ■ エンド ユーザーがデスクトップを使用していない週末や夜間の時間帯に対しては、パワーオン状態のデスクトップの数がゼロまたは少なくなるようスケジュール設定することができます。 ■ エンド ユーザーの需要が増大することが予測できる特定の日や特定の時間幅に対しては、その需要を満たすには利用可能になるパワーオン状態のデスクトップの最小数が増加するスケジュールを設定できます。 フローティング VDI デスクトップ割り当てに対して最大 10 個のスケジュールを指定できます。期間が重複しているのに、デスクトップの最小数の指定値が異なっているスケジュールがある場合は、システムはその重複する期間において大きい値の方のデスクトップの最小数を使用します。 a [+] アイコンをクリックして [電源管理をスケジュール] セクションで最初の行を追加します。 b 1 番目のスケジュールの識別名を入力します。 c 1 番目のスケジュールの日数を選択します。 **注：** 行が追加されると、1 日がデフォルトで自動的に選択されます。選択した日をこのスケジュールに含めないようにするには、ドロップダウンをクリックしてその選択された日の選択を解除します。 d 指定された日数の該当する時間を指定します。次のいずれかを行います。 ■ 指定した日数のすべての時間帯でこのスケジュールを有効にするには、[全日] チェック ボックスを選択します。 ■ それぞれの日に期間の開始時間と終了時間を指定します。 **注：** 暗号化された仮想マシンは、暗号化されていない仮想マシンよりもパワーオンに時間がかかります。[ディスクの暗号化] を [はい] に設定し、暗号化された仮想マシンのエンド ユーザー接続が、一日のうちの特定の時間帯に 100% 利用できるように設定したい場合、起動時間をその時間よりも早く設定する必要があります。暗号化された仮想マシンが多数ある場合のファームと VDI デスクトップの割り当ての電源管理のスケジューリングを参照してください。

オプション	説明
	e タイムゾーンを選択します。エンド ユーザーの場所に最も近いタイムゾーンが推奨されます。選択されたタイムゾーンに適した夏時間が自動的に適用されます。 **注：** 2 つのスケジュールで同じタイム ゾーン設定が使用されていて、時間の重複がある場合、警告が表示されます。ただし、2 つのスケジュールのタイム ゾーン設定が異なっていて、重複がある場合は、この警告は表示されません。例として、全日土曜日のスケジュールが 2 つ設定されていて、1 つが [ヨーロッパ/ロンドン] タイム ゾーンを選択していてもう 1 つが [アメリカ/トロント] を選択している場合、重複についての警告は表示されません。 f [デスクトップの最小数] フィールドに、指定した期間内にパワーオンするデスクトップの最小数を入力します。指定された期間内に、その最小数のデスクトップがパワーオンされ、その期間内でエンド ユーザーの要求に対応できます。この数の範囲はゼロ (0) からフローティング VDI デスクトップ割り当て全体の [デスクトップの最大数] に指定された数の間になります。この数値がゼロ (0) で、スケジュールの開始時点でアクティブなエンド ユーザー セッションがない場合は、割り当てのデスクトップがパワーオフされます。このシナリオでは、その後エンド ユーザーがスケジュールされた期間内にこの割り当てからデスクトップに接続しようとすると、デスクトップが使用可能な状態になるまで遅延が発生します。これは、基盤となるデスクトップ仮想マシンをパワーオンする必要があるためです。 **注：** デフォルトでは、ユーザーがスケジュールの時間外にあるときにデスクトップからログオフすると、システムは [パワーオフ保護時間] フィールドに指定した時間、その仮想マシンがパワーオフすることを防止します。デフォルトは 30 分です。

6 [ユーザー] の手順で、登録済みの Active Directory ドメイン内のユーザーとグループを検索し、この割り当てからデスクトップを使用する資格を付与するユーザーとグループを選択し、[次へ] をクリックします。

7 [サマリ] の手順で構成を確認し、[送信] をクリックします。

結果

システムは、デスクトップ インスタンスを構成するプロセスを開始し、選択したユーザーに VDI デスクトップを提供します。[割り当て] ページの [ステータス] 列に現在の進捗が反映されます。

注： 暗号化されたデスクトップ仮想マシンの作成は、暗号化されていない仮想マシンの作成の約 2 倍の時間がかかります。その結果、ディスクの暗号化が有効になっている VDI デスクトップの割り当てを作成する場合は、無効になっている場合と比べて、開始から完了までの時間が約 2 倍かかります。

次のステップ

特別なポートを開く必要があるアプリケーションがこのフローティング VDI デスクトップ割り当てのイメージにある場合、この割り当てに関連付けられたネットワーク セキュリティ グループ (NSG) を Microsoft Azure で変更する必要があります。NSG の詳細については、Horizon Cloud ポッド内のネットワーク セキュリティ グループと VDI デスクトップについてを参照してください。

この割り当てに NSX Cloud 管理を指定した場合、NSX Cloud 環境の Service Manager (CSM) を使用して、デスクトップ仮想マシンが NSX Cloud で管理されていることを確認できます。ユーザー環境の CSM にログインし、[クラウド] - [Azure] - [インスタンス] の順に移動します。その [インスタンス] ページに、デスクトップ インスタンスの管理対象のステータスが表示されたら、それらに NSX ポリシーの実装を開始できます。

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

Horizon Cloud では、デスクトップ割り当てを作成して、仮想デスクトップをエンド ユーザーにプロビジョニングします。Horizon Universal Console の [割り当て] 領域を使用して専用 VDI デスクトップ割り当てを作成します。Horizon Cloud テナントが Microsoft Azure のポッドでシングルポッド タイプの仲介を使用するように構成されている場合、ここの手順に従って、シングル ポッドから仮想デスクトップを仲介するデスクトップ割り当てを作成します。

注： テナントが Microsoft Azure のポッドで Universal Broker を使用するように構成されている場合は、ここで説明する手順に従うのではなく、マルチクラウド割り当てという、同じ割り当て内にある複数のポッドからリソースをプロビジョニングできるものを構成します。Microsoft Azure の Horizon Cloud ポッド - 第 1 世代環境での VDI マルチクラウド割り当ての作成と表示を参照してください。

テナント環境でのデスクトップ割り当てに関する全般的な情報については、Microsoft Azure の Horizon Cloud ポッドに基づくテナントのデスクトップ割り当ての概要を参照してください。

前提条件

- デプロイによっては、ブローカを設定しないとポッドに関連する割り当てを作成できないというメッセージが、コンソールの割り当て関連ページに表示されることがあります。このメッセージが表示された場合は、画面上の手順を実行します。
- Microsoft Windows クライアント オペレーティング システムを持つ少なくとも 1 つの公開イメージがあることを確認します。このようなイメージがない場合、VDI デスクトップ割り当てを作成することはできません。確認するには、[イメージ] ページに移動し、該当するイメージが一覧表示されているかを確認します。公開イメージの作成手順については、構成済みイメージ仮想マシンをポッドごとに Horizon Cloud の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。
- デスクトップに暗号化されたディスクを使用するかどうかを決定します。VDI デスクトップ割り当てを作成するときに、ディスクの暗号化を指定する必要があります。割り当ての作成後にディスクの暗号化を追加することはできません。ディスク機能の説明については、Horizon Cloud 環境のファームおよび VDI デスクトップでの Microsoft Azure ディスク暗号化の使用を参照してください。

  重要： このリリースでは、データ ディスクが接続されたイメージ仮想マシンを使用するフローティング VDI 割り当てのディスク暗号化をサポートしていません。割り当てで使用する予定のイメージにデータ ディスクがないことを確認してください。

- デスクトップ仮想マシンで NSX Cloud 機能を使用できるようにするかどうかを決定します。VDI デスクトップ割り当てを作成するときは、NSX Cloud 管理を有効にする必要があります。NSX Cloud 管理の割り当ては、作成後に有効にすることはできません。この割り当て用に選択する公開済みイメージには、NSX エージェントがインストールされていることが必要です。イメージの公開前に NSX エージェントをインストールする必要があります。Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッド とそのサブトピックを参照してください。
- この割り当てのデスクトップ仮想マシンをポッドのプライマリ仮想マシン サブネット（テナント サブネットともいいます）とは異なる仮想マシン サブネットに接続するかどうかを決定します。ポッドでマニフェスト 2298 以降が実行されていて、仮想マシン サブネットをさらに追加するためにポッドを編集してある場合は、そのサブ

ネットをこのデスクトップ割り当てに使用するよう指定できます。このユースケースでは、使用する仮想マシン サブネットが `Ready` の状態でポッドの詳細ページの [ネットワーク] セクションに表示されていることを確認する必要があります。これにより、そのサブネットがワークフローの手順で選択できるようになります。詳細については、ファーム用および VDI 割り当て用 Horizon Cloud ポッドでの複数のテナント サブネットの使用の概要 を参照してください。

手順

1 割り当て関連のコンソール ページに移動して、VDI デスクトップ割り当ての作成先を探し、新しい割り当てワークフローを開始します。

ヒント: コンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。コンソールの割り当て関連ページに表示されるラベルは、テナントの設定済みのブローカ設定、フリート内のクラウド接続されたポッドのタイプ、テナントの地域別クラウド プレーン、および特定のライセンスに基づく機能などの要因によって異なります。

2 [新しい割り当て] の開始画面で、[デスクトップ] アイコンをクリックします。

[新しいデスクトップ割り当て] ウィンドウが開き、最初のウィザードの手順が表示されます。

3 [専用] を選択します。

4 [定義] の手順での選択を完了し、[次へ] をクリックします。

注： 必要に応じてスクロール バーを使用して、すべての必須フィールドを表示します。

オプション	説明
場所	デスクトップを提供するポッドの場所を選択します。
ポッド	ポッドを選択します。 **ヒント:** 選択するポッドが表示されない場合は、[場所] リストにポッドがない場所が表示されていないことを確認します。[場所] フィールドは [ポッド] リストに表示され、選択した場所に関連付けられていないポッドを除外します。すでに場所にポッドがあり、そのポッドを削除するか別の場所に移動して、表示された場所にポッドが存在しなくなると、[ポッド] リストにはエントリが表示されなくなります。場所はアルファベット順に表示されているため、画面を開くと、アルファベット順で最初の場所が自動的に選択されます。その場所にポッドが関連付けられていない場合は、場所を別のエントリに切り替える必要があります。

オプション	説明
仮想マシン サブネットの指定	このトグルを有効にすると、割り当てのデスクトップ仮想マシンの接続先とする特定のサブネットを 1 つ以上選択できます。トグルを有効にしたら、表示される一覧から特定のサブネットを選択できます。 このトグルがオフに切り替えられている場合、割り当てのデスクトップ仮想マシンはデフォルトでポッドのプライマリ仮想マシン サブネットに接続されます。

オプション	説明
モデルのフィルタリング	1 つ以上のフィルタを設定して、[モデル] ドロップダウン メニューで使用できるモデルを制御します。モデルは、タイプ、シリーズ、CPU の数、メモリ、およびタグでフィルタできます。モデルの選択の詳細については、Horizon Universal Console でのファームと割り当ての仮想マシン タイプとサイズの管理を参照してください。ここでは、[仮想マシンのタイプとサイズ] ページ（[設定] - [仮想マシンのタイプとサイズ]）のオプションについて説明しています。  フィルタを設定するには、まずドロップダウン メニューで条件を選択し、次に目的の値を入力します。デフォルトでは、条件が [タグ]、値が [VMware 推奨] の単一のフィルタがあります。この最初のフィルタを編集し、[And] および [Or] 演算子によって接続されたフィルタをさらに追加できます。 次に、フィルタに使用できる基準と、それぞれに入力できる値の説明を示します。 **[タイプ]**  このオプションを選択すると、2 番目のドロップダウン メニューはデフォルトで [GPU と高パフォーマンス - GPU を使用するモデル] に設定されます。 **注：** GPU モデルを選択した場合、表示されるイメージのリストには「GPU を含める」フラグを選択して作成されたイメージのみが含まれるため、GPU モデルを使用してファームまたはプールを作成するにはそのようなイメージが少なくとも 1 つ必要です。GPU 以外のモデルを選択した場合、表示されるイメージのリストには、「GPU を含める」フラグなしで作成されたイメージのみが含まれます。 **[シリーズ]**  このオプションを選択すると、2 番目のドロップダウン メニューから一連のモデルを選択できます。リストの一番上にある [フィルタ] テキスト ボックスにテキストを入力してこのリストをフィルタリングすることもできます。 **[CPU の数]**  このオプションを選択すると、CPU 範囲を入力できます。 **重要：** 本番環境では、予期しないエンドユーザー接続の問題を回避するために、2 個以上の CPU を持つ仮想マシン モデルを使用します。 **[メモリ]** 

オプション	説明
	このオプションを選択すると、メモリ範囲（GB 単位）を入力できます。 **[タグ]**  このオプションを選択すると、2 番目のドロップダウン メニューからタグを選択できます。リストの一番上にある [フィルタ] テキスト ボックスにテキストを入力してこのリストをフィルタリングすることもできます。ドロップダウン メニューで使用可能なタグは、ハードコードされたシステム タグと、[仮想マシンのタイプとサイズ] ページ ([設定] - [仮想マシンのタイプとサイズ]) で作成したカスタム タグの両方です。 フィルタごとに次の手順を実行して、追加フィルタを設定できます。 a [追加] リンクをクリックします。 b 前のフィルタと作成中の新しいフィルタの間の演算子として And または Or を選択します。 c 新しいフィルタを設定するには、条件を選択して値を入力します。
モデル	デスクトップ インスタンスに使用するモデルを選択します。この選択では、デスクトップ インスタンスが作成されるときに使用される基盤となるリソースのセットを、キャパシティ（コンピューティング、ストレージなど）の観点から定義します。使用可能な選択肢は、Microsoft Azure で使用可能な標準の仮想マシン サイズにマッピングされます。 **重要：** 本番環境の場合は、2 個以上の CPU が搭載された仮想マシン モデルを選択します。第 1 世代の Horizon Cloud スケール テストでは、2 個以上の CPU を使用すると、予期しないエンド ユーザー接続の問題を回避す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、このようなモデルはテスト用または事前検証用にのみ使用する必要があります。
ディスク タイプ	利用可能なオプションからサポートされているディスク タイプを選択します。ディスク タイプのオプションは、選択したモデル、および Azure サブスクリプションとリージョンに基づいています。一般的に使用可能なディスク タイプは次のとおりです。 ■ 標準 HDD - デフォルトのディスク タイプ。 ■ 標準 SSD ■ プレミアム SSD - このオプションは、プレミアム I/O をサポートするモデルを選択した場合にのみ表示されます。 必要に応じて、割り当てを作成した後に選択内容を編集できます。
ディスク サイズ	この割り当ての仮想マシンの OS ディスク サイズを GB 単位で入力します。 ■ デフォルト値は、基本イメージの OS ディスク サイズ（通常は 128GB）です。 ■ サイズを編集する場合、入力する値は基本イメージの OS ディスク サイズよりも大きくなければなりません。また、選択したモデルでサポートされる最大サイズ（通常は 1024GB）を超えることはできません。 ■ この値は、必要に応じて後で編集することもできます。 **重要：** ディスク サイズを編集する場合は、仮想マシンが予期したとおりに作成されるように、追加のアクションを実行する必要があります。詳細については、ファームまたは VDI デスクトップ割り当てのディスク サイズが増加した場合に必要な管理者のアクションを参照してください。
ドメイン	お使いの環境に登録されている Active Directory ドメインを選択します。

オプション	説明
ドメインへの参加	[はい] を選択し、デスクトップ インスタンスが作成後に自動的にドメインに参加されるようにします。
ディスクの暗号化	デスクトップ インスタンスが暗号化されたディスクを持つようにするため [はい] を選択します。 **重要：** ディスクを暗号化する場合は、VDI デスクトップ割り当てを作成するときにこの選択を行う必要があります。割り当ての作成後にディスクの暗号化を追加することはできません。
NSX Cloud 管理	割り当てのデスクトップ インスタンスを持つ NSX Cloud の機能を使用できるように、[はい] を選択します。Microsoft Azure のデスクトップでの NSX Cloud 機能の使用については、Microsoft Azure 内の VMware NSX Cloud と Horizon Cloud ポッドおよびそのサブトピックを参照してください。 **重要：** ■ デスクトップ インスタンスを持つ NSX Cloud を使用する場合、VDI デスクトップ割り当ての作成時にこの選択を行う必要があります。NSX Cloud 管理は、割り当て作成後に有効にすることはできません。 ■ 割り当てのデスクトップ インスタンスで NSX Cloud 管理機能を使用するには、この割り当て用に選択したイメージに NSX エージェントがインストールされている必要があります。この設定を [はい] に切り替えるときは、[イメージ] で選択したイメージに NSX Agent がインストールされている必要があります。システムは、VDI デスクトップ割り当てを作成するときに、選択したイメージに NSX エージェントがあるかどうかを検証しません。
イメージ	エンド ユーザーに割り当てるイメージを選択します。 選択したポッドの公開イメージのうち、VDI デスクトップに適しているものだけがここに一覧表示されます。公開イメージは、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も呼ばれ、基本イメージまたはゴールド イメージをデスクトップに変換してシステムに公開したものです。 **重要：** [NSX Cloud 管理] を [はい] に設定する場合は、ここで選択したイメージに NSX Agent がインストールされていることを確認します。割り当てのデスクトップ インスタンスで NSX Cloud 管理機能を使用するには、この割り当て用に選択したイメージに NSX エージェントがインストールされている必要があります。システムは、VDI デスクトップ割り当てを作成するときに、選択したイメージに NSX エージェントがあるかどうかを検証しません。
割り当ての名前	この専用 VDI デスクトップ割り当てのわかりやすい名前を入力します。エンド ユーザーにデスクトップの資格がまだ割り当てられていない場合、または割り当てられているもののまだ要求していない場合、クライアントで資格のあるデスクトップにアクセスする際に、この形式の割り当ての名前が表示されます。 名前には文字、ハイフン、数字のみを含める必要があります。スペースは使用できません。名前を英字以外の文字で始めることはできません。
仮想マシン名	この割り当てで作成されたデスクトップ仮想マシンの基底名。仮想マシン名はこの基本名に数値を加えたもの、たとえば、win10-1、win10-2 などになります。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。エンド ユーザーが、クライアントでデスクトップにアクセスする際に、この名前が表示されます。

オプション	説明
既定のプロトコル	エンド ユーザー セッションで使用するデフォルトの表示プロトコルを選択します。 デフォルトのプロトコルではなく、別のプロトコルが使用される状況が発生する場合があります。たとえば、クライアント デバイスがデフォルトのプロトコルをサポートしない場合や、エンド ユーザーが、選択されているデフォルト プロトコルよりも他のプロトコルを優先して使用する場合があります。 **注：** Microsoft Windows 7 Enterprise オペレーティング システムのイメージの場合、サポートされている選択肢は RDP のみです。
優先クライアント タイプ	エンド ユーザーが Workspace™ ONE™ Access からデスクトップを起動するときに使用する優先クライアント タイプを選択します。これは Horizon Client、または HTML Access 用のブラウザのいずれかになります。 **注：** Microsoft Windows 7 Enterprise オペレーティング システムのイメージの場合、サポートされている選択肢は Horizon Client のみです。
キャパシティ	割り当てに必要なデスクトップ数を入力します。
デスクトップの最小数 **デスクトップの最大数**	**ヒント:** 専用 VDI デスクトップ割り当てに対するこの [最小デスクトップ] 設定は、フローティング VDI デスクトップ割り当ての設定とは少し異なります。専用の VDI デスクトップ割り当ての場合、[最小デスクトップ] の設定は、未割り当てのデスクトップを表します。デスクトップがユーザーに割り当てられると、そのデスクトップ仮想マシンは未割り当てのデスクトップではなくなり、その結果、[最小デスクトップ] の設定によって管理されるデスクトップのセットの一部とは見なされません。割り当て内の未割り当てのデスクトップ仮想マシンの数が [最小デスクトップ] の値よりも小さい場合、パワーオン状態の仮想マシンの数が [最小デスクトップ] の値未満であることがわかります。 ■ [最小デスクトップ] - この割り当てによって定義されたプール内にあるパワーオン状態の未割り当てのデスクトップ仮想マシンの数を設定します。割り当てが最初に作成されるとき、割り当て可能な最大数の合計（[最大デスクトップ] の数で設定）からゼロのデスクトップ仮想マシンが割り当てられます。したがって、その時点では、ここで設定する数は、可能な最大数のうち、最初にパワーオンする未割り当ての仮想マシンの数のサブセットです。[最小デスクトップ] にゼロ (0) を指定した場合は、割り当てが最初に作成されるときに未割り当てのデスクトップ仮想マシンをパワーオンしないことを示します。 一部の未割り当ての仮想マシンをパワーオンするように設定することのメリットは、主に、ユーザーがすぐにログインできるように未割り当ての仮想マシンを用意しておくことです。時間の経過とともに、これらのパワーオン状態で未割り当てのデスクトップがユーザーに割り当てられると、デスクトップを要求する初回のログインを行うユーザーから、または [割り当て] アクションを使用してデスクトップをユーザーに明示的に割り当てる管理者から、システムは [最大デスクトップ] 数に達するまで追加の未割り当てのデスクトップをパワーオンします。最後に、割り当て内のすべてのデスクトップ仮想マシンがユーザーに割り当てられている場合、[最小デスクトップ] の値は、ユーザーからのデスクトップの割り当て解除を明示的に開始するまであまり使用されません。 ■ [最大デスクトップ] - この割り当てによって定義された仮想マシンのプールに必要なデスクトップ仮想マシンの総数を設定します。

オプション	説明
パワーオフ保護時間	パワーオンしているデスクトップをシステムが自動的にパワーオフするまでの待機時間（分）を指定します。1 から 60 の値を入力できます。デフォルトは 30 分です。 この保護時間は主として、システムが自動的にデスクトップ仮想マシンをパワーオフする状況で使用されます。この [パワーオフ保護時間] 設定を使用すると、仮想マシンのパワーオフを開始するまでに、システムを指定された時間待機させることができます。たとえば、[電源管理をスケジュール] でスケジュールが定義されている場合、設定されたスケジュールに適合するようにシステムがデスクトップを自動的にパワーオフすることができます。設定されたスケジュール内における割り当てのデスクトップのいずれかを手動でパワーオンする場合、設定されたスケジュールに一致するように、システムは [パワーオフ保護時間] に指定されている時間だけ待機してから仮想マシンをパワーオフします。デフォルトの待機時間は 30 分です。
Windows ライセンスの質問	このウィザードでは、イメージ内にあり、デスクトップ仮想マシンに入ることになる Microsoft Windows オペレーティング システムを使用するための適格なライセンスがあることを確認するよう求められます。画面に表示される指示に従います。 クライアント オペレーティング システムの場合、Horizon Cloud はデフォルトで Windows クライアント ライセンス タイプを使用するように VDI 割り当てのデスクトップ仮想マシンを設定します。この設定は変更できません。

オプションで、詳細プロパティを構成します。

オプション	説明
コンピュータの OU	デスクトップ仮想マシンが配置される Active Directory 組織単位。識別名（たとえば、`OU=RootOrgName,DC=DomainComponent,DC=eng` など）を使用して Active Directory 組織単位を入力します。OU およびネストされた OU 内の各パスには、文字、数字、特殊文字、および空白の任意の組み合わせを含めることができ、最大で 64 文字にすることができます。 ネストされた組織単位を使用する必要がある場合は、ネストされた Active Directory ドメイン組織単位の使用についての考慮事項を参照してください。 **注：** [コンピュータの OU] が `CN=Computers` に設定されている場合、システムは、仮想マシンのデフォルトの Active Directory `Computers` コンテナを使用します。Active Directory には、組織単位クラスのコンテナにリダイレクトされるデフォルトのコンテナがあります。
1 回実行スクリプト	（オプション）仮想マシンの作成プロセスの後に、割り当てのデスクトップ仮想マシンで実行するスクリプトの場所。 **注：** スクリプトは、仮想マシンを再起動するための再起動ステップで終了する必要があります。そうしないと、エンド ユーザーは手動で再起動を実行するまで、デスクトップにログインすることができません。再起動のための Windows コマンド ラインを以下に示します。 `shutdown /r /t 0` スクリプトが再起動ステップで終了する必要がある理由は、sysprep プロセス後にスクリプトが実行されるときのシーケンスのためです。システムが割り当てのデスクトップ仮想マシンを作成すると、仮想マシンが起動し、Windows オペレーティング システムの `sysprep` プロセスを完了します。`sysprep` プロセスが完了したら、デスクトップ仮想マシンのエージェントがドメイン参加を行おうとします。同時に、エージェントはここで指定するスクリプト パスを取得します。エージェントは `Windows RunOnce` パス (`System run once`) を設定し、デスクトップ仮想マシンを再起動します。次の再起動時に、システムはローカル管理者アカウントを使用して Windows オペレーティング システムにログインし、スクリプトを実行します。デスクトップ仮想マシンが、ユーザーのログインに対応できるようになるのは、スクリプトに指定されているように、次回以降の再起動後になります。

オプション	説明
最大デスクトップ削除	これは、[設定] - [全般設定] ページの [削除保護] で設定したレートに対してカウントされる前に、割り当て内で削除できるデスクトップ仮想マシンの数を設定します。ドロップダウン メニューから次のオプションを 1 つ選択します。 ■ [無制限]：無制限の数のデスクトップ仮想マシンを割り当てから削除できます。この場合、[削除保護] の設定は関係なくなります。 ■ [なし]：[削除保護] で設定したレートに対してカウントされる前に、追加で削除できるデスクトップ仮想マシンはありません。この場合、システムは [削除保護] のみを使用して削除を許可またはブロックします。[なし] は [削除保護] のデフォルト値です。 ■ [カスタム]：[削除保護] で設定したレートに対してカウントされる前に、追加で削除できるデスクトップ仮想マシンの数。[カスタム] を選択した場合は、このドロップダウン メニューの右側に数値も入力する必要があります。 たとえば、[最大デスクトップ削除] を 10、[削除保護] を 1 に設定するとします。この場合、最初の 10 台の仮想マシンが削除された後 （数が 10 になるまでの時間に関係なく）、システムはそれ以降、1 時間あたり 1 台の追加の仮想マシンのみを削除できます。 **重要：** 専用デスクトップ割り当てに新しいイメージを指定すると、システムでは必要に応じて [最大デスクトップ削除] の設定を変更して、未割り当てのデスクトップ仮想マシンをすべて新しいイメージで再構築できるようにします。 **注：** [削除保護] で [無制限] を選択した場合、[最大デスクトップ削除数] 設定を使用する必要はありません。 [削除保護] 設定の詳細については、Horizon Cloud テナント環境のカスタマイズ可能な全般設定を参照してください。 専用デスクトップ割り当て内のすべての仮想マシンの削除を防止するには、[割り当て] ページの [削除の防止] 設定を使用します。専用デスクトップ割り当ての削除の防止または削除の許可を参照してください。

オプション	説明
セッション タイムアウトの間隔	この間隔は、システムがデスクトップから強制的にログオフする前に、エンド ユーザーのセッションがアイドル状態を保持する時間です。このタイムアウトは、基盤となる Windows オペレーティング システムへのログイン セッションに適用されます。ここで指定する時間は、エンド ユーザーの Horizon Client または HTML Access ログイン セッションを制御するタイムアウト設定とは別のものです。 **注意：** 基盤となる Windows オペレーティング システムのセッションでシステムが強制的にログオフすると、保存されていないデータは失われます。データが意図せずに失われるのを防ぐには、ユーザーのビジネス ニーズに応じてこの間隔の値を十分に大きくします。 デフォルトの間隔は 1 週間（10080 分）です。 **注：** タイムアウトの間隔に達する前にユーザー アクティビティが発生しない場合、30 秒以内に [OK] をクリックしないとログオフされることを示すメッセージがユーザーに表示されます。ログアウトが発生すると、ドキュメントやファイルなど、保存されていないユーザー データは失われます。
Azure リソース タグ	（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。 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、[追加] 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。 ■ 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。 < > % & \ ? / ■ 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。 割り当てが作成されると、Azure リソース タグを追加したり、その割り当てのタグを編集または削除できます。

5 ウィザードの [管理] の手順で、フィールドに情報を入力し、該当する項目を選択して、[次へ] をクリックします。

オプション	説明
イメージの更新	[同時の静止デスクトップ] 設定は、この専用 VDI デスクトップ割り当ての中で、割り当てのイメージの更新中に同時に静止することができる割り当て解除されたデスクトップの数を制御します。たとえば、後で別のイメージを使用するためにこの専用 VDI デスクトップ割り当てを編集すると、システムはこの割り当て解除された数のデスクトップを同時にパワーオフします。次にシステムは、パワーオフ状態の割り当て解除されたデスクトップのセットに新しいイメージをプロビジョニングするために必要なアクションを実行します。 **注：** ユーザーにマッピングされた専用 VDI デスクトップ割り当てのデスクトップは、それらのユーザーに割り当てられている、と言います。専用 VDI デスクトップ割り当ての割り当て解除されたデスクトップは、まだ特定のユーザーにマッピングされていないデスクトップです。
タイムアウト処理	システムでデスクトップのユーザー セッションを処理する方法を設定します。 **注：** これらの設定によって管理されるユーザー セッションは、デスクトップの Windows オペレーティング システムへのユーザー ログインです。これらのセッションは、Horizon Client、Horizon HTML Access、または Workspace ONE のユーザー ログインではありません。 ユーザーのセッションは、ユーザーがデスクトップの Windows オペレーティング システムに対して認証されると開始します。 ■ [切断済みセッションのログオフ] - 切断されたセッションからシステムがいつユーザーをログオフするかを選択します。 ■ [セッションの最大有効期間] - システムが単一のユーザー セッションに対して許可する最大分数を指定します。
電源管理をスケジュール	Microsoft Azure でデスクトップ仮想マシンの省電力とパフォーマンスを最適化するために、週単位で繰り返し、パワーオン状態の割り当て解除されたデスクトップ インスタンスの最小数を調整するスケジュールを任意に構成することができます。次に例を示します。 ■ エンド ユーザーがデスクトップを使用していない週末や夜間の時間帯に対しては、パワーオン状態の割り当て解除されたデスクトップの数がゼロまたは少なくなるようスケジュール設定することができます。 ■ エンド ユーザーの需要が増大することが予測できる特定の日や特定の時間幅に対しては、その需要を満たすには利用可能になるパワーオン状態の割り当て解除されたデスクトップの最小数が増加するスケジュールを設定できます。

オプション	説明
	専用 VDI デスクトップ割り当てに対して最大 10 個のスケジュールを指定できます。期間が重複しているのに、割り当て解除されたデスクトップの最小数の指定値が異なっているスケジュールがある場合は、システムはその重複する期間において大きい値の方の割り当て解除されたデスクトップの最小数を使用します。 **注意：** 既定では、ここで専用 VDI デスクトップ割り当てのスケジュールを構成すると、システムはスケジュールに関係なく割り当て済みのすべてのデスクトップ仮想マシンをパワーオン状態のままにします。これは以下を意味します。 ■ ここでスケジュールを設定すると、システムは現在割り当てられている（ユーザーにマッピングされている）デスクトップ仮想マシンをパワーオン状態のままにします。スケジュールは、割り当て解除されたデスクトップ（もしあれば）の電源状態のみを制御します。 ■ このときにスケジュールが設定されている場合、割り当て済みのデスクトップのパワーオン動作をシステムが処理する方法は、スケジュールが設定されていない場合の方法とは異なります。ここでスケジュールが構成されていない場合、システムはユーザーがログインしていない割り当て済みのデスクトップをパワーオフします。 たとえば、この専用 VDI デスクトップ割り当てのすべてのデスクトップがユーザーにマッピングされ（割り当て済み）、ここでスケジュールが構成されている場合、システムは設計上それらの割り当て済みのデスクトップをパワーオフしません。この設計の目的は、スケジュールが有効であっても、割り当て済みのデスクトップがマッピングされたユーザーのログイン要求を満たす準備ができるようにすることです。 その結果、すべてのデスクトップが割り当て済みの状態になっている場合、ここでスケジュールを設定すると、割り当て済みのユーザーがログインしていなくてもそれらの割り当て済みのデスクトップはパワーオン状態のままになります。週末のような特定の日にすべての割り当て済みのデスクトップ仮想マシンをパワーオフする場合は、ここでスケジュールを設定しないでください。 スケジュールを構成するには、次の手順を実行します。 a [+] アイコンをクリックして [電源管理をスケジュール] セクションで最初の行を追加します。 b 1 番目のスケジュールの識別名を入力します。 c 1 番目のスケジュールの日数を選択します。 **注：** 行が追加されると、1 日がデフォルトで自動的に選択されます。選択した日をこのスケジュールに含めないようにするには、ドロップダウンをクリックしてその選択された日の選択を解除します。 d 指定された日数の該当する時間を指定します。次のいずれかを行います。 ■ 指定した日数のすべての時間帯でこのスケジュールを有効にするには、[全日] チェック ボックスを選択します。 ■ それぞれの日に期間の開始時間と終了時間を指定します。 **注：** 暗号化された仮想マシンは、暗号化されていない仮想マシンよりもパワーオンに時間がかかります。[ディスクの暗号化] を [はい] に設定し、暗号化された仮想マシンのエンド ユーザー接続が、一日のうちの特定の時間帯に 100% 利用できるように設定したい場合、起動時間をその時間よりも早く設定する必要があります。暗号化された仮想マシンが多数ある場合のファームと VDI デスクトップの割り当ての電源管理のスケジューリングを参照してください。

オプション	説明
	e タイムゾーンを選択します。エンド ユーザーの場所に最も近いタイムゾーンが推奨されます。選択されたタイムゾーンに適した夏時間が自動的に適用されます。 **注：** 2 つのスケジュールで同じタイム ゾーン設定が使用されていて、時間の重複がある場合、警告が表示されます。ただし、2 つのスケジュールのタイム ゾーン設定が異なっていて、重複がある場合は、この警告は表示されません。例として、全日土曜日のスケジュールが 2 つ設定されていて、1 つが [ヨーロッパ/ロンドン] タイム ゾーンを選択していてもう 1 つが [アメリカ/トロント] を選択している場合、重複についての警告は表示されません。 f [デスクトップの最小数] フィールドに、指定した期間内にパワーオンする割り当て解除されたデスクトップの最小数を入力します。指定された期間内に、入力した最小数の割り当て解除されたデスクトップがパワーオンされ、その期間内でのエンド ユーザーの要求に対応するために使用できます。この数の範囲はゼロ (0) から専用 VDI デスクトップ割り当て全体の [デスクトップの最大数] に指定された数の間になります。 **重要：** 電源管理スケジュールの [デスクトップの最小数] フィールドは、割り当て解除されたデスクトップのみを制御します。割り当て済みのデスクトップは電源管理スケジュールに参加しません。専用 VDI デスクトップ割り当てのすべてのデスクトップが割り当て済みの状態になると、割り当て解除されたデスクトップを制御するこの [デスクトップの最小数] の値はデフォルトのゼロ (0) になります。 この数値がゼロ (0) で、スケジュールの開始時点でアクティブなエンド ユーザー セッションがない場合は、割り当てのデスクトップがパワーオフされます。このシナリオでは、その後エンド ユーザーがスケジュールされた期間内にこの割り当てからデスクトップに接続しようとすると、デスクトップが使用可能な状態になるまで遅延が発生します。これは、基盤となるデスクトップ仮想マシンをパワーオンする必要があるためです。 **注：** デフォルトでは、ユーザーがスケジュールの時間外にあるときにデスクトップからログオフすると、システムは [パワーオフ保護時間] フィールドに指定した時間、その仮想マシンがパワーオフすることを防止します。デフォルトは 30 分です。

6 [ユーザー] の手順で、登録済みの Active Directory ドメイン内のユーザーとグループを検索し、この割り当てからデスクトップを使用する資格を付与するユーザーとグループを選択し、[次へ] をクリックします。

7 [サマリ] の手順で構成を確認し、[送信] をクリックします。

結果

システムは、デスクトップ インスタンスを構成するプロセスを開始し、選択したユーザーに VDI デスクトップを提供します。[割り当て] ページの [ステータス] 列に現在の進捗が反映されます。

注： 暗号化されたデスクトップ仮想マシンの作成は、暗号化されていない仮想マシンの作成の約 2 倍の時間がかかります。その結果、ディスクの暗号化が有効になっている VDI デスクトップの割り当てを作成する場合は、無効になっている場合と比べて、開始から完了までの時間が約 2 倍かかります。

また、イメージ仮想マシンにデータ ディスクがある場合は、そのイメージ仮想マシンに基づいて、暗号化されたデスクトップ仮想マシンを作成するための追加の時間が必要になります。より大きい、テラバイト単位のサイズのデータ ディスクでは、極めて長い時間がかかります。

次のステップ

特別なポートを開く必要があるアプリケーションが VDI デスクトップにある場合、この VDI デスクトップ割り当てに関連付けられたネットワーク セキュリティ グループ (NSG) を Microsoft Azure で変更する必要があります。ポッドの NSG の詳細については、Horizon Cloud ポッド内のネットワーク セキュリティ グループと VDI デスクトップについてを参照してください。

この割り当てに NSX Cloud 管理を指定した場合、NSX Cloud 環境の Service Manager (CSM) を使用して、デスクトップ仮想マシンが NSX Cloud で管理されていることを確認できます。ユーザー環境の CSM にログインし、[クラウド] - [Azure] - [インスタンス] の順に移動します。その [インスタンス] ページに、デスクトップ インスタンスの管理対象のステータスが表示されたら、それらに NSX ポリシーの実装を開始できます。

Horizon Cloud on Microsoft Azure - シングルポッド ブローカの概要

この記事では、シングルポッド ブローカと呼ばれる仲介タイプについて簡単に説明します。

シングルポッド仲介タイプは、レガシーまたはクラシック仲介とも呼ばれます。これは、Horizon Cloud ポッドが初めて登場したときに利用できる最初で唯一の仲介タイプであったためです。最新のより高度な仲介テクノロジーは Universal Broker です。シングルポッド仲介を使用するように構成されたテナントは、Universal Broker を使用するように移行できます。7 章 シングル ポッド ブローカから Universal Broker への移行についてを参照してください。

v2111 サービス リリースの時点では、グリーンフィールドのお客様テナント環境ではシングルポッド仲介を使用できません。このコンテキストでは、グリーンフィールドとは、テナントの Horizon Cloud ポッドに対してコンソールの [ブローカ] ページ内でコンソールの有効化手順が一度も開始されたことのないテナント環境を意味します。

シングルポッド仲介とエンド ユーザー割り当て

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、Horizon Cloud ポッドから次のタイプのポッド単位の割り当てが可能になります。

- 単一の Horizon Cloud ポッドからの仮想デスクトップで構成される VDI デスクトップ割り当て
- 単一の Horizon Cloud ポッド内の Microsoft リモート デスクトップ サービス (RDS) ホストからのセッションベースのデスクトップで構成されるセッション デスクトップ割り当て
- Horizon Cloud ポッド内の RDS ホストによってプロビジョニングされたアプリケーションで構成されるリモート アプリケーション割り当て
- Horizon Cloud ポッド内にある VDI デスクトップによってホストされている App Volumes アプリケーションで構成される App Volumes アプリケーション割り当て

シングルポッド ブローカ - Horizon Cloud ポッド - URL リダイレクトのカスタマイズを作成し、ユーザーに割り当てる

この機能は、シングルポッド仲介を使用するように構成された環境でのみ使用できます。Horizon Universal Console では、エンド ユーザーの環境をカスタマイズする設定の割り当てを行うカスタマイズ割り当てを作成します。カスタマイズのタイプの 1 つは、URL リダイレクトです。Horizon Client がエンド ユーザーのクライアント マシンから Horizon Cloud 環境で提供されるデスクトップまたはアプリケーションに URL をリダイレクトするときに適用される URL 処理ルールを定義します。URL リダイレクト構成では、どの URL をユーザーのローカル シス

テムで開く代わりにエンド ユーザーに割り当てた Horizon Cloud デスクトップまたはアプリケーションで処理するのかについての情報を Horizon Client に提供します。

注：

- 管理コンソールには、クライアントからエージェントへの URL リダイレクトを構成するためのユーザー インターフェイスがあります。エージェントからクライアントへの URL リダイレクトを構成するには、シングルポッド ブローカ - Horizon Cloud ポッドと URL コンテンツ リダイレクト機能の説明に従ってグループ ポリシー設定を使用する必要があります。以下の手順では、クライアントからエージェントへの URL リダイレクトを構成します。
- Microsoft Azure のポッドに Universal Broker を使用するように Horizon Cloud テナントが構成されている場合、これらの URL リダイレクトのカスタマイズの作成は現在サポートされていません。

ユーザーがローカル デバイスの Horizon Client にログインするときに、Horizon Client はエンド ユーザーの割り当て済み URL リダイレクト ルールをフェッチします。次に、そのユーザーがローカル ドキュメントまたはファイル内のリンクを開こうとし、そのリンクが割り当てられた設定内の URL パターン ルールに一致する場合、Horizon Client は使用する適切なハンドラを決定します。指定されたハンドラは、ユーザーに割り当てられたデスクトップまたはアプリケーション（URL リダイレクト設定で指定した適切なハンドラによって決定される）を開いて、URL リンクを処理します。URL リダイレクト ハンドラによってデスクトップを使用するように指定された場合、リンクの指定されたプロトコルに対するデスクトップのデフォルト アプリケーションが URL を処理します。ハンドラによってアプリケーションを使用するように指定された場合、ユーザーに割り当てられたアプリケーションが URL を処理します。ユーザーがハンドラで指定されたデスクトップまたはアプリケーションを使用する資格を持たない場合、ハンドラの [厳密な一致] を [いいえ] に設定していない限り、Horizon Client はユーザーにメッセージを返します。

[厳密な一致] が [いいえ] に設定されている場合、システムは次のフォールバック動作に基づいて使用するリソースを見つけます。

1 システムは、ハンドラに指定されたターゲット リソースの部分文字列の一致を使用してユーザーの割り当てを検索します。部分文字列に一致する割り当てが見つかると、システムはその割り当てられたデスクトップまたはアプリケーションを使用してリンクを開きます。

2 ハンドラの [リソース タイプ] が [アプリケーション] に設定されている場合、部分文字列の一致検索に失敗すると、システムは、ユーザーのアプリケーション割り当て内で、ハンドラの [スキーム] フィールドで指定されたプロトコルを処理できる割り当て済みアプリケーションを検索します。

   注： このフォールバック動作の手順はアプリケーションにのみ適用されます。[リソース タイプ] が [デスクトップ] に設定されている場合、この手順はスキップされます。

3 システムがユーザーの割り当て内でプロトコルを処理できるリソースを見つけることができない場合、Horizon Client はユーザーにメッセージを返します。

重要： クライアントが URL リダイレクト機能を処理できるようにするには、ユーザーの Horizon Client を `URL_FILTERING_ENABLED=1` オプションを使用してインストールする必要があります。詳細については、VMware Horizon のドキュメントにある『Horizon リモート デスクトップ機能と GPO』ガイド内のオプションに関する情報を参照してください。

Workspace ONE Access に統合された環境でユーザーに対して URL リダイレクト機能が動作するには、ユーザーは Horizon Client を使用して少なくとも 1 つのアプリケーションを開いている必要があります。[クライアントで開く] オプションを使用して 1 つ以上のアプリケーションを開くと、ユーザーに割り当てられた URL リダイレクト設定がクライアント デバイスのレジストリ（Horizon Client はここで設定の値を取得できる）にロードされます。

[割り当て] ページで [オフラインにする] ボタンを使用してカスタマイズ割り当てを非アクティブにすることができます。ユーザーには、URL リダイレクト設定に対して複数のアクティブなカスタマイズを割り当てることができます。異なるアクティブな設定のルール間の潜在的な競合を回避するには、ユーザーが Horizon Client にログインすると、システムは次のように動作します。

- ユーザーがアクティブな割り当て済み設定を複数持っている場合でも、1 つの設定のみを有効にします。
- アルファベット順の最初の URL リダイレクト設定を、ユーザーに対する有効な設定として使用します。

前提条件

コンソールで、Horizon Cloud インベントリ内でデスクトップまたはリモート アプリケーションがない場合でも、URL リダイレクトのカスタマイズを作成することができます。ただし、このカスタマイズで指定されたエンド ユーザーに対して URL リダイレクト フローが機能するには、次の前提条件を満たす必要があります。

- [Marketplace からの仮想マシンのインポート] ワークフローを使用してイメージ仮想マシンが作成されたときに、[URL リダイレクト] という名前の Horizon Agent 機能が [はい] に設定されていること。
- Horizon Cloud インベントリに、構成で使用するデスクトップとリモート アプリケーションがあること。
- カスタマイズで [厳密な一致] が [はい] に設定されている場合、そのカスタマイズで指定されたエンド ユーザーに特定のデスクトップおよびリモート アプリケーションを付与する割り当てが存在すること。

手順

1 [割り当て] ページで、[新規] をクリックします。

2 [新しい割り当て] ウィンドウで、[カスタマイズ] アイコンをクリックします。

[新しいカスタマイズ割り当て] ウィザードが開いて最初のステップが表示されます。

3 選択を行ってから、次の手順に進みます。

オプション	説明
割り当ての名前	この割り当てにわかりやすい名前を入力します。
場所	使用するポッドの場所を選択します。

オプション	説明
ポッド	ポッドを選択します。このポッドは、セッション デスクトップとリモート アプリケーションが提供されるポッドです。
説明	オプションで、構成の説明を入力します。

4 [ソース] については、この構成が Horizon Client にクライアント システム上でインターセプトするよう指示する URL パターンのリストを作成します。

a [URL パターン] フィールドに、インターセプトする URL 一致パターンを指定する文字列を入力します。

ワイルドカードを使用して、複数の URL に一致する URL パターンを指定できます。

次に例を示します。

- `google.*` と入力すると、テキスト `google` を含むすべての URL がインターセプトされます。
- `.*`（ピリオド アスタリスク）を入力すると、すべてのプロトコル スキーム（すべてに一致）のすべての URL がインターセプトされます。
- `mailto://.*.example.com` と入力すると、テキスト `mailto://.*.example.com` を含むすべての URL がインターセプトされます。

重要： [URL のパターン] フィールドに入力する URL は、`docs.vmware.com` のようにホスト名の部分を含めて大文字と小文字が区別されることに注意してください。URL リダイレクト機能の動作は、ここに入力する URL パターンの大文字と小文字を識別します。たとえば、パターンとして `DOCS.VMWARE.COM/*` を入力し、エンド ユーザーが `https://docs.vmware.com` リンクをクリックしても、実際に存在するホスト名が小文字のため、URL リダイレクトは発生しません。ホスト名は小文字で入力してください。URL パスのサブディレクトリを一致させる必要がある場合は、ワイルドカードを使用するか、`docs.vmware.com/en/VMware-Horizon-Cloud-Service/*` のように実際に存在するとおりにパスを入力します。

b 指定した URL パターンをリストに追加するには、Enter キーを押します。

c パターンで入力して Enter キーを押して URL 一致パターンを追加するという手順を繰り返します。

5 ルールについては、どのターゲット インベントリ リソースが各種プロトコルを処理するかを決定するハンドラのセットを定義します。

ハンドラは、ユーザーが使用資格を持つどのデスクトップまたはアプリケーションが特定のプロトコルを処理するかを定義します。たとえば、ユーザーが `mailto` ハイパーテキスト リンクを持つ Microsoft Word ドキュメントを開き、ドキュメント内でそのリンクをクリックすると、ハンドラは、Microsoft Outlook や Mozilla Thunderbird など、資格のあるどのアプリケーションが要求を処理するかを決定します。

a ルールの設定を行います。

オプション	説明
スキーム	このハンドラが適用される `http`、`https`、`mailto`、`callto` などのプロトコルを入力します。
リソース タイプ	デスクトップまたはアプリケーションのどちらが指定したプロトコルを処理するかを選択します。
ターゲット リソース	[スキーム] フィールドで指定したプロトコルを処理する、インベントリのターゲット リソースの名前を入力します。
厳密な一致	[ターゲット リソース] フィールドで指定された名前と、ユーザーが使用できる資格のあるセッション デスクトップまたはリモート アプリケーションの名前との間で完全一致を強制するには [はい] を選択します。 システムでフォールバック動作を使用し、エンド ユーザーが [ターゲット リソース] フィールドに指定された名前と完全一致する名前のリソースの割り当てを持たない状況に対応できるようにするには、[いいえ] を選択します。 たとえば、[リソース タイプ] が [アプリケーション] に設定されていて、`mailto` プロトコルを処理するターゲット リソースとして Microsoft Outlook を指定したとします。ユーザーが Microsoft Outlook アプリケーションの割り当てを持っていない場合、[厳密な一致] が [いいえ] に設定されていると、システムは、`mailto` プロトコルを処理するためにそのユーザーに割り当てられた互換性のあるアプリケーション（Mozilla Thunderbird など）を検索します。

b さらにハンドラを追加するには、[行の追加] をクリックし、フィールドに入力します。

6 ウィザードの次の手順に進みます。

7 この割り当てのユーザーとグループを検索して選択してから、次の手順に移動します。

8 概要情報を確認し、ウィザードを完了します。

シングルポッド ブローカ - Horizon Cloud ポッドと URL コンテンツ リダイレクト機能

このドキュメント ページでは、Horizon Cloud on Microsoft Azure 環境での URL コンテンツ リダイレクト機能の仕組みについて説明します。URL コンテンツ リダイレクト機能を使用するには、シングルポッド仲介を使用するように環境を構成する必要があります。

簡単な紹介

リモート デスクトップまたはアプリケーションからクライアントへのリダイレクトは、エージェントからクライアントへのリダイレクトと呼ばれます。クライアントからリモート デスクトップまたはアプリケーションへのリダイレクトは、クライアントからエージェントへのリダイレクトと呼ばれます。

エージェントからクライアントへのリダイレクト

エージェントからクライアントへのリダイレクトでは、Horizon Agent は URL を Horizon Client に送信し、クライアント マシンで URL に指定されたプロトコルのデフォルト アプリケーションを開きます。エージェントからクライアントへのリダイレクトの構成の詳細については、このページの各セクションを参照してください。

クライアントからエージェントへのリダイレクト

クライアントからエージェントへのリダイレクトでは、システムは、ユーザーが指定したリモート デスクトップまたはアプリケーションを開いて URL を処理します。クライアントからエージェントへのリダイレクトの構成の詳細については、シングルポッド ブローカ - Horizon Cloud ポッド - URL リダイレクトのカスタマイズを作成し、ユーザーに割り当てるを参照してください。

一部の URL をリモート デスクトップまたはアプリケーションからクライアントにリダイレクトし、それ以外の URL をクライアントからリモート デスクトップまたはアプリケーションにリダイレクトできます。HTTP、HTTPS、mailto、および callto など、リダイレクトに必要なプロトコルをいくつでもリダイレクトできます。

エージェントからクライアントへのリダイレクトの構成

エージェントからクライアントへのリダイレクトを有効にするには、次の構成タスクを実行します。

- シングルポッド ブローカ - Horizon Cloud ポッド - URL リダイレクトのカスタマイズを作成し、ユーザーに割り当てるの前提条件セクションの説明に従って、イメージ仮想マシンの Horizon Agent で URL コンテンツ リダイレクト機能が有効になっていることを確認します。
- URL コンテンツ リダイレクトのグループ ポリシー設定をリモート デスクトップとアプリケーションに適用します。ADMX テンプレートを GPO に追加する方法については、次のセクションを参照してください。
- グループ ポリシー設定を構成して、Horizon Agent での URL のリダイレクト方法をプロトコルごとに示します。グループ ポリシー設定については、次のセクションを参照してください。

GPO への URL コンテンツ リダイレクト ADMX テンプレートの追加

URL コンテンツ リダイレクト ADMX テンプレート ファイル (`urlRedirection.admx`) には、URL リンクをクライアントで開く（エージェントからクライアントへのリダイレクト）か、リモート デスクトップまたはアプリケーションで開く（クライアントからエージェントへのリダイレクト）かどうかを制御できる設定が含まれています。

URL コンテンツ リダイレクト グループ ポリシー設定をリモート デスクトップおよびアプリケーションに適用するには、Active Directory サーバの GPO に ADMX テンプレート ファイルを追加します。リモート デスクトップやアプリケーションでクリックされる URL リンクに関するルールについては、仮想デスクトップおよび RDS ホストを含む組織単位 (OU) に GPO がリンクされる必要があります。

また、ユーザーの Windows クライアント コンピュータが含まれる組織単位 (OU) にリンクされている GPO にグループ ポリシー設定を適用することもできますが、クライアントからエージェントへのリダイレクトを構成するときに推奨されるのは、`vdmutil` コマンドライン ユーティリティを使用する方法です。macOS は GPO をサポートしていないため、Mac クライアントを使用している場合には、`vmdutil` を使用する必要があります。

前提条件

- Horizon Agent をイメージ仮想マシンにインストールするときは、シングルポッド ブローカ - Horizon Cloud ポッド - URL リダイレクトのカスタマイズを作成し、ユーザーに割り当てるの説明に従って URL コンテンツ リダイレクト機能が含まれていることを確認します。
- URL コンテンツ リダイレクトのグループ ポリシー設定用に Active Directory GPO が作成されていることを確認します。
- MMC およびグループ ポリシー管理エディタ スナップインが Active Directory サーバで使用できることを確認します。

手順

1 VMware Horizon Service のダウンロード の VMware Customer Connect から `Horizon GPO` バンドル をダウンロードします。

その URL から、Horizon Cloud Service on Microsoft Azure ダウンロードの場所に移動します。このページには、ダウンロード可能な項目のリストが表示されます。`Horizon GPO` バンドルという名前のエントリを見つけて、その ZIP ファイルをダウンロードします。Horizon 関連コンポーネントのグループ ポリシー設定を提供するすべての ADMX ファイルは、このファイルにあります。

2 ZIP ファイルを解凍して、次のファイルを Active Directory サーバの指定された場所にコピーします。

a `urlRedirection.admx` ファイルを `C:\Windows\PolicyDefinitions` フォルダにコピーします。

b 言語リソース ファイル `urlRedirection.adml` を `C:\Windows\PolicyDefinitions` 内の適切なサブフォルダにコピーします。

たとえば、EN（英語）の場合、`urlRedirection.adml` ファイルを `C:\Windows\PolicyDefinitions\en-US` フォルダにコピーします。

3 Active Directory サーバで、[グループ ポリシー管理エディタ] を開きます。

URL コンテンツ リダイレクトのグループ ポリシー設定は、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware Horizon URL リダイレクト] にインストールされます。

次に、Active Directory サーバのグループ ポリシー設定を構成します。グループ ポリシー設定については、次のセクションを参照してください。

URL コンテンツ リダイレクトのグループ ポリシー設定

URL コンテンツ リダイレクトのテンプレート ファイルには、Horizon Cloud 環境におけるエージェントからクライアントへのリダイレクト機能を設定するためのルールを作成するグループ ポリシー設定が含まれています。このテンプレート ファイルには、コンピュータの構成設定のみが含まれます。設定はすべて、グループ ポリシー管理エディタの [VMware Horizon URL リダイレクト] フォルダにあります。

重要： Horizon Cloud で、URL コンテンツ リダイレクトのテンプレート ファイルにクライアントからエージェントへのリダイレクトに関連するグループ ポリシー設定が含まれていても、クライアントからエージェントへのリダイレクトの構成にはグループ ポリシー設定を使用しません。代わりに、Horizon Universal Console を使用してクライアントからエージェントへのリダイレクトのルールを作成します。コンソールで URL リダイレクトの割り当てを作成するときに、クライアントからエージェントへのリダイレクトのルールを作成します。詳細な手順についてはシングルポッド ブローカ - Horizon Cloud ポッド - URL リダイレクトのカスタマイズを作成し、ユーザーに割り当てるを参照してください。

次の表に、URL コンテンツ リダイレクトのテンプレート ファイルで使用可能なグループ ポリシー設定の説明を記載します。

表 6-4. URL コンテンツ リダイレクトのグループ ポリシー設定

設定	プロパティ
`IE Policy: Prevent users from changing URL Redirection plugin loading behavior`	ユーザーが URL コンテンツ リダイレクト機能を無効にできるかどうかを決定します。 デフォルトでは、この設定は構成されていません。
`IE Policy: Automatically enable URL Redirection plugin`	新しくインストールされた Internet Explorer プラグインを自動的に有効にするかどうかを決定します。 デフォルトでは、この設定は構成されていません。
`Url Redirection Enabled`	URL コンテンツ リダイレクト機能を有効にするかどうかを決定します。この機能をクライアントまたはエージェントにインストールしている場合でも、この設定を使用して URL コンテンツ リダイレクト機能を無効にできます。 デフォルトでは、この設定は構成されていません。

表 6-4. URL コンテンツ リダイレクトのグループ ポリシー設定 （続き）

設定	プロパティ
`Url Redirection Protocol 'http'`	HTTP プロトコルを使用するすべての URL について、リダイレクトする URL を指定します。この設定には次のオプションがあります。 ■ [ブローカ ホスト名] - URL をリモート デスクトップまたはアプリケーションにリダイレクトするときに使用する Connection Server ホストの IP アドレスまたは完全修飾名。 ■ [リモート項目] - [エージェント ルール] で指定された URL を処理できるリモート デスクトップまたはアプリケーション プールの表示名。 ■ [クライアント ルール] - クライアントにリダイレクトする必要がある URL。たとえば、[クライアント ルール] を **`.*.mycompany.com`** に設定している場合、「`mycompany.com`」というテキストを含むすべての URL は、Windows ベースのクライアントにリダイレクトされ、クライアントのデフォルト ブラウザで開かれます。 ■ [エージェント ルール] - [リモート項目] で指定されるリモート デスクトップまたはアプリケーションにリダイレクトする必要がある URL。たとえば、[エージェント ルール] を **`.*.mycompany.com`** に設定している場合、「`mycompany.com`」というテキストが含まれるすべての URL がリモート デスクトップまたはアプリケーションにリダイレクトされます。 エージェント ルールを作成するときは、[ブローカ ホスト名]オプションを使用して Connection Server ホストの IP アドレスまたは完全修飾ドメイン名を指定し、[リモート項目] オプションを使用してデスクトップまたはアプリケーション プールの表示名を指定する必要があります。 **注：** クライアント ルールを構成する場合には、`vdmutil` コマンドライン ユーティリティを使用することをお勧めします。 デフォルトでは、この設定は有効になっています。
`Url Redirection Protocol '[...]'`	HTTP 以外のプロトコル（HTTPS、mailto、および callto など）にこの設定を使用します。 このオプションは、`Url Redirection Protocol 'http'` の場合と同じです。 その他のプロトコルを構成する必要がない場合は、URL コンテンツ リダイレクトのテンプレート ファイルを Active Directory に追加する前に、このエントリを削除またはコメント アウトできます。 ベスト プラクティスとして、HTTP および HTTPS プロトコルに対して同じリダイレクト設定を構成します。この方法では、ユーザーが `mycompany.com` などの部分的な URL を Internet Explorer に入力し、そのサイトが自動的に HTTP から HTTPS にリダイレクトされると、URL コンテンツ リダイレクト機能が期待どおりに動作します。この例では、HTTPS のルールを設定していても、HTTP に対して同じリダイレクト設定を設定していない場合、ユーザーが入力する部分的な URL はリダイレクトされません。 デフォルトでは、この設定は構成されていません。

Microsoft Azure での Horizon Cloud ポッドの公開イメージの管理

イメージを公開した後、Horizon Universal Console を使用してそのイメージを管理できます。公開されたイメージは Horizon Cloud のシーリング プロセスを正常に完了したイメージで、Horizon Cloud はそれを RDS ファーム（RDSH 対応のイメージの場合）または VDI デスクトップのプロビジョニングに使用できます。これらのイメー

ジを説明するために使用される他の用語として、シールドされたイメージや、割り当て可能なイメージなどがあります。イメージのシーリングは、デスクトップへのイメージの公開やイメージの変換とも呼ばれることがあります。

Microsoft Azure の Horizon Cloud ポッドから発行されたイメージに対して実行できるアクション

イメージを公開した後、Horizon Universal Console を使用してそのイメージを管理できます。公開されたイメージは Horizon Cloud のシーリング プロセスを正常に完了したイメージであり、Horizon Cloud はそれを使用して、RDSH ファーム内の RDSH 仮想マシン（RDSH 対応イメージの場合）または VDI デスクトップ仮想マシンをプロビジョニングできます。これらのイメージを説明するために使用される他の用語として、シールドされたイメージや、割り当て可能なイメージなどがあります。イメージがシールドされている場合、コンソールにはそのイメージのステータスが「公開済み」として表示されます。

ヒント: 第 1 世代テナント - 第 1 世代 Horizon Universal Console のツアーに記載されているように、クラウドベースのコンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。機能へのアクセスは、クラウドに接続されたポッドがポッドの最新レベルのソフトウェアを実行しているかどうか、機能がクラウド プレーンのテナント レコードで設定された特定のオプションに基づいているかどうかなどの要因によって異なります。ポッドのフリートまたはテナント 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、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。これは、コンソールに表示されるラベルが、ここで説明しているものとは少し異なる場合があることを意味します。使用したい機能が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て、お持ちのテナント 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。

コンソールは非常に動的なので、環境に応じてコンソールには異なるラベルが表示されることがあります。

手順

1 [インベントリ] をクリックして、操作対象のイメージがあるイメージ関連のページに移動します。

2 そのイメージに対応するチェック ボックスをクリックします。

3 イメージに対してアクションを実行するには、イメージのチェック ボックスを選択し、いずれかのアクション ボタンをクリックします。

ボタン	説明
名前の変更	**注：** このページには、Microsoft Azure にデプロイされたポッドのイメージで現在サポートされていないために「非アクティブ」状態である [Rename] という名前のアクションが含まれています。
複製	複製ワークフローは通常、イメージ仮想マシンでのアプリケーションのインストールや更新など、ファームまたは VDI デスクトップ割り当ての基盤となるゴールド イメージを更新するときに使用されます。既存のイメージを複製して、同じ構成を使用した新しい名前のイメージを作成することができます。 ファームおよび VDI デスクトップ割り当てに使用されるイメージを変更する手順の詳細については、Horizon Cloud でのファームに使用されるイメージの変更および VDI デスクトップ割り当てに使用されるイメージの変更を参照してください。 [複製] をクリックするときには、新しい複製された仮想マシンの名前を入力する必要があります。新しい名前を入力して [保存] をクリックした後、システムは新しい基本仮想マシンを作成するためにシールドされたイメージの仮想マシンのクローンを作成し、[インポートされた仮想マシン] ページに新しい仮想マシンを表示します。[インポートされた仮想マシン] ページに新しい仮想マシンのエージェントがアクティブであることが表示されたら、ログインして変更を加えることができます。変更を完了したら、複製を公開して、割り当て可能な（シールドされた）イメージにします。 **注：** システムでクローン作成のプロセスが開始すると、元のシールドされたイメージは、プロセスの最初の部分で移行中ステータスになります。しばらくすると、元のシールドされたイメージは元の状態に戻ります。[インポートされた仮想マシン] ページまたは [アクティビティ] ページを使用して、複製イメージの進行状況を監視できます。
エージェントのアップデート	イメージのエージェントに関連するソフトウェア コンポーネントをより新しいバージョンにアップデートします。このボタンをクリックすると、[エージェントのアップデート] ウィザードが開きます。 エージェントのアップデートがイメージに対して利用可能な場合、イメージの名前の横に青いドットが表示されます。その青いドットの上にカーソルを置くと、そのイメージで使用可能なエージェントのアップデートがポップアップにすべて示されます。 詳細については、次のいずれかのトピックを参照してください。 ■ Horizon Cloud の RDSH イメージのエージェント ソフトウェアをアップデートする ■ Horizon Cloud ポッド - フローティング VDI デスクトップ割り当てによって使用されるイメージのエージェント ソフトウェアを更新する **重要：** 専用 VDI デスクトップ割り当ての場合、通常はイメージ内のエージェントを更新するのではなく [割り当て] ページからエージェントを更新します。専用 VDI デスクトップ割り当て用のエージェント ソフトウェアを更新するを参照してください。

その他の実行可能なアクションのいずれかを実行するには、[詳細] をクリックして、適切なオプションを選択します。

注： イメージが選択されるときに [ブートス トラップのダウンロード] および [パスワードの更新] のアクションが表示されても、これらのアクションはどのイメージにも適用されません。

ドロップダウン オプション	説明
削除	選択したイメージを完全に削除します。 **注：** ファームなどでイメージが使用中であることをシステムが検出した場合、イメージを削除することはできません。
公開	ファームまたは VDI デスクトップ割り当てに使用されるイメージの場合、このアクションは複製されたイメージを再公開し、再度割り当て可能にします。イメージがすでに割り当て可能（シールド済み）である場合は、このアクションは使用できません。割り当て可能なイメージとは、ステータスが公開済みのイメージです。
デスクトップへの変換	このアクションは、公開ワークフローに失敗し、「公開済み」ステータスに達していないイメージに対してのみ使用します。このアクションを使用すると、公開済みのイメージがシールド前の仮想マシンに変換されます。シールド前の仮想マシンは、その時点で [インポートされた仮想マシン] ページに一覧表示されます。 **注意：** このアクションは頻繁に使用しないでください。このアクションを同じイメージで繰り返し使用すると、予期しない結果が発生し、イメージを再公開しようとするときにイメージのシールドに失敗することがあります。たとえば、新しいイメージを作成し、そのイメージで [公開] を実行して「公開済み」ステータスに到達してから、[デスクトップへの変換] を実行し、再度 [公開] を実行すると、公開ワークフローで発生する Sysprep プロセスが失敗することがあります。再度イメージをシールド前のイメージに変換すると、その時点以降、イメージは常に公開ワークフローに失敗する可能性があります。その場合は、操作をやり直し、新しい基本イメージを作成することが賢明です。
イメージの割り当て	コンソールにこのアクションが表示されていても、このアクションは Microsoft Azure 環境のイメージには使用されません。その結果、アクションにアクセスできなくなります。
イメージの一括割り当て	このオプションは、シングルポッド仲介用に構成された環境でのみ使用できます。Microsoft Azure のポッドに対して Universal Broker を使用するように環境が構成されている場合、このアクションは現在その構成でサポートされていないため、無効になっています。 直接の親イメージ（選択されたイメージが複製または更新されたイメージ）に基づく複数の割り当てまたはファームにイメージを割り当てます。 [イメージの一括割り当て] ダイアログ ボックスで、リストから割り当てとファームを選択し、[更新] をクリックします。 **注：** シングルポッド仲介用に構成された環境では、このオプションは、[複製]操作を使用して作成されたイメージ、およびエージェントの[更新操作]を使用して新しいバージョンのエージェントに更新されたイメージでのみ使用できます。

4 （オプション） イメージの詳細を表示するには、イメージの名前をクリックします。

画面には、イメージの詳細ページと、その詳細ページからイメージに対して実行できるアクションのボタンも表示されます。

たとえば、この画面には `lawin2016` という RDS 対応の割り当て可能なサーバ イメージの情報が表示されています。このイメージは `lakjun30` という名前のポッドに属し、2 つの RDSH ファームによって参照されています。

Horizon Cloud でのファームに使用されるイメージの変更

最初の RDSH 対応イメージを公開し、それを使用してファームを作成したら、そのイメージを変更し、そのイメージを使用しているすべてのファームに変更をプッシュできます。通常、すでに公開されているイメージを更新するのは、追加のサードパーティ アプリケーションやその他の機能をインストールするためです。このワークフローは、Horizon Universal Console で開始します。

注： Horizon Cloud エージェント関連のコンポーネントを更新する RDSH 対応イメージを変更している場合は、別の手順を使用します。Horizon Cloud の RDSH イメージのエージェント ソフトウェアをアップデートするを参照してください。

概要レベルでは、使用中のイメージを更新するワークフローは次のとおりです。

1 既存のイメージを複製して、同じ構成を使用した新しい名前のイメージを作成します。複製プロセスでは、システムはシールドされたイメージの仮想マシン (VM) のクローンを作成して新しい未公開のゴールド イメージの仮想マシンを作成し、[インポートされた仮想マシン] ページに新しい仮想マシンをリストします。

2 [インポートされた仮想マシン] ページに新しい仮想マシンのエージェントがアクティブであることが報告されたら、仮想マシンにログインして、その複製された仮想マシンに対して必要な変更を行います。

3 [イメージに変換] を使用して複製された仮想マシンを公開し、割り当て可能な（シールドされた）イメージにします。

4 元のイメージを使用しているファームを編集し、元のイメージの代わりに新しく更新された複製イメージを使用します。

前提条件

イメージにログインして更新するには、ローカル管理者アカウント認証情報があることを確認します。この管理者アカウントは、[新しいイメージ] ワークフローを使用してイメージを公開するために使用したものと同じです。構成済みイメージ仮想マシンを Horizon Cloud の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。

注： Microsoft リモート デスクトップ クライアントを RDP ソフトウェアとして使用して仮想マシンに接続する場合は、それが最新のバージョンであることを確認してください。たとえば、Windows 7 オペレーティング システムのデフォルトの RDP ソフトウェアのバージョンはこの条件を満たしていません。バージョンは、バージョン 8 以降である必要があります。

手順

1 [インベントリ] をクリックして、イメージが表示されているイメージ関連のページに移動します。

2 イメージのチェックボックスをオンにして、[複製] をクリックします。

ダイアログ ボックスに、複製イメージの名前を入力します。新しい名前を入力して [保存] をクリックした後、システムは新しいイメージ仮想マシンを作成するためにシールドされたイメージの仮想マシンのクローンを作成し、[インポートされた仮想マシン] ページに新しい仮想マシンを表示します。

注： システムでクローン作成のプロセスが開始すると、元のシールドされたイメージは、プロセスの最初の部分で移行中ステータスになります。しばらくすると、元のシールドされたイメージは元の状態に戻ります。

3 [インベントリ] - [インポートされた仮想マシン] に移動し、[インポートされた仮想マシン] ページに新しい仮想マシンのエージェントがアクティブであることがいつ報告されるかを確認します。

4 新しい仮想マシンのエージェントがアクティブであることが [インポートされた仮想マシン] ページに表示されたら、仮想マシンの IP アドレスと RDP ソフトウェアを使用して RDSH 対応の Windows オペレーティング システムに接続します。

- 元のイメージがパブリック IP アドレスを使用して作成された場合、新しい複製された仮想マシンにはパブリック IP アドレスがあり、その IP アドレスを RDP ソフトウェアで使用できます。
- 元のイメージがパブリック IP アドレスを使用して作成されていない場合、新しい複製された仮想マシンには、Microsoft Azure クラウド環境のプライベート IP アドレスがあり、次の 2 つの方法のいずれかを使用して仮想マシンに対して RDP を実行する必要があります。
  - パブリック IP アドレスを持つ Microsoft Azure サブスクリプション内で別の仮想マシンを使用し、仮想マシンに対してアウトバウンド RDP を実行する。
  - VPN と RDP を企業のネットワーク経由で仮想マシン内で使用する

5 イメージが作成されたときに [イメージのインポート] ウィザードで指定されたユーザー名とパスワードを使用して、Windows オペレーティング システムにログインします。

ローカルの管理者名を使用している場合は、`\username` の形式でユーザー名を入力します。

6 Windows オペレーティング システムで、目的の更新を実行します。

追加のサードパーティ アプリケーションをインストールする場合は、Microsoft Windows Server オペレーティング システムを搭載した Horizon Cloud のインポートされた仮想マシンの場合:組織のニーズに合わせた仮想マシンのカスタマイズに記載されている手順を参照してください。

7 [インポートされた仮想マシン] ページに戻り、複製された仮想マシンのチェックボックスをオンにして、[詳細] - [イメージに変換] をクリックします。

システムは、標準の公開プロセスを通じて、複製および更新されたイメージを取得します。イメージは、このプロセスの開始時に表示されていたイメージ関連のページに表示されます。公開プロセスが完了すると、イメージが「公開済み」ステータスで表示されます。

8 複製および更新されたイメージのステータスが「公開済み」の場合、元のイメージを使用している各ファームを更新して、代わりに新しい複製イメージを使用します。このイメージには変更が反映されています。

各ファームの詳細ページで、[全般設定] の [編集] リンクをクリックしてウィンドウを開き、新しい複製イメージを選択して保存します。

結果

更新するファームは、更新されたイメージを使用して RDSH インスタンスを自動的に削除して再作成します。

次のステップ

元のイメージを使用しているファームを更新済みで、組織で元のイメージが不要になったと判断できる場合は、コンソールを使用して元のイメージを削除できます。組織内の他の管理者が、低いレベルのソフトウェアを持つイメージを使用しないようにするために、元のイメージを削除することはベスト プラクティスです。

VDI デスクトップ割り当てに使用されるイメージの変更

イメージを公開し、それを使用して VDI デスクトップ割り当てを作成したら、そのイメージを変更し、そのイメージを使用しているすべての VDI デスクトップ割り当てに変更をプッシュできます。通常、すでに公開されているイメージを更新するのは、追加のサードパーティ アプリケーションやその他の機能をインストールするためです。このワークフローは、Horizon Universal Console で開始します。

注： Horizon Cloud エージェント関連のコンポーネントを更新するためのイメージを変更している場合は、別の手順を使用します。Horizon Cloud ポッド - VDI デスクトップ割り当て、ファーム、公開イメージ、ベース仮想マシンにインストールされたエージェント関連ソフトウェアの更新 とそのサブトピックを参照してください。

概要レベルでは、使用中のイメージを更新するワークフローは次のとおりです。

1 既存のイメージを複製して、同じ構成を使用した新しい名前のイメージを作成します。複製プロセスでは、システムはシールドされたイメージの仮想マシン (VM) のクローンを作成して新しい未公開のゴールド イメージの仮想マシンを作成し、[インポートされた仮想マシン] ページに新しい仮想マシンをリストします。

2 [インポートされた仮想マシン] ページに新しい仮想マシンのエージェントがアクティブであることが報告されたら、仮想マシンにログインして、その複製された仮想マシンに対して必要な変更を行います。

3 [イメージに変換] を使用して複製された仮想マシンを公開し、割り当て可能な（シールドされた）イメージにします。

4 元のイメージを使用している VDI デスクトップ割り当てを編集して、元のイメージの代わりに新しく更新された複製イメージを使用します。

前提条件

イメージにログインして更新するには、ローカル管理者アカウント認証情報があることを確認します。この管理者アカウントは、[新しいイメージ] ワークフローを使用してイメージを公開するために使用したものと同じです。構成済みイメージ仮想マシンを Horizon Cloud の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。

注： Microsoft リモート デスクトップ クライアントを RDP ソフトウェアとして使用して仮想マシンに接続する場合は、それが最新のバージョンであることを確認してください。たとえば、Windows 7 オペレーティング システムのデフォルトの RDP ソフトウェアのバージョンはこの条件を満たしていません。バージョンは、バージョン 8 以降である必要があります。

手順

1 [インベントリ] をクリックして、イメージが表示されているイメージ関連のページに移動します。

2 イメージのチェックボックスをオンにして、[複製] をクリックします。

ダイアログ ボックスに、複製イメージの名前を入力します。新しい名前を入力して [保存] をクリックした後、システムは新しいイメージ仮想マシンを作成するためにシールドされたイメージの仮想マシンのクローンを作成し、[インポートされた仮想マシン] ページに新しい仮想マシンを表示します。

注： システムでクローン作成のプロセスが開始すると、元のシールドされたイメージは、プロセスの最初の部分で移行中ステータスになります。しばらくすると、元のシールドされたイメージは元の状態に戻ります。

3 [インベントリ] - [インポートされた仮想マシン] に移動し、[インポートされた仮想マシン] ページに新しい仮想マシンのエージェントがアクティブであることがいつ報告されるかを確認します。

4 新しい仮想マシンのエージェントがアクティブであることが [インポートされた仮想マシン] ページに表示されたら、仮想マシンの IP アドレスと RDP ソフトウェアを使用して Windows オペレーティング システムに接続します。

- 元のイメージがパブリック IP アドレスを使用して作成された場合、新しい複製された仮想マシンにはパブリック IP アドレスがあり、その IP アドレスを RDP ソフトウェアで使用できます。
- 元のイメージがパブリック IP アドレスを使用して作成されていない場合、新しい複製された仮想マシンには、Microsoft Azure クラウド環境のプライベート IP アドレスがあり、次の 2 つの方法のいずれかを使用して仮想マシンに対して RDP を実行する必要があります。
  - パブリック IP アドレスを持つ Microsoft Azure サブスクリプション内で別の仮想マシンを使用し、仮想マシンに対してアウトバウンド RDP を実行する。
  - VPN と RDP を企業のネットワーク経由で仮想マシン内で使用する

5 イメージが作成されたときに [イメージのインポート] ウィザードで指定されたユーザー名とパスワードを使用して、Windows オペレーティング システムにログインします。

ローカルの管理者名を使用している場合は、`\username` の形式でユーザー名を入力します。

6 Windows オペレーティング システムで、目的の更新を実行します。

追加のサードパーティ アプリケーションをインストールする場合は、Microsoft Windows クライアント オペレーティング システムを搭載した Horizon Cloud のインポートされた仮想マシンの場合：組織のニーズに合わせた仮想マシンのカスタマイズに記載されている手順を参照してください。

7 [インポートされた仮想マシン] ページに戻り、複製された仮想マシンのチェックボックスをオンにして、[詳細] - [イメージに変換] をクリックします。

システムは、標準の公開プロセスを通じて、複製および更新されたイメージを取得します。イメージは、このプロセスの開始時に表示されていたイメージ関連のページに表示されます。公開プロセスが完了すると、イメージが「公開済み」ステータスで表示されます。

8 複製および更新されたイメージのステータスが「公開済み」の場合、元のイメージを使用している各 VDI デスクトップ割り当てを編集して、代わりに新しい複製イメージを使用します。このイメージには変更が反映されています。

結果

VDI デスクトップ割り当てを更新してそのイメージを変更すると次のようになります：

- 割り当て内で割り当て解除されたパワーオフ状態の仮想マシンが、新しいイメージを使用して自動的に再作成されます。
- パワーオンされたがアクティブなエンド ユーザー接続のない割り当て解除された仮想マシンは、新しいイメージを使用して自動的に再作成されます。
- 割り当て解除された仮想マシンがパワーオン状態で、フローティング VDI デスクトップ割り当てなど、アクティブなエンド ユーザー接続がある場合、エンド ユーザーがログオフすると仮想マシンは新しいイメージで自動的に更新されます。
- 専用 VDI デスクトップ割り当てなど、エンド ユーザーにマッピングされたデスクトップ仮想マシンは、新しいイメージに自動的に更新されません。このような割り当て済みのデスクトップ仮想マシンを更新して、代わりに新しい複製イメージを使用するには、そのデスクトップ仮想マシンを手動で割り当て解除する必要があります。次回システムがデスクトップ仮想マシンをパワーオンするときに、新しいイメージが適用されます。次に、そのデスクトップ仮想マシンを特定のエンド ユーザーに手動で再割り当てすることができます。

次のステップ

元のイメージを使用している VDI デスクトップ割り当てを更新済みで、組織で元のイメージが不要になったと判断できる場合は、コンソールを使用して元のイメージを削除できます。組織内の他の管理者が、低いレベルのソフトウェアを持つイメージを使用しないようにするために、元のイメージを削除することはベスト プラクティスです。

Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた割り当ての管理

Microsoft Azure の 1 つ以上のポッドからのリソースを使用する割り当てを作成したら、Horizon Universal Console を使用して割り当てを管理できます。Horizon Cloud テナント環境内の割り当てのタイプは、作成したものによって異なります。

ヒント: コンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。コンソールの割り当て関連ページに表示されるラベルは、テナントの設定済みのブローカ設定、フリート内のクラウド接続されたポッドのタイプ、テナントの地域別クラウド プレーン、および特定のライセンスに基づく機能などの要因によって異なります。

コンソールの割り当て関連のページから割り当てを操作します。割り当てで使用できるアクションのタイプは、割り当てのタイプと、そのタイプに対してそのアクションを使用できるかどうかによって異なります。たとえば、[エージェントの更新] アクションは専用 VDI デスクトップ割り当てのみに適用されますが、[削除] アクションはすべての割り当てのタイプで使用できます。割り当ての作成方法の詳細については、それぞれの手順を参照してください。通常（常にではありませんが）、あるアクションが一覧にある割り当てに適用されない場合、コンソールではそのアクションが非表示になります。

次の表は、さまざまな割り当てタイプを作成するための手順へのリンクを提供します。

割り当てのタイプ	手順
VDI デスクトップ	■ 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 Horizon Cloud ポッド - 第 1 世代環境での VDI マルチクラウド割り当ての作成と表示
セッションベースのデスクトップ	Horizon Cloud ポッド - RDS ベースのセッション デスクトップ割り当てを作成して、エンド ユーザーのために RDS ホストからのデスクトップ セッションを提供する
App Volumes アプリケーションの割り当て	Horizon Cloud：App Volumes 割り当ての作成
リモート アプリケーション	リモート アプリケーション - Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされたリモート アプリケーションのリモート アプリケーション割り当ての作成
URL リダイレクトのカスタマイズ	シングルポッド ブローカ - Horizon Cloud ポッド - URL リダイレクトのカスタマイズを作成し、ユーザーに割り当てるを参照してください。 **注：** Microsoft Azure のポッドで Universal Broker を使用するようにテナント環境が構成されている場合、URL リダイレクトのカスタマイズの使用は現在サポートされていません。

コンソールの [割り当て] 領域内のいずれかのページで表示されている操作対象割り当てを指定してからは、対応するチェックボックスを選択し、表示されるアクションで該当するものをクリックすると、その割り当てに対してアクションを開始できます。一部のボタンには、[詳細] アクションまたは [...] アクションでアクセスします。

注意: コンソールは動的であり、特定のユースケースに適したワークフローと、テナント環境の最新の状況を反映しているため、コンソール ページに表示されるアクション ボタンは、割り当てがリストされているページに特定のアクションが適切かどうかによって異なってきます。結果として、次に列挙するボタンは、割り当てに関連する特定のページで表示されない場合があります。表示されている場合でも、リストされている特定の割り当てでは機能しない場合があります。

[編集]

このボタンをクリックすると、割り当ての編集可能な設定を変更できるウィザードが起動します。起動されているウィザードには、変更できない設定の読み取り専用フィールドがあり、その割り当てタイプの作成ウィザードに似ています。フィールドの詳細な説明については、上記のドキュメント リンクで作成に関するトピックを参照してください。既存の専用またはフローティング VDI デスクトップ割り当てを編集して Microsoft Azure 仮想マシン モデルを変更する方法については、Microsoft Azure の 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の仮想マシン モデルの変更を参照してください。

割り当てのタイプによっては、[編集] ボタンを使用する代わりに、割り当ての名前をクリックして、割り当ての [サマリ] ページから設定を更新することもできます。

複製

このアクションを使用すると、選択したデスクトップ割り当てを複製して、仕様が同じで新しい名前の新しい割り当てを作成することができます。開かれるウィザードは、複製しているのと同じデスクトップ割り当てタイプの作成ウィザードと同じです。

[オフラインにする]

このアクションは、フローティング VDI デスクトップ割り当て、専用の VDI デスクトップ割り当て、および URL リダイレクトのカスタマイズ割り当てに適用されます。このボタンをクリックすると、割り当てをオフラインにするウィンドウが開きます。

割り当てをオフラインにするときのシステムの動作は、選択された割り当てのタイプによって異なります。

- アクティブな URL リダイレクトのカスタマイズ割り当ての場合、[オフラインにする] を使用して、割り当てで定義されている URL リダイレクトの動作をオフにします。
- VDI デスクトップ割り当ての場合、[オフラインにする] を使用して、受信する接続リクエストに影響する可能性があるメンテナンス アクションを実行するために割り当てをオフにします。VDI デスクトップ割り当てについて [オフラインにする] をクリックすると、システムは割り当てをオフライン モードに切り替え、ユーザーが割り当てのデスクトップにログインできないようにします。

  注： オフラインの割り当てではイメージの更新が開始されません。オフラインの割り当てを編集して更新されたイメージを使用できるようにできる場合でも、システムは割り当てがオンライン状態に戻るまで更新操作を開始しません。

エージェントのアップデート

[割り当て] ページでは、このアクションは専用の VDI デスクトップ割り当てにのみ適用されます。専用 VDI デスクトップ割り当て用のエージェント ソフトウェアを更新するを参照してください。

[オンラインにする]

このボタンをクリックすると、オフラインの割り当てをオンラインに戻すウィンドウが開きます。

[削除 (Delete)]、[削除 (Remove)]

コンソールでは、この 2 つのラベルのいずれかを使用して、このアクションを表示できます。このボタンを使用して、選択した割り当てを削除します。Horizon Cloud 環境からの割り当ての削除。

VDI デスクトップ割り当ての詳細ページ内で実行できるアクション

VDI デスクトップ割り当てでは、割り当ての詳細ページ内で、その割り当てタイプに固有のアクションを実行できます。これらの詳細ページを表示するには、コンソールの割り当てに関連するページでその割り当てを見つけ、名前をクリックします。最初に、[サマリ] ページが表示されます。

[サマリ] ページ

[サマリ] ページには、VDI デスクトップ割り当ての現在の設定が表示されます。コンソールでこのページから値を編集できる場合、編集関連のアイコンをクリックすると、既存の VDI デスクトップ割り当てについてシステムによって更新が許可されている設定を変更できます。VDI デスクトップ割り当てでは、ポッドなどの一部の設定は作成後に変更できません。

[デスクトップ] ページ

[デスクトップ] ページには、VDI デスクトップ割り当てにある既存のデスクトップ仮想マシンが表示されます。コンソールの動的な性質の結果として、表示され、クリックできるアクションは、デスクトップ仮想マシンの現在の状態と、割り当てがフローティング VDI デスクトップ割り当てか専用 VDI デスクトップ割り当てかによって異なってきます。例として、[エージェント ペアリングをリセット] アクションが、専用 VDI デスクトップ割り当てのデスクトップには提供されていても、フローティング VDI デスクトップ割り当てのデスクトップには提供されません。

- フローティング VDI デスクトップ割り当てのデスクトップに対しては、再起動したり、(デスクトップがパワーオンになっている場合) パワーオフしたりできます。現在接続されているユーザーがいる場合は、そのユーザーをログオフするか切断することもできます。

  注: フローティング VDI デスクトップ割り当てのデスクトップを手動で削除しないでください。システムの電源管理機能により、削除されたマシンの代わりとして新しいデスクトップ仮想マシンが自動的に作成されてしまいます。フローティング VDI デスクトップ割り当てでのデスクトップの数を調整する方法については、Horizon Cloud 環境での VDI デスクトップ割り当てのサイズ変更を参照してください。

- 専用 VDI デスクトップ割り当てのデスクトップに対しては、再起動したり、デスクトップの現在の状態に応じてパワーオンまたはパワーオフしたり、現在接続されているユーザーがいる場合にそのユーザーをログオフまたは切断したり、デスクトップが未割り当ての場合はデスクトップを特定のユーザーに割り当てたり、デスクトップがユーザーに割り当てられている場合はデスクトップの割り当てを解除したり、デスクトップがパワーオンされたがエージェントのステータスがアクティブとして表示されていない場合はエージェントのペアリングをリセットしたりすることができます。デスクトップの割り当てを解除すると、そのユーザーへのデスクトップのマッピングが削除され、別のユーザーにマッピングすることが可能になります。エージェントのペアリングをリセットすると、デスクトップ仮想マシンと Horizon Cloud のペアリング状態が修復されます。 デスクトップのエージェント更新に失敗した場合は、[ステータス] 列にビジュアル インジケータが表示されます。この問題が発生した場合は、ロールバック オプションを使用して、デスクトップを以前のエージェント ソフトウェアのバージョンに戻すことができます。警告アイコンにポインタを置くと、ロールバックの実行可能期間が表示されます。

  注: [デスクトップ] ページでアクションを行える場合でも、手動でデスクトップをパワーオンしないでください。デスクトップを手動でパワーオンすると、専用 VDI デスクトップ割り当てで設定されている電源管理設定と競合する可能性があります。デスクトップを手動でパワーオンした場合は、その他のデスクトップがパワーオフになる、予期しない結果が発生する可能性があります。デスクトップをパワーオンする代わりに、[再起動] アクションを使用します。

[システム アクティビティ] ページ

[システム アクティビティ] ページには、電源管理スケジュールを満たすようにデスクトップをパワーオフするなどの、システム アクションによるデスクトップ割り当て内のアクティビティが表示されます。[システム アクティビティ] ページでは、タスクをキャンセルしたり、レポートをエクスポートしたりできます。

- リストでタスクを選択して [タスクをキャンセル] ボタンをクリックすることによって、いくつかのタスクを完了する前にキャンセルすることができます。
  - キャンセルするタスクの選択を行う前に、ビューを更新して表示されているタスクのステータスを最新の状態にします。
  - タスクが現在、システムによってキャンセルできる状態になっている場合、そのキャンセル可能なタスクに対応しているチェック ボックスを選択できます。

次の表はキャンセルできるタスクを示しています。

タスク	タスクがキュー状態にあるときにキャンセル	タスクが実行状態にあるときにキャンセル
ファームの拡張	サポートされています **注：** システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。	サポートされています 次の点に注意してください。 ■ システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。 ■ 仮想マシンや OS/データ ディスクなど、すでに作成されているリソースは、タスクがキャンセルされると破棄されます。仮想マシンが破棄された場合または作成されていない場合、割り当てのサイズは変わります。 ■ このオプションは、マルチクラウドの割り当てでは使用できません。
割り当ての拡張	サポートされています **注：** システムによって、VDI デスクトップ割り当ての拡張タスクが自動的に作成され、割り当ての作成または更新が進行中である場合は、タスクをキャンセルできます。割り当ての作成/更新が終了した後、タスクをキャンセルすることはできません。	サポートされています 次の点に注意してください。 ■ システムによって RDSH ファームに対する拡張タスクが自動的に作成された場合は、そのタスクをキャンセルできるようになるには、ファームがオフラインになる必要があります。 ■ 仮想マシンや OS/データ ディスクなど、すでに作成されているリソースは、タスクがキャンセルされると破棄されます。仮想マシンが破棄された場合または作成されていない場合、割り当てのサイズは変わります。 ■ このオプションは、マルチクラウドの割り当てでは使用できません。
仮想マシンのイメージへの変換	サポートされています **注：** このタスクをキャンセルして再試行する場合は、まず仮想マシンが変換可能な状態であることを確認します。不明な場合は、仮想マシンをパワーオフしてからパワーオンします。	サポートされています **注：** このタスクをキャンセルして再試行する場合は、まず仮想マシンが変換可能な状態であることを確認します。不明な場合は、仮想マシンをパワーオフしてからパワーオンします。

- [レポートのエクスポート] 機能で、表示されている情報をレポート ファイルとしてエクスポートできます。

  レポートをエクスポートすると、[レポート] ページの [エクスポートされたレポート] タブに表示されます。ここから、レポートをダウンロードできます。詳細については、第 1 世代テナント - 第 1 世代 Horizon Universal Console の [レポート] ページを参照してください。

  エクスポートを開始するときに、すべてのデータをエクスポートするか、現在フィルタされているデータのみをエクスポートするかを選択できます。次に、レポートが生成中であることを示すメッセージがページの最上部に表示されます。[レポート] ページの [エクスポートされたレポート] タブで、レポートの進行状況を確認したり、エクスポートが完了したレポートをダウンロードできます。この準備はレコードの数に応じて数分間かかります。たとえば、50,000 レコードのレポートには、約 10 分かかります。

  注目: Microsoft Azure のポッドのいずれかが 2552 より前のマニフェストにある場合、より大きなレポートの処理は次のようになります。

  - エクスポートを開始すると、レポートがコンパイル中で、しばらく時間がかかることを知らせるメッセージが表示されます。この準備はレコードの数に応じて数分間かかります。たとえば、50,000 レコードのレポートには、約 10 分かかります。
  - 準備が完了すると、「**レポートが正常に生成されました**」というメッセージおよび [ダウンロード] ボタンが表示された別のダイアログボックスが表示されます。[ダウンロード] ボタンをクリックした後、このダイアログ ボックスを閉じる前にダウンロードが完了するまで待機する必要があります。ダウンロードが完了する前に閉じると、ダウンロードがキャンセルされます。

  このプロセスが完了するまでコンソールでその他のアクションを実行することはできないため、大量のアクティビティ レコードがある場合は、情報のエクスポートを、コンソールで他のタスクを実行するまでに最大 10 分ほど待つことができるときに計画する必要があります。

[ユーザー アクティビティ] ページ

[ユーザー アクティビティ] ページには、割り当てによって提供されるセッションのログインやログオフなど、ユーザー アクションによって発生する VDI デスクトップ割り当て内のアクティビティが表示されます。

[レポートのエクスポート] 機能で、表示されている情報をレポート ファイルとしてエクスポートできます。

レポートをエクスポートすると、[レポート] ページの [エクスポートされたレポート] タブに表示されます。ここから、レポートをダウンロードできます。詳細については、第 1 世代テナント - 第 1 世代 Horizon Universal Console の [レポート] ページを参照してください。

エクスポートを開始するときに、すべてのデータをエクスポートするか、現在フィルタされているデータのみをエクスポートするかを選択できます。次に、レポートが生成中であることを示すメッセージがページの最上部に表示されます。[レポート] ページの [エクスポートされたレポート] タブで、レポートの進行状況を確認したり、エクスポートが完了したレポートをダウンロードできます。この準備はレコードの数に応じて数分間かかります。たとえば、50,000 レコードのレポートには、約 10 分かかります。

注目: Microsoft Azure のポッドのいずれかが 2552 より前のマニフェストにある場合、より大きなレポートの処理は次のようになります。

- エクスポートを開始すると、レポートがコンパイル中で、しばらく時間がかかることを知らせるメッセージが表示されます。この準備はレコードの数に応じて数分間かかります。たとえば、50,000 レコードのレポートには、約 10 分かかります。
- 準備が完了すると、「**レポートが正常に生成されました**」というメッセージおよび [ダウンロード] ボタンが表示された別のダイアログボックスが表示されます。[ダウンロード] ボタンをクリックした後、このダイアログボックスを閉じる前にダウンロードが完了するまで待機する必要があります。ダウンロードが完了する前に閉じると、ダウンロードがキャンセルされます。

このプロセスが完了するまでコンソールでその他のアクションを実行することはできないため、大量のアクティビティ レコードがある場合は、情報のエクスポートを、コンソールで他のタスクを実行するまでに最大 10 分ほど待つことができるときに計画する必要があります。

Workspace ONE UEM を使用して Microsoft Azure の Horizon Cloud ポッド内の専用 VDI デスクトップを管理する

Workspace ONE UEM を使用して Windows 10 物理 PC を管理している場合は、それを使用して Horizon Cloud ポッド内の Windows 10 専用 VDI デスクトップを管理することもできます。このアプローチは、Windows 10 の物理および仮想デスクトップ全体で Day-2 の操作を標準化するのに役立ちます。

これらのタイプの専用 VDI デスクトップを Workspace ONE UEM に登録するには、コマンドライン登録を使用した Windows 10 のオンボーディング：VMware Workspace ONE 操作チュートリアルを参照してください。

重要： ユーザーが専用デスクトップにログインすると、Workspace ONE UEM はユーザーのデスクトップを登録します。その時点で、ユーザーのデスクトップの割り当てを解除するオプションが Horizon Universal Console で利用可能になります。

ただし、Horizon Universal Console を使用してユーザーのデスクトップの割り当てを解除しても、Horizon Cloud はそのデバイスを Workspace ONE UEM から削除しません。したがって、Workspace ONE UEM 管理コンソールにログインして、登録済みのデバイスを削除する必要があります。Workspace ONE UEM からデバイスを削除しない場合、そのデバイスは元のユーザーに登録されたままになり、デスクトップを別のユーザーに割り当てようとすると失敗します。

Horizon Cloud 環境で現在設定されている割り当ての表示

Horizon Universal Console の左側のナビゲーション バーにある [割り当て] を使用して、Horizon Cloud 環境で現在設定されているすべての割り当ての概要や詳細なビューを表示するさまざまなページに移動します。それぞれの割り当てをクリックして、個々の割り当ての詳細を表示することができます。一部の割り当てタイプでは、割り当

てのハイパーリンク名をクリックすると、その割り当てで使用される個々のアセットに対してアクションを実行できる場所に移動できます。

ヒント: コンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。コンソールの割り当て関連ページに表示されるラベルは、テナントの設定済みのブローカ設定、フリート内のクラウド接続されたポッドのタイプ、テナントの地域別クラウド プレーン、および特定のライセンスに基づく機能などの要因によって異なります。

割り当てのタイプ	説明
セッションベースのデスクトップ	デスクトップ割り当ての詳細を表示し、オプションで [編集] をクリックして特定のプロパティを更新します。 関連する RDSH ファームのリンクをクリックすると、個々のデスクトップ セッション、ファーム内のシステムおよびユーザーのアクティビティに関する情報に移動して、ファームの RDSH 仮想マシンに対するアクションを実行できます。
リモート アプリケーション	リモート アプリケーションの詳細を表示し、オプションで [編集] をクリックして特定のプロパティを更新します。 関連する RDSH ファームのリンクをクリックすると、個々のセッション、ファーム内のシステムおよびユーザーのアクティビティに関する情報に移動して、ファームの RDSH 仮想マシンに対するアクションを実行できます。
App Volumes アプリケーション	App Volumes アプリケーションの詳細を表示し、必要に応じて使用可能なアクションを実行して特定のプロパティを更新します。
URL リダイレクトのカスタマイズ	カスタマイズの詳細を表示し、オプションで [編集] をクリックして特定のプロパティを更新します。
VDI デスクトップ	デスクトップ割り当ての詳細を表示し、[デスクトップ]、[システム アクティビティ]、または [ユーザー アクティビティ] の順にクリックして、これらの各ページの情報を表示したり、仮想デスクトップを操作したりします。 ■ [サマリ] ページには、割り当て、デスクトップの作成元のイメージの名前、割り当てられたユーザーのリストについての定義情報が表示されます。 ■ [デスクトップ] ページには、デスクトップ割り当ての一部として作成された個々のデスクトップについての情報が表示されます。個別のデスクトップで、その現在の状態に応じて、アクションを実行することもできます。 また、[デスクトップ] ページを使用して、デスクトップ割り当て内の個々のデスクトップを管理することもできます。 ■ [システム アクティビティ] および [ユーザー アクティビティ] ページには、指定した時間内の割り当てに関するアクティビティ情報が表示されます。 **注:** この VDI デスクトップ割り当てが、ポッドのマニフェスト バージョンが 1101 よりも小さい Microsoft Azure のポッドで作成された場合、割り当てによって Windows クライアント ライセンスがこの割り当てに使用されたイメージから継承されているにもかかわらず [ライセンス タイプ] フィールドには [ライセンスがありません] と表示されます。[編集] リンクをクリックすると、編集ウィンドウには Windows クライアント ライセンスが使用されていることが表示されます。

Horizon Cloud 環境での割り当ての編集

Horizon Universal Console を使用して、Horizon Cloud 環境内の割り当てを編集できます。[割り当て] をクリックして、変更する割り当てを特定するための適切なページに移動します。変更できるプロパティは、割り当てのタイプによって異なります。

重要： App Volumes の割り当てを編集する前に、Microsoft Azure のすべてのポッドが良好な状態であることを確認します。App Volumes の割り当てはテナントレベルのリソースであるため、変更はすべてのポッドに伝達されます。この場合、いずれかのポッドが非健全な状態になると、割り当てがエラー状態になる可能性があります。

手順

1 コンソールで、[割り当て] をクリックします。

2 変更する割り当てのタイプに対応するページを選択します。

3 編集する割り当ての横のチェック ボックスを選択して、[編集] をクリックします。

対応する割り当てタイプのウィザードが表示されます。

4 ウィザードの指示に従って変更を行い、[送信] をクリックします。

ウィザードのフィールドに入力する手順については、編集する割り当てのタイプを作成する方法を説明するドキュメント トピックを参照してください。これらのトピックは、Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた割り当ての管理 に一覧表示されています。

Horizon Cloud 環境からの割り当ての削除

不要になった割り当てを削除できます。Horizon Universal Console で、[割り当て] をクリックし、表示されるオプションを使用して、削除する割り当てが表示されている該当する割り当てページに移動し、その割り当てを特定します。その後、その特定の割り当てページで使用可能なアクションに応じて、[削除 (Remove)] アクションまたは [削除 (Delete)] アクションを使用して、その割り当てを削除します。[削除] アクションは、通常、[詳細] メニューにあります（[詳細] - [削除]）。

ご利用の環境から割り当てを削除するための固有の手順は、割り当てのタイプによって異なります。次の表は、割り当てが一覧表示されている該当するコンソール ページに既に移動している場合に、割り当てで実行する手順を示しています。

ヒント: コンソールは動的であり、Horizon Cloud テナント環境の最新の状況に適したワークフローと設定が反映されます。コンソールの割り当て関連ページに表示されるラベルは、テナントの設定済みのブローカ設定、フリート内のクラウド接続されたポッドのタイプ、テナントの地域別クラウド プレーン、および特定のライセンスに基づく機能などの要因によって異なります。

割り当てのタイプ	詳細
フローティング VDI デスクトップ割り当て	割り当てを選択し、[詳細] - [削除] の順にクリックします。削除を確定すると、システムがデスクトップ仮想マシンの削除を開始します。 [アクティビティ] ページを使用して、削除プロセスを監視できます。システムがデスクトップ仮想マシンを削除すると、すべての仮想マシンが仲介不能としてマークされて、削除プロセス中に新しいエンド ユーザー接続が発生しないようになります。既存のエンド ユーザー接続があるデスクトップ仮想マシンについては、コンソールにこれらのセッションが終了するという警告が表示されます。接続済みのエンド ユーザーのデスクトップには警告は表示されません。 **注：** 割り当ての [デスクトップ] タブから、フローティング VDI デスクトップ割り当てのデスクトップ仮想マシンを手動で削除しないでください。フローティング VDI デスクトップ割り当てからデスクトップ仮想マシンを手動で削除すると、システムの電源管理機能により、削除されたマシンの代わりとして新しいデスクトップ仮想マシンが自動的に作成されます。フローティング VDI デスクトップ割り当てからデスクトップ仮想マシンを削除するには、[デスクトップの最小数] と [デスクトップの最大数] の値を常に編集します。
専用の VDI デスクトップ割り当て	専用の VDI デスクトップ割り当てを削除するには： 1 [割り当て] ページの [オフラインにする] ボタンを使用して、割り当てをオフラインにします。割り当てをオフラインにすると、次の手順でインスタンスを削除しているときに、システムの電源管理機能により自動的に新しいデスクトップ仮想マシンを作成しようとする操作が防止されます。 2 割り当てのデスクトップ仮想マシンをすべて削除します。割り当ての詳細ページに移動し、[デスクトップ] タブをクリックしてすべてのデスクトップ仮想マシンを選択し、[詳細] - [削除] の順に選択したら、ダイアログの [割り当てのサイズを減らす] セクションで [はい] を選択し、削除を確認します。 **注：** ログイン ユーザーのセッションがあるデスクトップ仮想マシンは削除できません。[ログオフ] アクションの使用後に、デスクトップ仮想マシンを削除します。 3 [アクティビティ] ページを使用して削除プロセスを監視し、すべてのデスクトップ仮想マシンが削除され、すべてのタスクが完了する時期について判断します。割り当てのサイズを 0 として表示しているコンソール ページを信用しないでください。すべてのデスクトップ仮想マシンが 0 であるかもしれない場合でも、システムのレコードを完全に更新するための追加のタスクがまだ実行中である可能性があります。これらの実行中のタスクは、すべて完了するまで、コンソール ページから割り当てを削除することを防止します。すべてのデスクトップを削除することは、その数によっては長い時間がかかる可能性があります。 4 すべてのデスクトップ仮想マシンが削除され、割り当てのキャパシティが 0 とレポートされた場合、割り当てを選択し、[詳細] - [削除] をクリックして削除できます。
セッション デスクトップ割り当て	割り当てを選択し、[詳細] - [削除] の順にクリックします。セッション デスクトップ割り当ては、ファーム内の RDSH 仮想マシンに接続する資格が付与されたユーザー向けのものであるため、この割り当てタイプを削除しても実際に削除される仮想マシンはありません。割り当てのレコードがシステムから削除されます。
■ App Volumes アプリケーションの割り当て ■ リモート アプリケーションの割り当て ■ URL リダイレクトのカスタマイズ割り当て	割り当てを選択し、コンソールでその割り当てが表示されるページに提供されている内容に応じて、[削除 (Remove)] または [削除 (Delete)] アクションを使用します。

Horizon Cloud 環境での VDI デスクトップ割り当てのサイズ変更

VDI デスクトップ割り当てを作成するときに、[デスクトップの最大数] の値を使用して、VDI デスクトップ インスタンスの初期キャパシティを割り当てます。ユーザー数の変更に応じて、VDI デスクトップ割り当ての拡張または縮小が必要になる場合があります。

エンド ユーザーのニーズを満たすために追加のデスクトップ仮想マシンを追加することによって、VDI デスクトップ割り当てを展開します。

Microsoft Azure クラウド環境のキャパシティを解放するために VDI デスクトップ割り当てを縮小して、そのキャパシティを他の用途で使用できるようにします。エンド ユーザーが特定の VDI デスクトップ割り当てからデスクトップ仮想マシンにアクセスする必要がなくなったときに、その不要なキャパシティを解放することがあります。

重要： 専用の VDI デスクトップ割り当てでは、そのキャパシティを削減するために、割り当ての詳細ページの [デスクトップ] タブからデスクトップ仮想マシンを削除する必要があります。[デスクトップの最大数] の値を減らしても、既存の専用 VDI デスクトップの割り当てを縮小させることはできません。

VDI デスクトップ割り当ての拡大

VDI デスクトップ仮想マシンを VDI デスクトップ割り当てに追加することによって、VDI デスクトップ割り当てのキャパシティを増やします。フローティングまたは専用の VDI デスクトップ割り当てを編集してデスクトップ仮想マシンを追加し、[デスクトップの最大数] の値を増やすことができます。Horizon Universal Console を使用して VDI デスクトップ割り当てを編集する方法については、Horizon Cloud 環境での割り当ての編集を参照してください。割り当ては、ポッド内の VDI デスクトップのスケールの制限まで拡張することができます。

変更を送信すると、システムでは、新しいより大きな [デスクトップの最大数] の値と一致する新しいデスクトップ仮想マシンの作成を開始します。プロセスを監視するために VDI デスクトップ割り当ての [デスクトップ] および [アクティビティ] タブを使用することができます。これらのタブの詳細については、Horizon Cloud 環境で現在設定されている割り当ての表示を参照してください。

VDI デスクトップ割り当ての縮小

VDI デスクトップ割り当てのキャパシティを削減する方法は、そのタイプに応じて異なります。

VDI デスクトップ割り当てのタイプ	説明
フローティング	フローティング VDI デスクトップ割り当てのキャパシティを減らすには、割り当てを編集し、[デスクトップの最大数] の値をより小さい値に変更します。変更を送信すると、システムは、使用中でない VDI デスクトップ仮想マシンの削除を開始して、割り当て内の合計数が新しい値に一致するように仮想マシンを削除します。 新しい要求数が、現在ログイン中のエンド ユーザーにより、またはエンド ユーザーがデスクトップ仮想マシンに対するセッションを切断しているために、使用中でないデスクトップ仮想マシンの数を下回っている場合、システムはこのプロセスを禁止し、コンソールにエラー メッセージが表示されます。この状況で割り当てを縮小するには、次のいずれか 1 つまたは複数を組み合わせた方法を使用できます。 ■ 割り当てを再編集し、別の [デスクトップの最大数] の値を使用して、現在使用中でないデスクトップをすべて削除します。 ■ ユーザーが使用中のデスクトップから完全にログオフするのを待つか強制的に実行してから、[デスクトップの最大数] の値を減らすように割り当てを編集します。割り当ての [デスクトップ] タブから、デスクトップを選択して [...] - [ログオフ] をクリックすることによって、強制的にログオフを実行することができます。
専用	最初に割り当てからデスクトップに接続するときに、専用 VDI デスクトップ割り当てのデスクトップ インスタンスは特定のエンド ユーザーにマッピングされているため、システムでは、[デスクトップの最大数] の値を変更することによって割り当てのキャパシティが減らされることを防ぎます。この理由は、その数を減らしても、合計数からどの特定のデスクトップ インスタンスが削除されるかについては、システムに通知されないためです。 専用の VDI デスクトップ割り当てのサイズを減らすには、明示的に割り当ての [デスクトップ] タブからデスクトップを削除する必要があります。そのタブで、削除するデスクトップの隣にあるチェックボックスを選択して [...] - [削除] をクリックし、削除を確定します。ユーザーに割り当てられている VDI デスクトップと未割り当ての VDI デスクトップの両方を削除することができます。 1 [割り当て] ページの [オフラインにする] ボタンを使用して専用の VDI デスクトップ割り当てをオフラインにします。割り当てをオフラインにすると、いくつかのデスクトップを削除することになるため、システムの電源管理機能により自動的に新しいデスクトップ仮想マシンを作成しようとする操作が防止されます。 2 削除するデスクトップの隣にあるチェックボックスを選択し、[...] - [削除] をクリックして、ダイアログの [割り当てのサイズを減らしますか?] で [はい] を選択し、削除を確定します。 3 システムがデスクトップの削除を完了したら、割り当てをオンラインに再び戻して、[オンラインにする] ボタンを使用します。 システムが選択した VDI デスクトップを削除した後、割り当てのサイズは自動的に、元の [デスクトップの最大数] の値から削除済みの数を引いた数に一致するまで減少します。 **注：** [デスクトップ] タブで、アクティブ状態または切断されたセッションがあると示されているデスクトップを削除することはできません。デスクトップを削除する前に、エンド ユーザーを完全にログオフする必要があります。 専用 VDI デスクトップ割り当てのキャパシティと同じ全体的なキャパシティを維持しながら、既にユーザーにマッピングされているデスクトップを別のユーザーに使用させる場合は、割り当ての [デスクトップ] タブでデスクトップを選択し、[...] - [割り当て解除] を選択します。次に、そのデスクトップを別のユーザーに明示的に割り当てることができます。

Microsoft Azure の 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の仮想マシン モデルの変更

既存の専用またはフローティング VDI デスクトップ割り当てで Microsoft Azure 仮想マシン モデルを変更できます。この機能を使用すると、仮想マシン モデルが混在する VDI デスクトップ割り当てが可能になります。

Microsoft Azure で 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を作成する場合は、VDI デスクトップ割り当ての初期モデルを割り当てます。ユーザー要件が変更されると、割り当てを編集してモデルを変更できます。

割り当ての編集中にモデルを変更できます。[デスクトップ割り当ての編集] ウィザードを実行する一般的な手順については、Horizon Cloud 環境での割り当ての編集を参照してください。さまざまなタイプの VDI デスクトップ割り当てを作成するための具体的な手順については、Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた割り当ての管理を参照してください。

1 [デスクトップ割り当ての編集] ウィザードの処理を続行し、[モデル] メニューに進みます。

コンソールの [モデル] メニューの横に鉛筆アイコンが表示されます。強調表示された鉛筆アイコンは、モデルを変更できることを示します。アイコンが無効になっている（グレーアウトされている）場合は、アイコンの上にカーソルを置くと、ステータス メッセージが表示されます。たとえば、割り当てがマルチクラウド割り当てであり、サポートされていないポッドが 1 つ以上含まれている場合、鉛筆アイコンは無効になり、対応するステータス メッセージに詳細が表示されます。

図 6-3. 鉛筆アイコンがアクティブになっていないモデル メニュー

図 6-4. 鉛筆アイコンが強調表示された [モデル] メニュー

2 新しいモデルを選択するためのフィールドを表示するには、アクティブな鉛筆アイコンをクリックします。

[フィルタ] および [新しいモデル] メニューが表示されます。

3 必要に応じて [フィルタ] メニューを使用し、[新しいモデル] メニューを使用して、VDI デスクトップ割り当てに使用する新しいモデルを選択します。

フィルタ オプションを使用する手順については、このトピックですでに紹介した、VDI デスクトップ割り当ての作成に関するトピックを参照してください。

結果

システムは、選択したユーザーへの VDI デスクトップ割り当てのモデルを更新します。[割り当て] ページの [モデル] 列に現在のモデルが反映されます。モデル情報にカーソルを合わせると、ディスク タイプとサイズの詳細が表示されます。

注： 専用 VDI デスクトップ割り当ての編集中に行った仮想マシン モデルの変更は、既存のデスクトップを更新せず、将来の専用デスクトップに適用されます。

Horizon Cloud ポッド - VDI 専用デスクトップ割り当ての特定の VDI デスクトップのサイズ変更

このドキュメント ページでは、VDI 専用デスクトップ割り当てにすでに存在する特定の個々の VDI デスクトップのサイズを変更する方法について説明します。

サービス リリース 2204 以降では、既存の割り当てられた専用 VDI デスクトップを編集して、仮想マシン モデル、ディスク サイズ、およびディスク タイプを変更できます。この機能を使用するには、ポッドでそのリリースのマニフェスト バージョン以降が実行されている必要があります。

この機能は通常、次のシナリオで使用されます。

- 割り当て済みのデスクトップで、割り当てのエンド ユーザーの一部に、割り当ての仮想マシン構成とは異なる CPU、メモリ、またはディスク タイプのニーズがある。
- VDI 専用割り当て自体は仮想マシン モデルとディスク タイプおよびサイズを使用し、既存のデスクトップがあったが、その後割り当て自体が別の仮想マシン モデルまたは異なるディスク タイプ、あるいはディスク サイズを使用するように編集された。このシナリオでは、割り当ての新しい仮想マシン構成と一致するようにこれらのデスクトップを個別に編集するまで、既存のデスクトップは割り当ての元の仮想マシン モデルまたはディスク構成を使用したままになります。

この機能に関する注意事項：

- 特定の VDI デスクトップを編集することは、そのデスクトップの基盤となる仮想マシンに使用される Azure 仮想マシン モデル、ディスク サイズ、およびディスク タイプを変更することを意味します。
- VDI 専用デスクトップ割り当て内の特定のデスクトップを編集すると、そのデスクトップが存在する割り当て全体が混合タイプの割り当てと見なされます。
- 割り当て全体は、指定された仮想マシン設定を引き続き使用します。その結果、後でその VDI 専用デスクトップ割り当て内のデスクトップの数を増やすと、割り当ての拡張から作成された新しい VDI デスクトップに割り当ての仮想マシン設定が適用されます。
- この機能は、単一セッションの Windows 10 および Windows 11 オペレーティング システムでサポートされています。

- 次のオペレーティング システムでの使用はサポートされていません：Windows 7 およびマルチセッション Windows オペレーティング システム。（Horizon Cloud for Microsoft Azure 環境では、マルチセッションの Windows オペレーティング システムはファームで使用されることに注意してください。この機能は、VDI 専用デスクトップ割り当てのコンテキストで使用されます。したがって、これらのマルチセッション システムは VDI 専用デスクトップ割り当てに使用されないため、この機能がこのようなマルチセッション システムでサポートされることは想定されていません。）
- この機能での ZRS ディスク タイプの使用は現在サポートされていません。Microsoft Azure クラウドでは、ZRS（ゾーン冗長ストレージ）オプションは限定プレビューで提供されます。ZRS ディスク タイプで構成されたデスクトップを編集すると失敗することがあります。デスクトップを編集して ZRS 以外のディスク タイプから ZRS ディスク タイプに切り替えると、失敗することがあります。
- コンソールの VDI 専用デスクトップ割り当ての [デスクトップ] タブにある [モデル] 列には、割り当てのデスクトップに使用されている Azure 仮想マシン モデルが表示されます。その [モデル] 列から、どのデスクトップが他のデスクトップとは異なる仮想マシン モデルを使用しているかを確認できます。

前提条件

VDI デスクトップで [編集] アクションを実行するには、VDI デスクトップをパワーオフ状態にする必要があります。

割り当ての電源管理ポリシーが VDI デスクトップのパワーオフを妨げないようにします。電源管理ポリシーがデスクトップを確実にパワーオンするように設定されている場合、VDI デスクトップをパワーオフして編集すると、システムは自動的にパワーオンしようと試みます。必要に応じて、電源管理ポリシーを一時的に調整し、VDI デスクトップをパワーオフして編集できるようにします。次に、デスクトップを更新するシステム アクティビティが終了したら、割り当ての電源管理ポリシーを以前の状態に戻します。

手順

1. Horizon Universal Console で、デスクトップが存在する VDI 専用デスクトップ割り当ての詳細に移動し、[デスクトップ] タブを選択します。
2. デスクトップがまだオフになっていない場合は、パワーオフします。
3. パワーオフ状態のデスクトップを選択し、[詳細] - [編集] の順にクリックします。
4. 新しい仮想マシン モデルを選択するか、ディスク タイプまたはサイズを変更します。

   注： この機能での ZRS ディスク タイプの使用は現在サポートされていません。ZRS タイプを選択すると失敗することがあります。

5. [保存] をクリックします。

次のステップ

VDI デスクトップをパワーオフして編集できるように電源管理ポリシーを一時的に調整した場合は、割り当ての電源管理ポリシーを以前の状態に戻します。

ディスク サイズを増やすと、デスクトップの基盤となる仮想マシンでのゲスト OS の操作が必要になる場合があります。詳細については、ファームまたは VDI デスクトップ割り当てのディスク サイズが増加した場合に必要な管理者のアクションを参照してください。

シングルポッド ブローカ - 専用デスクトップ割り当て間の仮想マシンの移行

この記事では、1 台以上の仮想マシン (VM) を 1 つの専用デスクトップ割り当てから別の割り当てに移動する方法について説明します。移行プロセスでは、各仮想マシンの名前、構成、ユーザー データが保持され、元のユーザー資格がソース割り当てからターゲット割り当てにコピーされます。仮想マシン移行機能は、シングルポッド ブローカ環境での Microsoft Azure の Horizon Cloud ポッドでサポートされます。

注意: クラウドベースの Horizon Universal Console のツアーで説明されているように、第 1 世代のコンソールは動的であり、第 1 世代のテナント環境の最新の構成に適した機能を反映しています。このドキュメントで説明されている機能へのアクセスは、以下の要因（ただしこれらに限定されない）に依存する場合があります。

- その機能が最新の第 1 世代の Horizon Cloud ポッド マニフェスト、Horizon ポッドのバージョン、または Horizon Cloud Connector のバージョンでのみ使用可能なシステム コードに依存するかどうか。
- 機能が初登場したときに、リリース ノートに記載されているように制限付きで機能へのアクセスが提供されるかどうか。
- 機能に特定のライセンスまたは SKU が必要かどうか。

このドキュメントに機能の記載があり、第 1 世代のコンソールにその機能が表示されない場合は、まずリリース ノートを読み、その機能のアクセスが制限されているかどうか、およびテナントで有効化をリクエストする方法について確認します。または、このドキュメントに記載されている機能を使用する資格があり、コンソールにその機能が表示されない場合は、VMware Horizon Cloud Service の担当者に問い合わせるか、担当者がいない場合は Customer Connect でサポート リクエストを発行する方法 (VMware KB 2006985)の記載内容に従って、サービス リクエストを Horizon Cloud Service チームに発行することができます。

仮想マシン移行機能の概要

移行機能を使用すると、仮想マシンをソース割り当てからターゲット割り当てに移動し、各仮想マシンの名前、構成、ユーザー データ、およびユーザー資格を保持できます。ソースとターゲットの両方が専用デスクトップ割り当てである必要があります。1 回の移行操作で最大 50 台の仮想マシンを移行できます。Horizon Universal Console の [アクティビティ] ページでは、進行中の移行タスクのステータスを監視できます。

移行をサポートするには、仮想マシンがこの記事の後述の「前提条件」セクションに記載されている要件を満たす必要があります。仮想マシンがすべての要件を満たしていない場合、移行は続行されません。

移行プロセス中は、ソースおよびターゲットの割り当てに対して書き込み操作を実行できません。書き込み操作の例には、割り当ての構成の変更、仮想マシンのパワーオフとパワーオンなどがあります。

移行プロセスは通常 15 ～ 30 分で完了しますが、移行する仮想マシンの数によってはさらに時間がかかる場合があります。

移行の結果と修正について

仮想マシンは、Azure リソース グループにある複数のリソースで構成されます。移行を正常に完了するには、仮想マシンに関連付けられているすべてのリソースを、ターゲット割り当ての該当するリソース グループに移動する必要があります。仮想マシンのリソースの一部がターゲットに移動し、他のリソースがソース割り当てに残っている場合、その仮想マシンは部分的に移行されたと見なされます。

したがって、移行の結果は次のいずれかになります。

- [成功]：すべての仮想マシンに関連付けられているすべての Azure リソースがターゲット リソースに正常に移動しました。
- [エラー]：操作に失敗し、どの仮想マシンも移行されませんでした。
- [部分的に成功しました]：操作の結果、次のいずれかのシナリオが発生しました。
  - 一部の仮想マシンが正常に移行されましたが、他の仮想マシンは失敗しました。
  - 少なくとも 1 台の仮想マシンが部分的にのみ移行されました。部分的に移行された仮想マシンとは、Azure リソースの一部がソース割り当てに残っている仮想マシンです。

移行が部分的に成功した場合は、該当する仮想マシンで修正操作を使用して、完了しなかった移行タスクを完了できます。修正操作により、ソース割り当てに残っている仮想マシンの Azure リソースが検出され、ターゲット割り当てに移動されます。

前提条件

デスクトップ割り当て間の仮想マシンの移行をサポートするには、システム環境が次の要件を満たしている必要があります。

- ソースとターゲットのどちらの割り当ても専用デスクトップ割り当てであること。
- ソースとターゲットのどちらの割り当ても Microsoft Azure の同じ Horizon Cloud ポッドに配置されていること。
- ポッドが最低でも VMware Horizon Cloud Service v2111 リリースで最初に使用可能になったポッド マニフェスト バージョンを実行していること。
- すべてのユーザーがソースとターゲットの両方の割り当てのすべてのセッションからログアウトされていること。
- ソース割り当てまたはターゲット割り当てのいずれの仮想マシンでもタスクが実行されていないこと。
- 仮想マシンがドメインに参加しており、かつターゲット割り当てと同じドメイン、OU、グラフィック設定を持っていること。

手順

1 Horizon Universal Console で、Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた専用 VDI デスクトップ割り当てを一覧表示するページに移動します。

2 [割り当て] ページで、移行する仮想マシンを含むソース割り当ての名前をクリックします。次に、[デスクトップ] タブをクリックします。

[デスクトップ] ページには、ソース割り当てに属する仮想マシンが一覧表示されます。

3 リストで 1 台以上の仮想マシンを選択し、[詳細] - [仮想マシンの移行] の順に選択します。

移行オプションを指定するためのコントロールを含むダイアログ ボックスが表示されます。

4 [割り当ての名前] テキスト ボックスに、選択した仮想マシンの移動先となるターゲット割り当ての名前を入力します。次に、表示される適格な割り当てのドロップダウン メニューからターゲット割り当てを選択します。

5 [移行] をクリックして移行を開始します。

コンソールに、移行要求が送信されたことを確認するアラート メッセージが表示されます。

移行中は、ソース割り当ておよびターゲット割り当ての構成を変更したり、仮想マシンに対してアクションを実行したりすることはできません。

6 移行タスクのステータスを監視するには、[監視] - [アクティビティ] - [管理者] の順に移動します。

アクティビティ リストの各行は、影響を受けるすべての仮想マシン全体に適用される移行タスクのステータスを監視します。

移行タスクは通常 15 ～ 30 分で完了しますが、選択した仮想マシンの数によってはさらに時間がかかる場合があります。

7 移行結果を表示するには、[割り当て] ページに戻ります。リストでターゲット割り当てを選択し、[デスクトップ] タブをクリックして、選択したすべての仮想マシンが準備完了のステータスでリストに表示されていることを確認します。

注： 選択した仮想マシンのすべてがターゲット割り当ての下に準備完了のステータスで表示されない場合、移行がエラーで失敗したか、部分的にのみ成功した可能性があります。移行が部分的に成功した場合、次のような状況が発生します。

- 選択した仮想マシンがターゲット割り当てに見つからないか、エラー ステータスで表示される。
- 選択した仮想マシンが引き続きソース割り当ての下に表示される。

部分的に成功した移行、または失敗した移行を修正するには、次の手順に進みます。

8 移行が完全に成功しなかった場合は、次のいずれかの修正方法を試してください。

- 移行がエラーで失敗した場合は、手順 3 に戻り、移行を繰り返します。
- 移行が部分的に成功した場合は、ターゲット割り当てにエラー ステータスで表示されている適格な仮想マシンを選択し、[詳細] - [修正] の順に選択します。次に、ソース割り当てに移動し、エラー ステータスで表示されている適格な仮想マシンを選択して、[詳細] - [修正] の順に選択します。

専用デスクトップ割り当ての削除の防止または削除の許可

[割り当て] ページの設定を使用して、専用デスクトップ割り当てでの仮想マシンの削除を防止したり、削除を許可したりできます。

[削除を防止] オプションを選択すると、システムは専用デスクトップ割り当てからデスクトップ仮想マシンを削除する要求をすべて拒否します。次のオプションを使用しても、仮想マシンの削除に制限を設定できます。

- [削除保護]：詳細については、Horizon Cloud テナント環境のカスタマイズ可能な全般設定を参照してください。

- [最大デスクトップ削除]: このオプションは専用デスクトップ割り当てを作成または編集するときに設定します。オプションの詳細については、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を参照してください。

注： 削除防止が有効になっている専用デスクトップ割り当てに新しいイメージを指定すると、システムは削除防止を無効にして削除設定を変更し、未割り当てのデスクトップ仮想マシンをすべて新しいイメージで再構築できるようにします。

削除を防止

1 [割り当て] ページで、割り当てのチェックボックスをオンにします。

その割り当てのオプションが有効になります。

2 [詳細] - [削除を防止] をクリックします。

割り当ての削除を防止することを確認するダイアログ ボックスが表示されます。

3 [続行] をクリックします。

操作が正常に実行されたことを示すメッセージが表示されます。

削除を許可

1 [割り当て] ページで、割り当てのチェックボックスをオンにします。

その割り当てのオプションが有効になります。

2 [詳細] - [削除を許可] をクリックします。

割り当ての削除を許可することを確認するダイアログ ボックスが表示されます。

3 [続行] をクリックします。

操作が正常に実行されたことを示すメッセージが表示されます。

Horizon Cloud ポッド内のネットワーク セキュリティ グループと VDI デスクトップについて

Microsoft Azure クラウドにデプロイされた Horizon Cloud ポッドごとに、ポッドのリソース グループにはテンプレートとして機能するネットワーク セキュリティ グループ (NSG) も作成されます。このテンプレートを使用して、VDI デスクトップの割り当てによって提供される VDI デスクトップに必要となる可能性がある追加のポートを確実に開くことができます。

Microsoft Azure では、ネットワーク セキュリティ グループ (NSG) は Azure Virtual Network (VNet) に接続されたリソースへのネットワーク トラフィックを管理します。NSG は、そのネットワーク トラフィックを許可または拒否するセキュリティ ルールを定義します。NSG によるネットワーク トラフィックのフィルタ方法の詳細については、Microsoft Azure のドキュメントで「Filter network traffic with network security groups」のトピックを参照してください。

Horizon Cloud ポッドが Microsoft Azure にデプロイされると、`vmw-hcs-podID-nsg-template` という名前の NSG がポッドの `vmw-hcs-podID` という同じ名前のリソース グループに作成されます。*podID* はポッド ID です。ポッドの詳細ページ（Horizon Universal Console の [キャパシティ] ページからアクセスする）からポッドの ID を取得できます。

デフォルトでは：

- Microsoft Azure は、各 NSG が作成されると自動的にいくつかのデフォルトのルールを作成します。作成されるすべての NSG で、Microsoft Azure はいくつかのインバウンド ルールとアウトバウンド ルールを 65000 以上の優先度で作成します。このような Microsoft Azure のデフォルトのルールは、ユーザーまたはシステムが Microsoft Azure で NSG を作成すると、Microsoft Azure によって自動的に作成されるので、このドキュメントのトピックでは説明されません。これらのルールは Horizon Cloud によって作成されるものではありません。これらのデフォルトのルールの詳細については、Microsoft Azure ドキュメントの「デフォルトのセキュリティ ルール」トピックを参照してください。
- Horizon Cloud ポッド デプロイヤは、ポッドのテンプレート NSG に次のインバウンド セキュリティ ルールを作成します。これらのデフォルトのインバウンド セキュリティ ルールは、Blast および PCoIP と USB のリダイレクトを使用して VDI デスクトップにアクセスするエンドユーザー クライアントをサポートします。

表 6-5. ポッドのテンプレート NSG で Horizon Cloud ポッド デプロイヤによって作成されたインバウンド セキュリティ ルール

優先順位	名前	ポート	プロトコル	ソース	送信先	アクション
1000	AllowBlastUdpIn	22443	UDP	インターネット	任意	許可
1100	AllowBlastTcpIn	22443	TCP	インターネット	任意	許可
1200	AllowPcoipTcpIn	4172	TCP	インターネット	任意	許可
1300	AllowPcoipUdpIn	4172	UDP	インターネット	任意	許可
1400	AllowTcpSideChannelIn	9427	TCP	インターネット	任意	許可
1500	AllowUsbRedirectionIn	32111	TCP	インターネット	任意	許可

このテンプレート NSG に加えて、VDI デスクトップ割り当てが作成されるときに、システムはテンプレート NSG をコピーすることによってその割り当てのデスクトップ プールの NSG を作成します。各 VDI デスクトップ割り当てのプールには、テンプレート NSG のコピーである独自の NSG があります。プールの NSG は、そのプールの VDI デスクトップ仮想マシン (VM) の NIC に割り当てられます。デフォルトでは、すべての VDI デスクトップ プールは、ポッドのテンプレート NSG で設定されているのと同じデフォルトのセキュリティ ルールを使用します。

テンプレート NSG と VDI デスクトップ割り当てごとの NSG の両方を変更できます。たとえば、追加のポートを開いておく必要があるアプリケーションが VDI デスクトップにある場合は、そのポートでネットワーク トラフィックを許可するように対応する VDI デスクトップ割り当てプールの NSG を変更します。同じポートを開く必要がある複数の VDI デスクトップ割り当てを作成する予定がある場合、テンプレート NSG をあらかじめ編集しておくと、VDI デスクトップ割り当ての作成が容易になります。

重要： 基本テンプレートを変更する計画の場合は、変更前にコピーを作成します。元のデフォルト設定に戻す必要がある場合に、コピーをバックアップとして使用することができます。

Horizon Cloud ポッド - VDI デスクトップ割り当て、ファーム、公開イメージ、ベース仮想マシンにインストールされたエージェント関連ソフトウェアの更新

次のポッドに関連付けられた仮想マシンでは、それらのライフサイクルの任意の時点（ベース仮想マシン、公開イメージ、ファーム ホスト仮想マシン、VDI デスクトップ仮想マシンなど）で、VMware のエージェント関連ソフトウェアをインストールしています。VMware では、新しい機能とバグ修正を提供するためにエージェントに関連するソフトウェアの更新を定期的に提供しています。ご利用の環境での必要に応じて、ベース仮想マシン、公開されたイメージ仮想マシン、ファーム ホスト仮想マシン、および VDI デスクトップ仮想マシンにインストールされるエージェント関連ソフトウェアを更新するために以下のトピックの手順を使用します。

重要： システムの更新マネージャ ジョブは、1 日に 1 回実行され、イメージまたは割り当てがエージェント関連ソフトウェアの更新の候補かどうかを評価します。そのジョブが実行されていない間に、イメージまたは割り当てのエージェント関連ソフトウェアが変更された場合、次回ジョブが実行されるまで、Horizon Cloud 管理コンソールのステータスが同期しないことがあります。この状況は主に、Horizon Agents Installer を仮想マシン上で手動で実行してエージェント ソフトウェアを更新するか、GPO を使用することによって、手動で最新のエージェント ソフトウェアに更新する場合に発生します。 例：

1 更新マネージャ ジョブは、毎日のスケジューリングされた時刻に実行され、エージェントの更新がイメージで使用可能であることをコンソールに示します。

2 ユーザーは、GPO を使用して、VDI デスクトップ割り当てのデスクトップ インスタンスを最新のエージェントに手動で更新します。

デスクトップ インスタンスのエージェント関連ソフトウェアで最新のソフトウェアが実行されていても、次回のスケジュール済み更新マネージャ ジョブの実行まで、コンソールではイメージに青いドットが表示され、エージェントの更新が利用可能であることを示します。

VMware Dynamic Environment Manager エージェント ソフトウェアについて

2019 年 7 月の Horizon Cloud リリース以降、VMware Dynamic Environment Manager エージェントのインストールは Horizon Agents Installer に組み込まれています。Horizon Agents Installer は、以下を行うソフトウェア パッケージです。

- [仮想マシンのインポート] ワークフローを実行するとき、またはイメージ仮想マシンを手動で作成してインポートするときに、エージェントに関連するソフトウェアを新しいイメージ仮想マシンにインストールします。ポッ

ド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリングすると、Horizon Agents Installer がバックグラウンドで実行され、エージェントがインストールされます。Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートする場合は、これらの手順の一部として Horizon Agents Installer をダウンロードして実行します。

- [エージェントの更新] ワークフローを実行するときに、既存のイメージ仮想マシンおよび専用 VDI デスクトップ割り当てのエージェントに関連するソフトウェアを更新します。Horizon Agents Installer は、インストールされたエージェントを更新するためにバックグラウンドで実行されます。

イメージ仮想マシンまたは専用 VDI デスクトップ割り当てのデスクトップ仮想マシン上で [エージェントの更新] ワークフローを実行した後、更新された仮想マシンの VMware Dynamic Environment Manager ファイルのインストール パスは、[エージェントの更新] ワークフローを実行する前に、仮想マシンへの元のエージェントのインストールがバージョン 19.2 以降であったかどうかによって異なります。

基本イメージ仮想マシンが最初に [デスクトップのインポート] ワークフローを使用して作成された場合

この場合、デフォルトでは、VMware Dynamic Environment Manager エージェントが自動的にインストールされていました。特定のインストール ファイルのパスは、基本イメージ仮想マシンが、19.2 バージョン以降のエージェント ソフトウェアで作成されたかどうかによって異なります。

- イメージ仮想マシンがマニフェスト 1493 以降のポッドで新しく作成された場合、VMware Dynamic Environment Manager のインストール ファイルのパスは `C:\Program Files\VMware\Horizon Agents\User Environment` です。その後、その仮想マシンで [エージェントの更新] ワークフローを実行すると、ファイル パスは `C:\Program Files\VMware\Horizon Agents\User Environment` のままになります。
- イメージ仮想マシンが 1493 以前のマニフェストのポッドで作成された場合、VMware Dynamic Environment Manager のインストール ファイルのパスは `C:\Program Files\Immidio\Flex Profiles` です。その後、その仮想マシンで [エージェントの更新] ワークフローを実行すると、ファイル パスは `C:\Program Files\Immidio\Flex Profiles` のままになります。

基本イメージ仮想マシンが最初に Microsoft Azure で手動で作成された場合

VMware Dynamic Environment Manager のインストール ファイルのパスは、手動で作成した仮想マシンに VMware Dynamic Environment Manager エージェントをインストールした方法によって異なります。

- Horizon Agents Installer バージョン 19.2 を使用して VMware Dynamic Environment Manager エージェントをインストールした場合、VMware Dynamic Environment Manager のインストール ファイルのパスは、`C:\Program Files\VMware\Horizon Agents\User Environment` です。その後、その仮想マシンで [エージェントの更新] ワークフローを実行すると、ファイル パスは `C:\Program Files\VMware\Horizon Agents\User Environment` のままになります。
- 別のスタンドアロンの VMware Dynamic Environment Manager インストーラを使用して VMware Dynamic Environment Manager エージェントをインストールした場合、VMware Dynamic Environment Manager のインストール ファイルのパスは `C:\Program Files\Immidio\Flex Profiles` です。その後、その仮想マシンで [エージェントの更新] ワークフローを実行すると、ファイル パスは `C:\Program Files\Immidio\Flex Profiles` のままになります。

また、基本イメージ仮想マシンが最初に Microsoft Azure で手動で作成され、その時点で VMware Dynamic Environment Manager エージェントをインストールしなかった場合、その後 [エージェントの更新] ワークフローでエージェントをインストールするときに、[エージェントの更新] ウィザードのコマンドラインの手順でコマンドライン引数 `ADDLOCAL=UEM` を使用します。

Horizon Cloud の RDSH イメージのエージェント ソフトウェアをアップデートする

現在ファームで使用されている RDSH イメージ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をアップデートするには、最初にイメージ上で [エージェントのアップデート] アクションを使用します。次にこれらのアップデートされたイメージを使用するファームを編集します。

概要レベルでは、システムのエージェントのアップデート機能は次のように機能します。

- システムは VMware CDS（コンポーネント ダウンロード サービス）ソフトウェア配布ネットワークと定期的に通信して、Horizon Agents Installer の新しいバージョンが使用可能かどうかを確認します。使用可能の場合、システムは自動的にそのバージョンを Horizon Cloud ポッドにダウンロードします。
- 新しいバージョンがダウンロードされた後、管理コンソールには、以前のエージェント関連のソフトウェアがインストールされているイメージのアップデートが利用可能であることが示されます。新しいバージョンより前のレベルでのエージェントに関連するソフトウェアがあるそれらのイメージに対してビジュアル インジケータが表示されます。
- エージェントのアップデート中は次のようになります。
  - システムは選択したイメージの仮想マシン (VM) をパワーオンして、そのパワーオン状態のイメージから仮想マシン (VM) の複製をクローン作成し、元の公開済みの状態に戻すために選択したイメージに対してイメージへの変換プロセスを実行します。プロセスのこの部分においては、コンソールに表示される選択したイメージのステータスが「公開済み」から「移行中」に変わります。
  - 重複した仮想マシンが存在する場合、システムはそれをパワーオンして、ウィザードで選択された新しい更新バージョンのエージェントに関連するソフトウェアをインストールしてから、その重複仮想マシンに対してイメージへの変換プロセスを実行して公開します。
- エージェントのアップデート プロセスの最後で、元のイメージとその複製イメージ（アップデートされたエージェント ソフトウェアがインストールされている）の両方が一覧表示されます。

重要： エージェントのアップデート プロセスの最後で、[エージェントのアップデート] をクリックしたときに選択した RDSH イメージは、元のエージェントのバージョン レベルで、プロセスが開始したときと同じ状態になります。新しい複製イメージは、選択したアップデート レベルでエージェント ソフトウェアを取得します。

エージェントのアップデート プロセスにより、エージェントに関連するソフトウェアがウィザードで指定するバージョンに更新された状態で、元のイメージの複製である新しい割り当て可能なイメージが生成されます。エージェントのアップデート ワークフローは、新しい仮想マシンを作るために自動的に元のイメージのクローンを作成し、指定されたレベルのエージェントに関連するソフトウェアをその仮想マシンにインストールして、その仮想マシンを割り当て可能な（公開済み）イメージに変換します。このシステムは、元のイメージの名前にダッシュと数字を付加した形式に基づいて、新しいイメージの名前を付けます。たとえば、元のイメージの名前が SalesGold である場合、エージェントのアップデート プロセスにより SalesGold-2 という名前のイメージが生成されます。プロセスの最後で、両方のイメージがコンソールに表示されます。

以下のスクリーンショットは、pat2016 という名前のイメージに対してエージェントのアップデートを実行して最新の利用可能なアップデート バージョンを選択した後に一覧表示される 2 つのイメージを示しています。元のイメージがプロセスの最後で変更されないため、青いドットはその横に表示されたままになります。pat2016-1 イメージにはアップデート レベルのエージェント ソフトウェアが含まれていて、より新しいアップデート バージョンはシステムに存在しないため、pat2016-1 イメージの横には青いドットが付いていません。

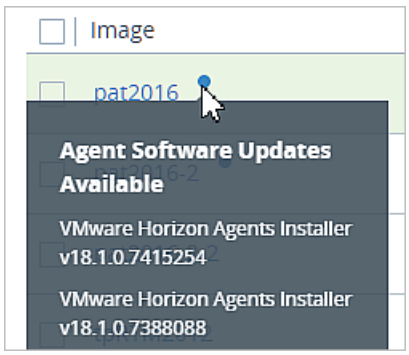
手順

1 [インベントリ] をクリックして、RDSH イメージが表示されているイメージ関連のページに移動します。

選択されたページでは、アップデートを適用する対象のすべてのイメージの名前の横に青いドットが表示されます。青いドットの上にカーソルを置くと、そのイメージで使用可能な Horizon Agents Installer の新しいバージョンを示すポップアップが表示されます。

次のスクリーンショットは、エージェントのアップデートが pat2016 という名前のイメージに対して利用可能であることを示しています。

どのようなアップデートが利用可能であるかを確認するには、その青いドットにカーソルを置きます。

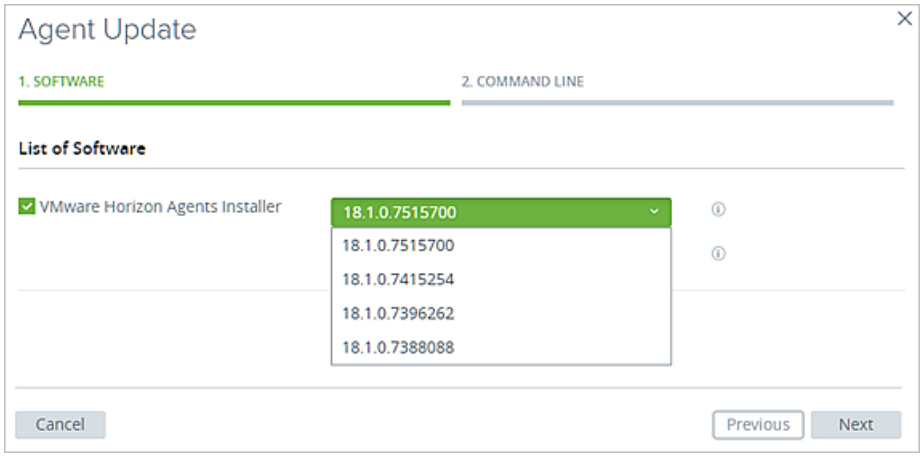


2 更新するイメージの横にあるチェック ボックスを選択します。

3 [エージェントのアップデート] をクリックします。

[エージェントのアップデート] ウィザードが表示されます。

4 [ソフトウェア] 手順で、ドロップダウン リストから使用するアップデートのバージョンを選択して、[次へ] をクリックします。



5 (オプション) コマンド ラインの手順で、イメージでのこのアップデートに関係する可能性がある任意のコマンドライン オプションを追加します。

ウィザードには、指定されたアップデートに対してコマンドライン オプションが利用可能かどうかを示すメッセージが表示されます。

6 [送信] をクリックします。

- アップデートが開始されたことを示すメッセージがページの最上部に表示されます。
- システムは、元のイメージのクローン仮想マシン (VM) を作成し、そのクローン イメージにエージェントに関連するコンポーネントをアップデートします。クローン イメージがアップデートされた後、システムはデスクトップへの変換プロセスを実行して、クローン イメージを公開済みのイメージに変換します。

[監視] > [アクティビティ] の順に選択すると、アップデート タスクの進捗を表示できます。タスクが 24 時間以内に正常に完了しない場合は、障害のステータスで表示されます。

次のステップ

- 元のイメージを使用しているファームが新しい複製イメージを使用するように、ファームを編集してアップデートします。そのイメージにはアップデートされたエージェント ソフトウェアが含まれています。ファームの [編集] アクションを使用し、開いたウィンドウで [イメージ] フィールドを見つけ、新しい複製イメージを選択して保存します。
- 元のイメージを使用していたファームを更新済みで、組織で元のイメージが不要になったと判断できる場合は、リストされたページから元のイメージを削除できます。組織内の他の管理者が、低いレベルのエージェントのあるイメージを使用しないようにするために、元のイメージを削除することはベスト プラクティスです。

専用 VDI デスクトップ割り当て用のエージェント ソフトウェアを更新する

専用 VDI デスクトップ割り当てで使用されるデスクトップ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を更新するには、まず割り当てで使用しているイメージを更新し、次に割り当てを更新します。イメージを更新すると、専用 VDI 割り当ての割り当て解除されたデスクトップが更新されます。このプロセスは、フローティング VDI デスクトップ割り当ての場合と同じです。専用 VDI デスクトップ割り当ての場合は、次に割り当てられたデスクトップのエージェントを更新します。

手順

1 割り当てに割り当てられていないデスクトップが多数ある場合は、割り当てが使用しているイメージのエージェント ソフトウェアを更新し、Horizon Cloud ポッド - 専用 VDI デスクトップ割り当てによって使用されるイメージのエージェント ソフトウェアを更新する で説明するように、更新されたイメージを使用するように割り当てを編集します。

これにより、割り当てられていないデスクトップでは、不要で時間のかかるエージェントの更新を回避できます。以下の 2 番目の手順を使用して、すべてのデスクトップを更新できますが、イメージの更新をすぐに計画している場合は、割り当てられていないデスクトップに対してこのプロセスを使用する必要はありません。

重要： イメージの更新と、更新されたイメージを使用するための割り当ての編集が完了したら、続行する前に、割り当てられていないすべてのデスクトップが更新され、更新されたイメージを使用していることを確認する必要があります。

2 該当するトピック専用 VDI デスクトップ割り当ての [割り当て] ページでエージェント ソフトウェアを更新するまたは専用 VDI デスクトップ割り当ての個々のデスクトップ上のエージェント ソフトウェアを更新するで説明されているとおりに、エージェントを割り当てレベルまたは個々のデスクトップ レベルで更新します。

Horizon Cloud ポッド - 専用 VDI デスクトップ割り当てによって使用されるイメージのエージェント ソフトウェアを更新する

専用 VDI デスクトップ割り当てのエージェントに関連するソフトウェアを更新するには、最初のタスクとして、割り当てで使用されるイメージにインストールされているソフトウェアを更新し、その更新されたイメージを使用するように専用 VDI デスクトップ割り当てを編集します。この手順では、割り当て内の未割り当てのデスクトップを更新します。

概要レベルでは、システムのエージェントのアップデート機能は次のように機能します。

- システムは VMware CDS（コンポーネント ダウンロード サービス）ソフトウェア配布ネットワークと定期的に通信して、Horizon Agents Installer の新しいバージョンが使用可能かどうかを確認します。使用可能な場合、システムはそのバージョンを Horizon Cloud ポッドにダウンロードします。
- 新しいバージョンがダウンロードされた後、管理コンソールには、アップデートの対象となるイメージにアップデートが利用可能であることが示されます。新しいバージョンより前のレベルでのエージェントに関連するソフトウェアがあるそれらのイメージに対してビジュアル インジケータが表示されます。
- エージェントのアップデート中は次のようになります。
  - システムは選択したイメージをパワーオンして、そのパワーオン状態のイメージから仮想マシン (VM) の複製をクローン作成し、元の公開済みの状態に戻すために選択したイメージに対してイメージへの変換プロセスを実行します。プロセスのこの部分においては、コンソールに表示されるイメージのステータスが「公開済み」から「移行中」に変わります。
  - 重複した仮想マシンが存在する場合、システムはそれをパワーオンして、ウィザードで選択された新しい更新バージョンのエージェントに関連するソフトウェアをインストールしてから、その重複仮想マシンに対してイメージへの変換プロセスを実行して公開します。

- エージェントのアップデート プロセスの最後で、元のイメージとその複製イメージ（アップデートされたエージェント ソフトウェアがインストールされている）の両方が一覧表示されます。

重要： エージェントの更新プロセスの最後で、[エージェントの更新] をクリックしたときに選択したイメージは、元のエージェントのバージョン レベルで、プロセスが開始したときと同じ状態になります。新しい複製イメージは、選択したアップデート レベルでエージェント ソフトウェアを取得します。

エージェントのアップデート プロセスにより、エージェントに関連するソフトウェアがウィザードで指定するバージョンに更新された状態で、元のイメージの複製である新しい割り当て可能なイメージが生成されます。エージェントのアップデート ワークフローは、新しい仮想マシンを作るために自動的に元のイメージのクローンを作成し、指定されたレベルのエージェントに関連するソフトウェアをその仮想マシンにインストールして、その仮想マシンを割り当て可能な（公開済み）イメージに変換します。このシステムは、元のイメージの名前にダッシュと数字を付加した形式に基づいて、新しいイメージの名前を付けます。たとえば、元のイメージの名前が SalesGold である場合、エージェントのアップデート プロセスにより SalesGold-2 という名前のイメージが生成されます。プロセスの最後で、両方のイメージがコンソールに表示されます。

以下のスクリーンショットは、あるイメージに対してエージェントのアップデートを実行して最新の利用可能な更新バージョンを選択した後に一覧表示される 2 つのイメージを示しています。元のイメージがプロセスの最後で変更されないため、青いドットはその横に表示されたままになります。別のイメージには更新レベルのエージェント ソフトウェアが含まれていて、より新しい更新バージョンはシステムに存在しないため、そのイメージの横には青いドットが付いていません。

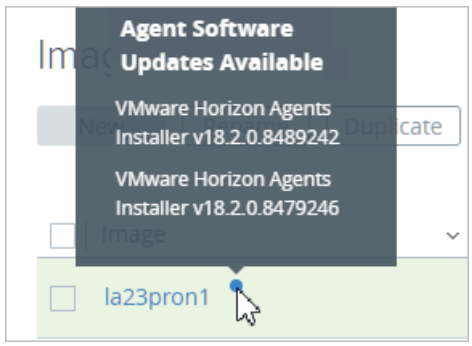
手順

1 [インベントリ] をクリックし、割り当てで使用されるイメージが表示されているイメージ関連のページに移動します。

選択されたページでは、アップデートを適用する対象のすべてのイメージの名前の横に青いドットが表示されます。青いドットにポインタを合わせると、そのイメージで利用可能な Horizon Agents Installer の新しいバージョンを示すポップアップ ウィンドウが表示されます。

次のスクリーンショットは、エージェントの更新が la24win10N という名前のイメージに対して利用可能であることを示しています。

どのようなアップデートが利用可能であるかを確認するには、その青いドットにポインタを合わせます。

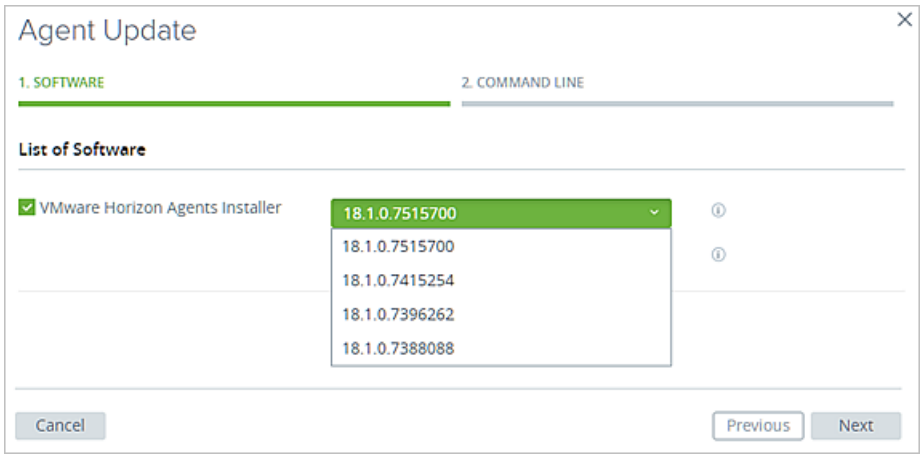


2 更新するイメージの横にあるチェック ボックスを選択します。

3 [エージェントのアップデート] をクリックします。

[エージェントのアップデート] ウィザードが表示されます。

4 [ソフトウェア] 手順で、ドロップダウン メニューから使用するアップデートのバージョンを選択して、[次へ] をクリックします。



5 (オプション) コマンド ラインの手順で、イメージでのこのアップデートに関係する可能性がある任意のコマンドライン オプションを追加します。

ウィザードには、指定されたアップデートに対してコマンドライン オプションが利用可能かどうかを示すメッセージが表示されます。

6 [送信] をクリックします。

- アップデートが開始されたことを示すメッセージがページの最上部に表示されます。
- システムは、元のイメージのクローン仮想マシン (VM) を作成し、そのクローン イメージにエージェントに関連するコンポーネントをアップデートします。クローン イメージがアップデートされた後、システムはデスクトップへの変換プロセスを実行して、クローン イメージを公開済みのイメージに変換します。

[監視] > [アクティビティ] の順に選択すると、アップデート タスクの進捗を表示できます。タスクが 24 時間以内に正常に完了しない場合は、障害のステータスで表示されます。

7 更新されたイメージに対して必要なテストを実行します。

8 元のイメージを使用している専用 VDI デスクトップ割り当てが新しい複製イメージを使用するように、割り当てを編集して更新します。そのイメージには更新されたエージェント ソフトウェアが含まれています。割り当てで [編集] アクションを選択し、開いたウィンドウで [イメージ] フィールドを見つけて、新しい複製イメージを選択し、保存します。

割り当ての編集の詳細については、Horizon Cloud 環境での割り当ての編集を参照してください。

9 未割り当てのすべてのデスクトップが、更新されたイメージにリンクされたことを確認します。

10 元のイメージを使用していた割り当てを更新済みで、組織で元のイメージが不要になったと判断できる場合は、リストされたページから元のイメージを削除できます。組織内の他の管理者が、低いレベルのエージェントのあるイメージを使用しないようにするために、元のイメージを削除することはベスト プラクティスです。

次のステップ

[割り当て] ページのエージェントの更新アクションを使用して、割り当てのエージェント ソフトウェアの更新を完了します。専用 VDI デスクトップ割り当ての [割り当て] ページでエージェント ソフトウェアを更新するを参照してください。

重要： 専用 VDI デスクトップ割り当ての更新を完了するには、[割り当て] ページでエージェント ソフトウェアの更新を実行する必要があります。

専用 VDI デスクトップ割り当ての [割り当て] ページでエージェント ソフトウェアを更新する

専用 VDI デスクトップ割り当てによって使用されるイメージを更新したら、割り当て内の割り当て済みデスクトップを更新するために、[割り当て] ページで割り当てを更新できます。

より詳細なデスクトップ レベルでエージェント ソフトウェアを更新するには、専用 VDI デスクトップ割り当ての個々のデスクトップ上のエージェント ソフトウェアを更新するを参照してください。次の手順はより広範なもので、割り当てレベルでエージェント ソフトウェアを更新できます。

専用 VDI デスクトップ割り当てに対して Horizon Cloud のエージェント更新機能の仕組みに関する高度な説明については、専用 VDI デスクトップ割り当てに対するエージェントのアップデート機能の仕組みを参照してください。

重要： これらの手順は、専用 VDI デスクトップ割り当てで使用します。これらの手順は、フローティング VDI デスクトップ割り当てには適用されません。フローティング VDI デスクトップ割り当てでのエージェントの更新の詳細については、Horizon Cloud ポッド - フローティング VDI デスクトップ割り当てによって使用されるイメージのエージェント ソフトウェアを更新するを参照してください。

注意： エージェントの更新操作が進行中のときには、割り当てのデスクトップ仮想マシンに電源変更操作が発生する原因として考えられるアクティビティが何も予定されていない状態を確保する必要があります。たとえば、他の管理者に対して、これらのデスクトップ仮想マシンを手動でパワーオフまたはパワーオンしないように通知したり、この割り当て内で構成された電源管理スケジュールによって、エージェントの更新タスクの実行中にデスクトップのパワーオンやパワーオフが行われないようにします。システムで仮想マシンのエージェントの更新タスクを実行しているときに、デスクトップ仮想マシンにおいて電源変更操作が行われると、予期しない結果が発生し、デスクトップ仮想マシンが手動でリカバリしなくてはならない状態になる可能性があります。

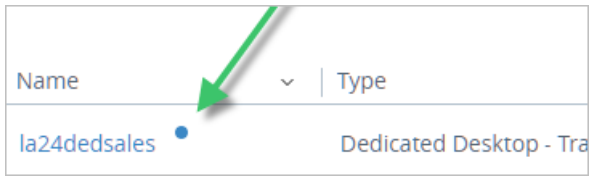
ベスト プラクティスは、割り当てを編集し、設定された電源管理スケジュールをすべて削除することで、エージェントの更新タスクの実行中に電源変更操作が行われないようにすることです。

手順

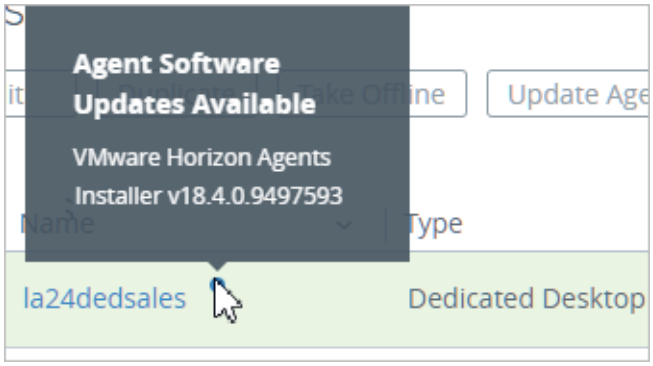
1 [割り当て] をクリックして、[割り当て] ページに移動します。

[割り当て] ページでは、更新を適用する対象の専用 VDI デスクトップ割り当ての名前の横に青いドットが表示されます。青いドットをポイントすると、その割り当てで利用可能な Horizon Agents Installer の新しいバージョンを示すポップアップ ボックスが表示されます。

次のスクリーンショットは、エージェントの更新が *la24dedsales* という名前の割り当てに対して利用可能であることを示しています。



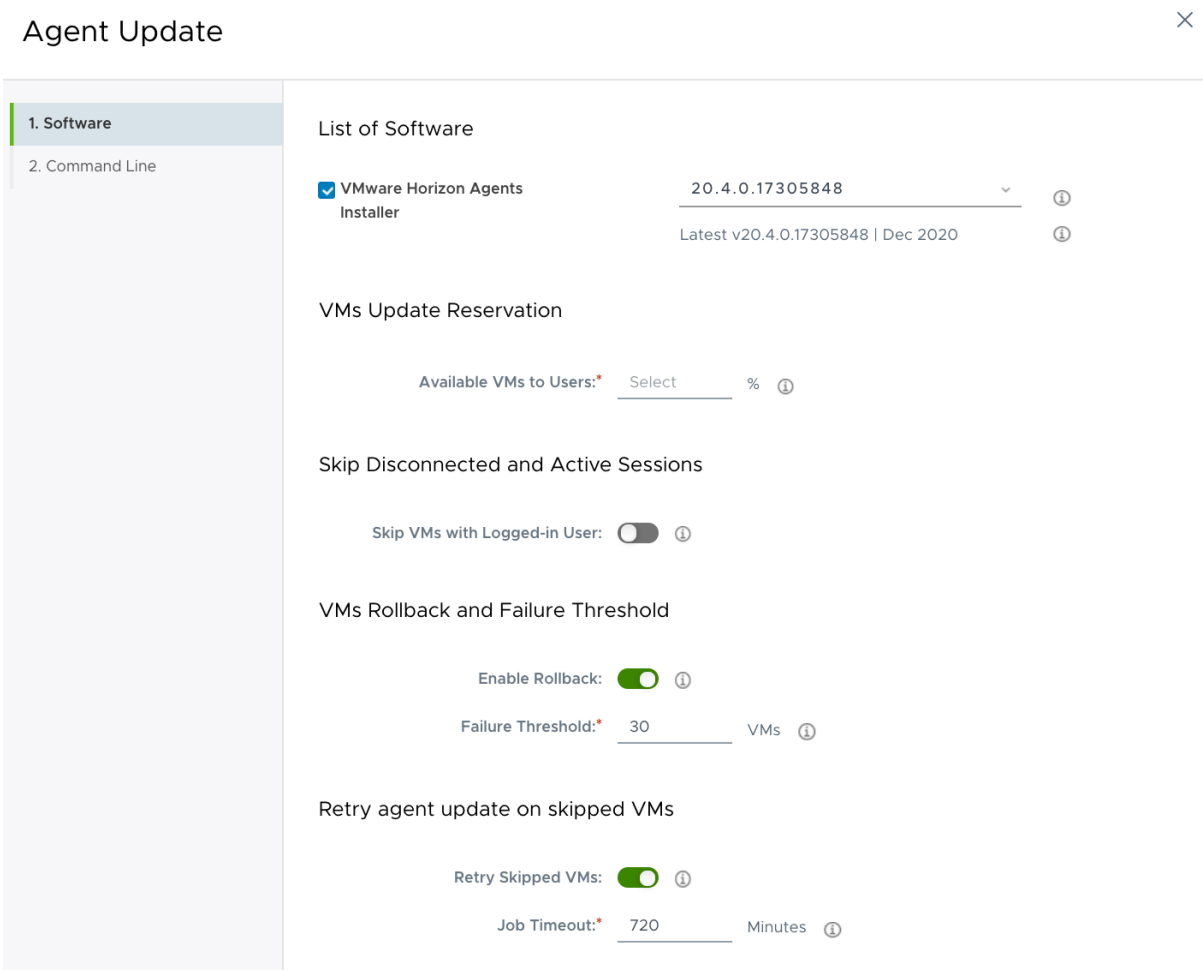
使用可能な更新を表示するには、その青いドットの上にポインタを置きます。



2 更新するイメージの横にあるチェック ボックスを選択します。

3 [エージェントのアップデート] をクリックします。

[エージェントのアップデート] ウィザードが表示されます。



4 [ソフトウェア] 手順で、ドロップダウン メニューから使用するアップデートのバージョンを選択します。

注： Microsoft Windows 7 を使用している割り当ての場合は、Horizon Agent Installer 20.3.x を選択する必要があります。

5 （必須） [ユーザーが利用可能な仮想マシン] テキスト ボックスで、更新プロセス中にパワーオンしてエンド ユーザーが利用できるようにする割り当て内のデスクトップ仮想マシンの割合を指定します。

重要： デスクトップを利用可能にする必要がない場合は、ゼロ (0) を入力します。更新プロセス中にデスクトップ仮想マシンをユーザーに利用可能にする必要がない場合でも、[ユーザーが利用可能な仮想マシン] の値を指定する必要があります。

この値は、システムが割り当てに対して更新を実行する期間中に、何台のデスクトップ仮想マシンをユーザーがアクセス可能にするかを決定します。この設定は、システムがデスクトップの更新を進める際に、小規模プールの高い割合を確実に利用可能にするので、デスクトップが 30 台または 30 台の 2 ～ 3 倍（60 台または 90 台）未満であるデスクトップ割り当てに有用です。例については専用 VDI デスクトップ割り当てに対するエージェントのアップデート機能の仕組みを参照してください。

利用可能割合をより高く設定することで、現在更新している仮想マシンのバッチにおけるデスクトップの数が調整されることになります。割り当てを更新する場合、システムは仮想マシンのバッチを並行して更新します。デフォルトでは、更新する仮想マシンの残りの数が 30 未満になるまで、システムはバッチごとに 30 台の仮想マシンを使用します。30 未満になった時点で、最終バッチは残りの仮想マシンに対して処理します。1 台の仮想マシンを完全に更新するには約 30 分から 45 分かかるため、仮想マシンのセットを並行して更新した場合でも、更新処理中の仮想マシンのセットはその時間中使用できません。

多数のデスクトップがある割り当てでは、割り当てにおけるデスクトップの総数に対してシステムの最大デフォルトである 1 バッチ 30 台の仮想マシンは小さな割合にしかならないので、このオプションはほとんど有用ではありません。

6 （オプション） ログインしているユーザー（アクティブまたは切断されたセッション）または競合するタスクが実行されているデスクトップをスキップするには、[ログイン ユーザーがいる仮想マシンをスキップ] トグルを有効化します。

7 （オプション） [ロールバックを有効にする] トグルを有効にすると、システムはエージェントの更新が実行される前にロールバック コピーを作成し、そのコピーを 7 日間保持します。この 7 日間においては、仮想マシンでエージェントの更新に失敗した場合、その仮想マシンの以前のエージェント バージョンにロールバックすることができます。詳細については、これらの手順の最後にある「次の手順」を参照してください。

注： ロールバックの時間枠はデフォルトで 7 日間に設定されていますが、この設定の変更を VMware に要求することもできます。

8 （必須） [障害のしきい値] には、更新プロセスが停止となるまでに許容される、エージェントの更新が失敗する仮想マシンの数を入力します。このしきい値により、大量の障害が発生するのを防ぎます。

デフォルト値は、[設定] - [全般設定] で構成したものです。

注： 仮想マシンの更新に失敗したことが原因で更新プロセスが停止した場合、設定したしきい値よりも多くの障害が発生した仮想マシンが表示されることがあります。これは、さまざまな理由で発生します。マルチポッドの割り当ての場合、システムは割り当てごとではなく、ポッドごとにしきい値設定を適用するため、この問題が発生する可能性があります。

9 （オプション） スキップされた仮想マシンを自動的に再試行するには、[スキップされた仮想マシンを再試行] トグルを有効にします。

10 （オプション） [ジョブのタイムアウト] フィールドで、スキップされた仮想マシンの更新をシステムが自動的に試行する期間を指定します。

[ジョブのタイムアウト] フィールドは、スキップされた仮想マシンの更新をシステムが再試行する分数を設定します。システムは、この時間に到達するまで、または割り当てのすべてのデスクトップ仮想マシンが更新されるまで、30 分ごとにスキップされた仮想マシンを更新します。

120 分（2 時間）から 1440 分（24 時間）までの値を入力できます。デフォルト値は 720 分（12 時間）です。

11 これがマルチクラウド割り当ての場合は、[更新するポッドを選択] で更新するポッドを選択します。マニフェスト バージョンが 2632 より前のポッドでは、ポッド名の横にある警告アイコンが表示され、そのポッドでロールバックと障害のしきい値がサポートされていないというテキストが示されます。

12 [次へ] をクリックします。

13 （オプション） コマンド ラインの手順で、イメージでのこのアップデートに関係する可能性がある任意のコマンドライン オプションを追加します。

ウィザードには、指定されたアップデートに対してコマンドライン オプションが利用可能かどうかを示すメッセージが表示されます。

14 [送信] をクリックします。

注： 環境がマルチクラウド割り当て用に構成されている場合、[送信] は選択できません。[次へ] をクリックして [サマリ] ページを確認し、[終了] をクリックします。

結果

- アップデートが開始されたことを示すメッセージがページの最上部に表示されます。
- システムにより、パワーオン状態のデスクトップで再起動が実行され、専用 VDI デスクトップ割り当て内のデスクトップ仮想マシン上のエージェントに関連するコンポーネントが更新されます。

[監視] - [アクティビティ] の順に選択すると、更新タスクの進捗を表示できます。

次のステップ

[割り当て - VDI デスクトップ] ページに移動して、更新が成功したかどうかを確認します。

リストされた仮想マシンの詳細をダウンロードするには、[監視] - [アクティビティ] を選択し、エージェントの更新タスクを選択し、[サマリ] ページで [詳細のダウンロード] をクリックします。

システムは、アクションを実行できる仮想マシンに関するステータス情報を提供する CSV ファイルをダウンロードします。各仮想マシンのアップグレード ステータスを使用して、実行するアクションを決定できます。

エージェントの更新の実行時にロールバックを有効にしている場合は、失敗した仮想マシンの割り当ての横にビジュアル インジケータが表示されます。割り当ての詳細ページの [デスクトップ] タブで、失敗した各仮想マシンを以前のエージェント バージョンにロールバックすることができます。割り当ての詳細ページで実行できるアクションの詳細については、Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた割り当ての管理を参照してください。

エージェントのアップグレードの失敗によってエージェントがオフライン状態のままになった場合、デスクトップはエージェントの再インストール操作の対象になります。専用 VDI デスクトップ割り当ての個々のデスクトップ上のエージェント ソフトウェアを再インストールするを参照してください。

専用 VDI デスクトップ割り当ての個々のデスクトップ上のエージェント ソフトウェアを更新する

専用 VDI デスクトップ割り当てによって使用されるイメージを更新した後、割り当て内の個々のデスクトップを更新できます。

より広範な割り当てレベルでエージェント ソフトウェアを更新するには、専用 VDI デスクトップ割り当ての [割り当て] ページでエージェント ソフトウェアを更新するを参照してください。次の手順はより詳細であり、1 つ以上のデスクトップをターゲットとして、エージェント ソフトウェアを更新できます。

専用 VDI デスクトップ割り当ての Horizon Cloud のエージェント更新機能の動作の概要については、専用 VDI デスクトップ割り当てに対するエージェントのアップデート機能の仕組みを参照してください。

重要： これらの手順は、専用 VDI デスクトップ割り当てで使用します。これらの手順は、フローティング VDI デスクトップ割り当てには適用されません。フローティング VDI デスクトップ割り当てでのエージェントの更新の詳細については、Horizon Cloud ポッド - フローティング VDI デスクトップ割り当てによって使用されるイメージのエージェント ソフトウェアを更新するを参照してください。

注意： エージェントの更新操作が進行中のときには、割り当てのデスクトップ仮想マシンに電源変更操作が発生する原因として考えられるアクティビティが何も予定されていない状態を確保する必要があります。たとえば、他の管理者に対して、これらのデスクトップ仮想マシンを手動でパワーオフまたはパワーオンしないように通知したり、この割り当て内で構成された電源管理スケジュールによって、エージェントの更新タスクの実行中にデスクトップのパワーオンやパワーオフが行われないようにします。システムで仮想マシンのエージェントの更新タスクを実行しているときに、デスクトップ仮想マシンにおいて電源変更操作が行われると、予期しない結果が発生し、デスクトップ仮想マシンが手動でリカバリしなくてはならない状態になる可能性があります。

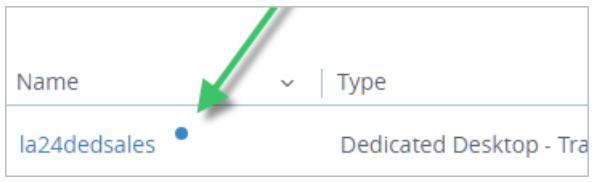
ベスト プラクティスは、割り当てを編集し、設定された電源管理スケジュールをすべて削除することで、エージェントの更新タスクの実行中に電源変更操作が行われないようにすることです。

手順

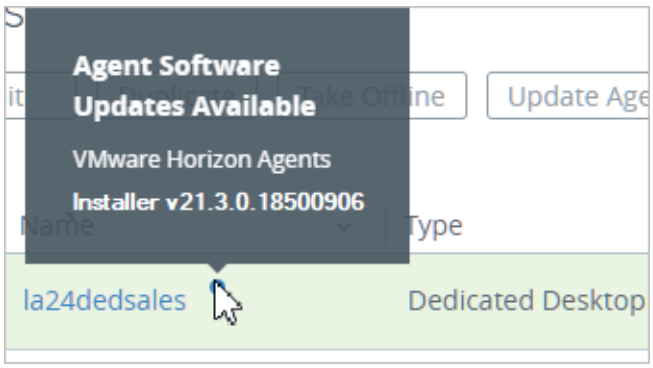
1 [割り当て] をクリックして、[割り当て] ページに移動します。

[割り当て] ページでは、更新を適用する対象の専用 VDI デスクトップ割り当ての名前の横に青いドットが表示されます。青いドットをポイントすると、その割り当てで利用可能な Horizon Agents Installer の新しいバージョンを示すポップアップ ボックスが表示されます。

次のスクリーンショットは、エージェントの更新が *la24dedsales* という名前の割り当てに対して利用可能であることを示しています。



使用可能な更新を表示するには、その青いドットの上にポインタを置きます。



2 対象となるデスクトップを含む割り当てをクリックします。

3 [デスクトップ] タブをクリックします。

4 複数のポッドを持つマルチクラウド割り当ての場合は、[ポッド] ドロップダウン セレクタから適切なポッドを選択します。

注： ポッド セレクタは、マルチクラウド割り当てが構成されている環境にのみ適用されます。

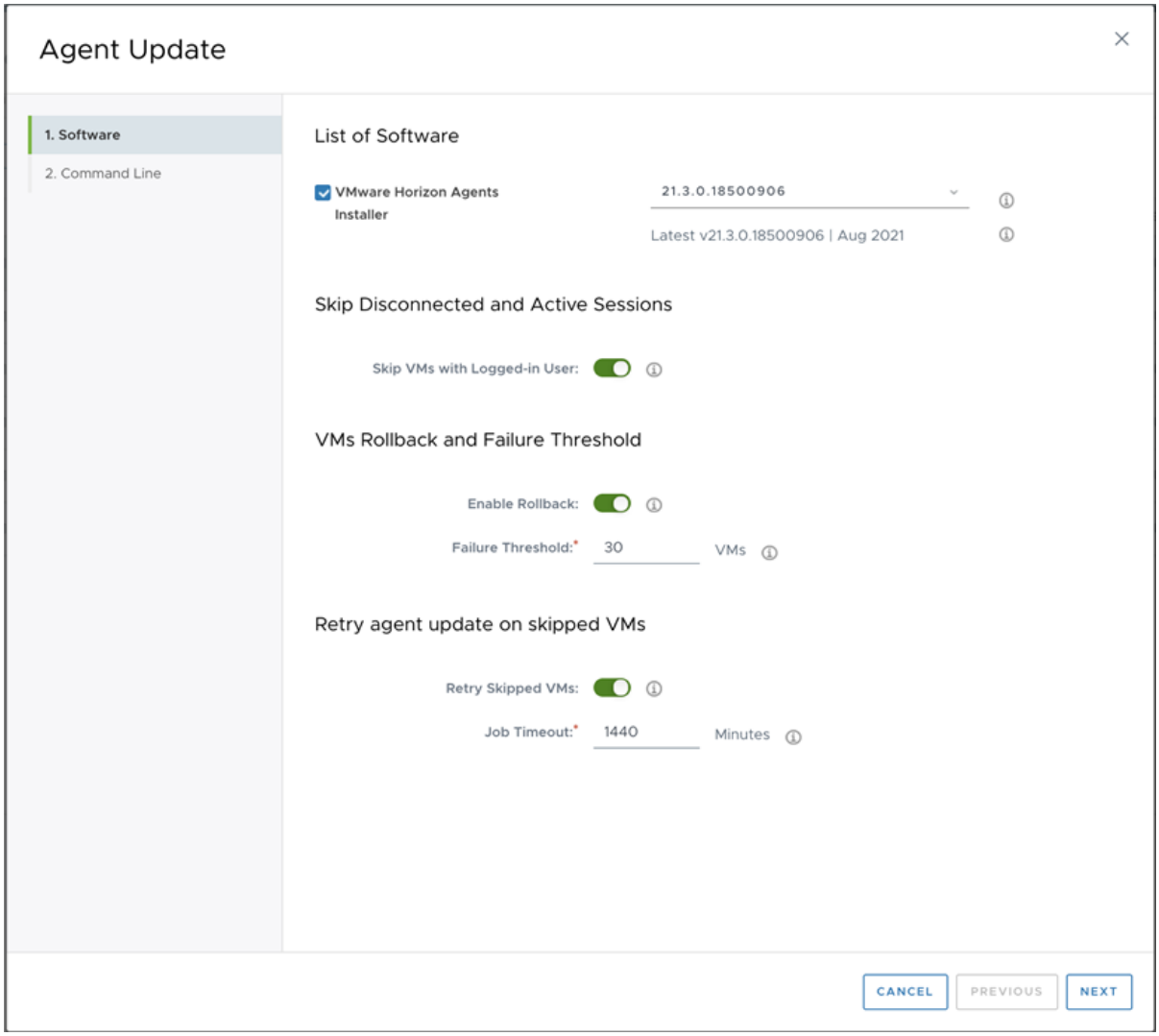
5 更新する各デスクトップの横にあるチェック ボックスを選択します。

割り当てに更新されたデスクトップが含まれている場合は、以前のエージェント バージョンでリストをフィルタリングできます。以前のエージェント バージョンとは、更新前にデスクトップで実行されていたエージェント バージョンを指します。このフィルタリングにより、更新の対象となるデスクトップにリストが絞り込まれます。

マルチクラウド割り当ての場合、フィルタリング オプションはデスクトップ リストの [エージェントのステータス] 列から使用できます。

6 [エージェント] - [エージェントのアップデート] の順に選択します。

アップデート ウィザードが表示されます。



7 [ソフトウェア] 手順で、ドロップダウン メニューから使用するアップデートのバージョンを選択します。

注： Microsoft Windows 7 を使用している割り当ての場合は、Horizon Agent Installer 20.3.x を選択する必要があります。

8 （オプション） ログインしているユーザー（アクティブまたは切断されたセッション）または競合するタスクが実行されているデスクトップをスキップするには、[ログイン ユーザーがいる仮想マシンをスキップ] トグルを有効化します。

9 （オプション）[ロールバックを有効にする] トグルを有効にすると、システムはエージェントの更新が実行される前にロールバック コピーを作成し、そのコピーを 7 日間保持します。この 7 日間においては、仮想マシンでエージェントの更新に失敗した場合、その仮想マシンの以前のエージェント バージョンにロールバックすることができます。詳細については、これらの手順の最後にある「次の手順」を参照してください。

注： ロールバックの時間枠はデフォルトで 7 日間に設定されていますが、この設定の変更を VMware に要求することもできます。

10 （必須）[障害のしきい値] には、更新プロセスが停止となるまでに許容される、エージェントの更新が失敗する仮想マシンの数を入力します。このしきい値により、大量の障害が発生するのを防ぎます。

デフォルト値は、[設定] - [全般設定] で構成したものです。

11 （オプション） スキップされた仮想マシンを自動的に再試行するには、[スキップされた仮想マシンを再試行] トグルを有効にします。

12 （オプション）[ジョブのタイムアウト] フィールドで、スキップされた仮想マシンの更新をシステムが自動的に試行する期間を指定します。

[ジョブのタイムアウト] フィールドは、スキップされた仮想マシンの更新をシステムが再試行する分数を設定します。システムは、この時間に到達するまで、または割り当てのすべてのデスクトップ仮想マシンが更新されるまで、30 分ごとにスキップされた仮想マシンを更新します。

120 分（2 時間）から 1440 分（24 時間）までの値を入力できます。デフォルト値は 720 分（12 時間）です。

13 [次へ] をクリックします。

14 （オプション） コマンド ラインの手順で、イメージでのこのアップデートに関係する可能性がある任意のコマンドライン オプションを追加します。

ウィザードには、指定されたアップデートに対してコマンドライン オプションが利用可能かどうかを示すメッセージが表示されます。

15 [送信] をクリックします。

注： 環境がマルチクラウド割り当て用に構成されている場合、[送信] は選択できません。[次へ] をクリックして [サマリ] ページを確認し、[終了] をクリックします。

結果

- アップデートが開始されたことを示すメッセージがページの最上部に表示されます。
- システムにより、パワーオン状態のデスクトップで再起動が実行され、デスクトップ仮想マシン上のエージェントに関連するコンポーネントが更新されます。

[監視] - [アクティビティ] の順に選択すると、アップデート タスクの進捗を表示できます。

次のステップ

[割り当て - VDI デスクトップ] ページに移動して、更新が成功したかどうかを確認します。

リストされた仮想マシンの詳細をダウンロードするには、[監視] - [アクティビティ] を選択し、エージェントの更新タスクを選択し、[サマリ] ページで [詳細のダウンロード] をクリックします。

システムは、アクションを実行できる仮想マシンに関するステータス情報を提供する CSV ファイルをダウンロードします。各仮想マシンのアップグレード ステータスを使用して、実行するアクションを決定できます。

エージェントの更新の実行時にロールバックを有効にしている場合は、失敗した仮想マシンの割り当ての横にビジュアル インジケータが表示されます。割り当ての詳細ページの [デスクトップ] タブで、失敗した各仮想マシンを以前のエージェント バージョンにロールバックすることができます。割り当ての詳細ページで実行できるアクションの詳細については、Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた割り当ての管理を参照してください。

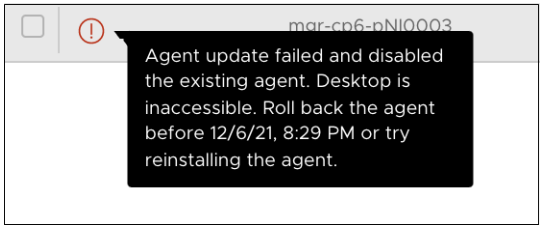
エージェントのアップグレードの失敗によってエージェントがオフライン状態のままになった場合、デスクトップはエージェントの再インストール操作の対象になります。専用 VDI デスクトップ割り当ての個々のデスクトップ上のエージェント ソフトウェアを再インストールするを参照してください。

専用 VDI デスクトップ割り当ての個々のデスクトップ上のエージェント ソフトウェアを再インストールする

専用 VDI デスクトップ割り当てのデスクトップでエージェントのアップグレードに失敗する場合、デスクトップでエージェントを再インストールできる場合があります。具体的には、アップグレードの失敗によってエージェントがオフライン状態のままになった場合、デスクトップはエージェントの再インストール操作の対象となり、[デスクトップ] ページからこの操作を実行できます。

エージェント ソフトウェアの更新を実行するときに、[ロールバックを有効にする] オプションを選択すると、後で以前のバージョンのエージェントにロールバックするオプションが表示されます。エージェントの更新を実行した後、エージェントの更新に失敗すると、ツールチップに障害に関する特定の情報が表示されます。たとえば、エージェントの再インストールを試行できることを示すメッセージが表示される場合があります。Horizon Agent ソフトウェアの更新の詳細については、該当するトピック、専用 VDI デスクトップ割り当ての [割り当て] ページでエージェント ソフトウェアを更新するまたは専用 VDI デスクトップ割り当ての個々のデスクトップ上のエージェント ソフトウェアを更新するを参照してください。

図 6-5. 失敗したエージェント更新のツールチップの例



デスクトップにエージェント ソフトウェアを再インストールすると、システムはデスクトップに使用可能な最新のエージェント ソフトウェアをインストールしようとします。ターゲット デスクトップ OS タイプにインストールする Horizon Agent 機能をカスタマイズすることもできます。各機能の詳細については、ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリングで説明されている [詳細オプション] を参照してください。

手順

1 失敗した割り当ての名前をクリックし、[デスクトップ] をクリックします。

[デスクトップ] ページには、ステータスが失敗としてリストされているデスクトップを含むすべてのデスクトップが一覧表示されます。このようなステータス アイコンにカーソルを合わせるとツールチップが表示され、エージェントの再インストールが推奨される場合があります。

2 再インストールの操作を実行するすべてのデスクトップの横にあるチェック ボックスをオンにします。

3 [エージェント] - [エージェントの再インストール] の順に選択します。

[Horizon Agent の再インストール機能] ページが表示されます。

4 必要に応じて機能をオンまたはオフにし、[再インストール] をクリックします。

機能の詳細については、これらの手順の前に記載されているリファレンス情報を参照してください。

結果

システムは Horizon Agent の再インストールを開始します。

次のステップ

再インストール プロセスのステータスを監視するには、[監視] - [アクティビティ] の順に移動します。プロセスが完了すると、システムは失敗ステータス アイコンを削除されます。

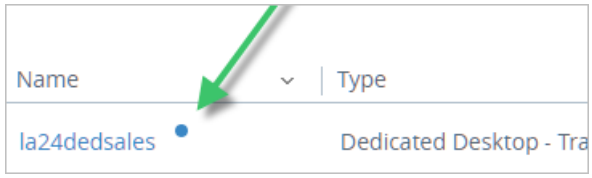
専用 VDI デスクトップ割り当てに対するエージェントのアップデート機能の仕組み

ここでは、専用の VDI デスクトップ割り当てに対する Horizon Cloud のエージェントのアップデート機能の仕組みを高いレベルで説明します。

この概要は、割り当てと個々のデスクトップの両方に適用されます。

システムは VMware CDS（コンポーネント ダウンロード サービス）ソフトウェア配布ネットワークと定期的に通信して、Horizon Agents Installer の新しいバージョンが使用可能かどうかを確認します。使用可能の場合、システムは自動的にそのバージョンを Horizon Cloud ポッドにダウンロードします。

割り当てレベルで、新しいバージョンがダウンロードされると、その割り当てが表示される管理コンソールのページに、更新が利用可能であることが反映されます。新しいバージョンより前のレベルでのエージェントに関連するソフトウェアがあるそれらの専用 VDI デスクトップ割り当てに対してビジュアル インジケータが表示されます。



専用 VDI デスクトップ割り当ての [割り当て] ページでエージェント ソフトウェアを更新すると専用 VDI デスクトップ割り当ての個々のデスクトップ上のエージェント ソフトウェアを更新するの手順に従って専用 VDI 割り当てを選択し、エージェントのアップデート ウィザードを開始すると、更新が開始されます。更新に使用するバージョンを選択するだけでなく、次のオプションを指定できます。

オプション	説明
[ユーザーが利用可能な仮想マシン]	この [ユーザーが利用可能な仮想マシン] オプションは、個々のデスクトップを更新するときではなく、割り当てを更新するときにのみ使用できます。 このフィールドを使用して、更新中にユーザーが利用可能な割り当ての仮想マシンの比率を指定します。このオプションは、デスクトップが 30 台または 30 台の 2 ～ 3 倍 (60 台または 90 台) 未満である小規模デスクトップ割り当てに有用です。 システムはデフォルトで 30 台単位でデスクトップをバッチ更新するので、割り当てに 30 台以下のデスクトップがある場合、すべてのデスクトップが同時に更新プロセスを開始します。すべてのデスクトップが更新プロセスを実行していると、その更新プロセスが完了するまで、資格付与されたユーザーがデスクトップに新たに接続することができません。エージェントの更新プロセスは、更新されたデスクトップがエンドユーザー接続の準備が整えるまで、約 30 分かかります。同様に、デスクトップ割り当てのデスクトップ数が約 60 の場合、デフォルト バッチの 30 台だと約 50% のデスクトップが使用不能になります。 そのため、このフィールドを使うことで、システムがデスクトップを更新する際に、小規模プールでより多くの割合を確実に利用可能にすることができます。利用可能割合をより高く設定することで、仮想マシン更新の各バッチにおけるデスクトップの数が調整されることになります。 多数のデスクトップがある割り当てでは、割り当てにおけるデスクトップの総数に対してシステムの最大デフォルトである 1 バッチ 30 台の仮想マシンは小さな割合にしかならないので、このオプションはほとんど有用ではありません。
[ログイン ユーザーがいる仮想マシンをスキップ]	ログインしているユーザー (アクティブまたは切断されたセッション) が存在する仮想マシン、または競合するタスクを実行している仮想マシンの更新がシステムによってスキップされるように設定します。この設定は、更新プロセスがデスクトップ上で起動した際に、エンド ユーザーを強制的にログオフにしてしまうシステムのデフォルト挙動を回避できます。
[ロールバックを有効にする]	(オプション) ロールバックが有効になっている場合、システムはエージェントの更新が実行される前にロールバック コピーを作成し、そのコピーを 7 日間保持します。この 7 日間においては、仮想マシンでエージェントの更新に失敗した場合、その仮想マシンの以前のエージェント バージョンにロールバックすることができます。 **注：** ロールバックの時間枠はデフォルトで 7 日間に設定されていますが、この設定の変更を VMware に要求することもできます。

オプション	説明
[障害のしきい値]	更新プロセスが停止となるまでに許容される、エージェントの更新が失敗する仮想マシンの数。このしきい値により、大量の障害が発生するのを防ぎます。 デフォルト値は、[設定] - [全般設定] で構成したものです。 **注：** 仮想マシンの更新に失敗したことが原因で更新プロセスが停止した場合、設定したしきい値よりも多くの障害が発生した仮想マシンが表示されることがあります。これは、さまざまな理由で発生します。マルチポッドの割り当ての場合、システムは割り当てごとではなく、ポッドごとにしきい値設定を適用するため、この問題が発生する可能性があります。
[スキップされた仮想マシンを再試行] と [ジョブのタイムアウト]	ログインしているユーザーのいる仮想マシン、または競合するタスクを実行している仮想マシンの更新をスキップするように指定した場合、オプションでスキップされた仮想マシンの更新をシステムにより自動的に再試行するかどうかを指定することができます。この場合、割り当て内のデスクトップ仮想マシンをスキャンし、ログイン ユーザーのいない仮想マシンを更新してから、システムは次を実行します。 1 当初スキップした仮想マシンにログイン ユーザーがいるか確認します。 2 スキップされた仮想マシンでログイン ユーザーがいないものについてはすべて更新します。 3 手順 1 および 2 を、[ジョブのタイムアウト] フィールドで指定した時間が経過するまで定期的に繰り返します。 システムによるスキップされた仮想マシンの自動再試行を設定しない場合は、後でそれらの仮想マシンを手動で処理することができます。 **注：** 更新プロセス中にエラーが発生した仮想マシンについては再試行は行われません。仮想マシンの更新に失敗した場合は、ロールバック オプションを有効にしておくと、仮想マシンを以前のバージョンにロールバックできます。

- ウィザードの最後のステップで更新タスクを送信した後、システムはデスクトップの更新を開始します。
  - 各デスクトップ仮想マシンで更新プロセスが開始されたら、仮想マシンの状態が健全であることを確認するプリフライト チェックが開始されます。これには、十分なディスク容量があること（300 MB 以上の空き容量）と、2 回の再起動によってクリアされていない Windows 更新プログラムによる再起動が行われていないこと、または 2 回の再起動によってクリアされない VMware 固有のアプリケーションのインストールによる再起動が行われていないことの確認が含まれます。
  - 更新が割り当てまたは個別デスクトップレベルで発生すると、システムは仮想マシンのバッチを並行して更新します。デフォルトでは、更新する仮想マシンの残りの数が 30 未満になるまで、システムはバッチごとに 30 台の仮想マシンを使用します。30 未満になった時点で、最終セットは、それらの残りの仮想マシンを更新するためのものです。仮想マシンを完全に更新するには約 30 分から 45 分かかります。必要な時間は負荷によって、また、ロールバック オプションが有効になっているかどうかによっても異なります。バッチのサイズを、30 よりも大きくすることはできません。割り当てに含まれるデスクトップが 30 台以下である場合、割り当てのすべてのデスクトップが同時にアップデートされます。ご要望に応じて、VMware の担当者がバッチのサイズを調整できます。

更新がデスクトップ レベルではなく割り当てレベルで行われる場合は、[ユーザーが利用可能な仮想マシン] テキスト ボックスを構成して、パワーオン状態でエンド ユーザーが利用できるようにする割り当て内のデスクトップ仮想マシンの割合を指定できます。処理中の仮想マシンの数は、更新中に利用可能に保つ仮想マシンの割合を指定したかどうかによって変わります。利用可能割合を設定すると、システムは、利用可能割合を満たすために更新中の仮想マシンのセットを調整します。次の表にいくつかの例を示します。

注： [監視] - [アクティビティ] ページで更新の進行状況を表示すると、実行中の仮想マシンの数がバッチ サイズに基づいて予測される数よりも大きくなることがあります。これは、システムがプリフライト チェックおよびロールバック コピーの作成プロセスで現在実行されている仮想マシンもカウントしているために発生します。

例	説明
[ユーザーが利用可能な仮想マシン] が設定されていない (= 0%)	利用可能割合を設定しない場合、利用可能割合は 0 であり、ランタイム バッチ サイズはデフォルトの 30 になります。割り当てのデスクトップ数が 30 台以下の場合、その割り当て内のすべてのデスクトップが 1 つのバッチでまとめて更新されます。
割り当てのデスクトップ数が 20 台で [ユーザーが利用可能な仮想マシン] = 80%	20 台のデスクトップがある割り当てで、その 80% を利用可能に保ちたい場合、システムは常時 16 台を利用可能にしておく必要があります。この場合、システムは次のように実行します。 1 最初に 4 台の仮想マシンから成るバッチを更新します（20 - 16）。 2 4 台の更新済み仮想マシンと 12 台の未更新仮想マシンで 16 台が利用可能に保たれるので、2 回目のバッチで 4 台の仮想マシンを更新します。 3 この時点では、8 台の仮想マシンが更新済みで 12 台が未更新です。システムは、未更新の仮想マシンに対して 4 台のバッチで更新を続けます。それぞれの後続のバッチで、利用可能に保たれるのは更新された仮想マシンと未更新の仮想マシンを組み合わせたものです。
割り当てのデスクトップ数が 100 台で [ユーザーが利用可能な仮想マシン] = 80%	100 台のデスクトップがある割り当てで、その 80% を利用可能に保ちたい場合、システムは常時 80 台を利用可能にしておく必要があります。この場合、システムは次のように実行します。 1 最初に 20 台の仮想マシンのバッチを更新します（100 - 80）。 2 20 台の更新済み仮想マシンと 60 台の未更新仮想マシンで 80 台が利用可能に保たれるので、2 回目のバッチで 20 台の仮想マシンを更新します。 3 この時点では、40 台の仮想マシンが更新済みで 60 台が未更新です。システムは、未更新の仮想マシンに対して 20 台のバッチで更新を続けます。
割り当てのデスクトップ数が 100 台で [ユーザーが利用可能な仮想マシン] = 25%	割り当てのデスクトップ数が 100 台で、その 25% を利用可能に保ちたいのであれば、75 台の仮想マシンを最初に更新することができます。この場合、システムは次のように実行します。 1 最初に更新するのは、デフォルトのバッチ サイズである 30 台の仮想マシンで、70 台が未更新になります。 2 70 台の未更新分から 2 回目のバッチで 30 台の仮想マシンが更新されるので、総数 100 台のデスクトップのうち 60 台が更新され、40 台が未更新になります。 3 ここで 60 台が更新されているので、更新済み仮想マシン 25 台で 25% の利用可能割合設定を満たすことができます。そのため、システムはデフォルトのバッチ サイズを使用して、残り 40 台の未更新仮想マシンのうちの 30 台を更新します。 4 システムは、最終バッチで残りの仮想マシン 10 台を更新します。

エージェントの更新プロセスの最後で、割り当ての [サマリ] ページに、有効になっている Horizon Agents Installer のバージョンが示されます。

システムがデスクトップを更新している間、デスクトップのエンド ユーザーは次の挙動に遭遇します。

- デスクトップにアクティブなセッションがあってアクティブなユーザーがいる仮想マシンのスキップを指定しなかった場合、更新が発生するまでの 5 分間ユーザーに警告が表示されます。この 5 分間の警告は、ユーザーに処理中の作業を保存する時間を与えるためのものです。
- 更新中のデスクトップにユーザーがログインしようとした場合、ログインは失敗して、デスクトップを利用できないというメッセージが表示されます。

[監視] > [アクティビティ] の順に選択すると、アップデート タスクの進捗を表示できます。タスクの説明欄には、実行されている更新と、更新が実行されている割り当てが表示されます。タスクが 24 時間以内に問題なく完了せず、再試行およびジョブ タイムアウトのオプションが有効になっていない場合、その更新タスクは失敗状態で表示されます。

更新タスクにおいて、いずれかの仮想マシンがスキップされた場合、その更新タスクは [アクティビティ] ページで「部分的に成功しました」状態になります。[アクティビティ] ページでは、その更新タスクでスキップされた仮想マシンの数を確認することができます。

- 再試行オプションが有効化されても、更新タスクの完了後に [アクティビティ] ページにスキップされた仮想マシンの数が表示される場合は、[ジョブのタイムアウト] の値が、システムがすべてのスキップされた仮想マシンを更新するために十分な時間ではない、またはエンド ユーザーがこれらの仮想マシンからログアウトしていません。
- 仮想マシンは、「Windows 更新プログラムの進行中」、「低ディスク容量」、「マシン上での再起動の保留中」などのプリフライト チェック エラーでスキップすることもできます。

何らかの理由でスキップされた仮想マシンの場合、管理者は後でエージェントの更新を再試行できます。

Horizon Cloud ポッド - フローティング VDI デスクトップ割り当てによって使用されるイメージのエージェント ソフトウェアを更新する

フローティング VDI デスクトップ割り当てで使用されるイメージ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を更新するには、最初にイメージ上で [エージェントのアップデート] アクションを使用します。次にこれらの更新されたイメージを使用するフローティング VDI デスクトップ割り当てを編集します。

概要レベルでは、システムのエージェントのアップデート機能は次のように機能します。

- システムは VMware CDS（コンポーネント ダウンロード サービス）ソフトウェア配布ネットワークと定期的に通信して、Horizon Agents Installer の新しいバージョンが使用可能かどうかを確認します。使用可能の場合、システムは自動的にそのバージョンを Horizon Cloud ポッドにダウンロードします。
- 新しいバージョンがダウンロードされた後、管理コンソールには、アップデートの対象となるイメージにアップデートが利用可能であることが示されます。新しいバージョンより前のレベルでのエージェントに関連するソフトウェアがあるそれらのイメージに対してビジュアル インジケータが表示されます。
- エージェントのアップデート中は次のようになります。
  - システムは選択したイメージをパワーオンして、そのパワーオン状態のイメージから仮想マシン (VM) の複製をクローン作成し、元の公開済みの状態に戻すために選択したイメージに対してイメージへの変換プロセスを実行します。プロセスのこの部分においては、コンソールに表示されるイメージのステータスが「公開済み」から「移行中」に変わります。

  - 重複した仮想マシンが存在する場合、システムはそれをパワーオンして、ウィザードで選択された新しい更新バージョンのエージェントに関連するソフトウェアをインストールしてから、その重複仮想マシンに対してイメージへの変換プロセスを実行して公開します。
- エージェントのアップデート プロセスの最後で、元のイメージとその複製イメージ（アップデートされたエージェント ソフトウェアがインストールされている）の両方が一覧表示されます。

重要： エージェントの更新プロセスの最後で、[エージェントの更新] をクリックしたときに選択したイメージは、元のエージェントのバージョン レベルで、プロセスが開始したときと同じ状態になります。新しい複製イメージは、選択したアップデート レベルでエージェント ソフトウェアを取得します。

エージェントのアップデート プロセスにより、エージェントに関連するソフトウェアがウィザードで指定するバージョンに更新された状態で、元のイメージの複製である新しい割り当て可能なイメージが生成されます。エージェントのアップデート ワークフローは、新しい仮想マシンを作るために自動的に元のイメージのクローンを作成し、指定されたレベルのエージェントに関連するソフトウェアをその仮想マシンにインストールして、その仮想マシンを割り当て可能な（公開済み）イメージに変換します。このシステムは、元のイメージの名前にダッシュと数字を付加した形式に基づいて、新しいイメージの名前を付けます。たとえば、元のイメージの名前が SalesGold である場合、エージェントのアップデート プロセスにより SalesGold-2 という名前のイメージが生成されます。プロセスの最後で、両方のイメージがコンソールに表示されます。

以下のスクリーンショットは、あるイメージに対してエージェントのアップデートを実行して最新の利用可能な更新バージョンを選択した後に一覧表示される 2 つのイメージを示しています。元のイメージがプロセスの最後で変更されないため、青いドットはその横に表示されたままになります。別のイメージには更新レベルのエージェント ソフトウェアが含まれていて、より新しい更新バージョンはシステムに存在しないため、そのイメージの横には青いドットが付いていません。

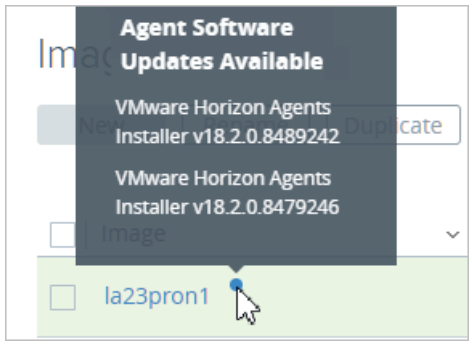
手順

1 [インベントリ] をクリックし、割り当てで使用されるイメージが表示されているイメージ関連のページに移動します。

  選択されたページでは、アップデートを適用する対象のすべてのイメージの名前の横に青いドットが表示されます。青いドットの上にカーソルを置くと、そのイメージで使用可能な Horizon Agents Installer の新しいバージョンを示すポップアップが表示されます。

  次のスクリーンショットは、エージェントの更新が la24win10N という名前のイメージに対して利用可能であることを示しています。

どのようなアップデートが利用可能であるかを確認するには、その青いドットにカーソルを置きます。

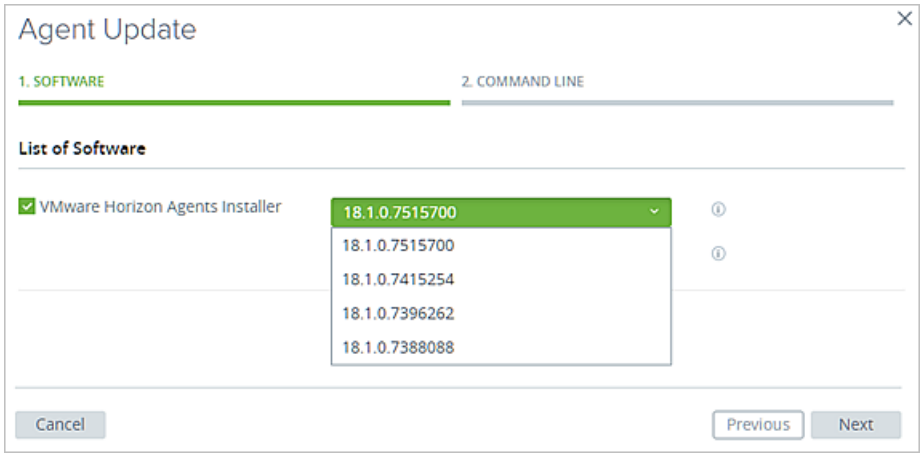


2 更新するイメージの横にあるチェック ボックスを選択します。

3 [エージェントのアップデート] をクリックします。

[エージェントのアップデート] ウィザードが表示されます。

4 [ソフトウェア] 手順で、ドロップダウン リストから使用するアップデートのバージョンを選択して、[次へ] をクリックします。



5 (オプション) コマンド ラインの手順で、イメージでのこのアップデートに関係する可能性がある任意のコマンドライン オプションを追加します。

ウィザードには、指定されたアップデートに対してコマンドライン オプションが利用可能かどうかを示すメッセージが表示されます。

6 [送信] をクリックします。

- アップデートが開始されたことを示すメッセージがページの最上部に表示されます。
- システムは、元のイメージのクローン仮想マシン (VM) を作成し、そのクローン イメージにエージェントに関連するコンポーネントをアップデートします。クローン イメージがアップデートされた後、システムはデスクトップへの変換プロセスを実行して、クローン イメージを公開済みのイメージに変換します。

[監視] > [アクティビティ] の順に選択すると、アップデート タスクの進捗を表示できます。タスクが 24 時間以内に正常に完了しない場合は、障害のステータスで表示されます。

次のステップ

- 元のイメージを使用しているフローティング VDI デスクトップ割り当てが新しい複製イメージを使用するように、割り当てを編集して更新します。そのイメージには更新されたエージェント ソフトウェアが含まれています。割り当てで [編集] アクションを選択し、開いたウィンドウで [イメージ] フィールドを見つけて、新しい複製イメージを選択し、保存します。
- 元のイメージを使用している専用 VDI デスクトップ割り当てがあり、それらを同じエージェントのレベルに移動する場合は、専用 VDI デスクトップ割り当て用のエージェント ソフトウェアを更新するの手順に従ってこれらの割り当てのエージェントを更新します。

  重要： 新しい複製イメージを使用するように専用 VDI デスクトップ割り当てを編集できる場合でも、その方法で更新されるのは未割り当てのデスクトップ仮想マシンのみになります。専用 VDI デスクトップ割り当て内のすべてのデスクトップ仮想マシン上のエージェントを更新する場合は、専用 VDI デスクトップ割り当て用のエージェント ソフトウェアを更新するの手順を使用します。
- 元のイメージを使用していた割り当てを更新済みで、組織で元のイメージが不要になったと判断できる場合は、元のイメージを削除できます。組織内の他の管理者が、低いレベルのエージェントのあるイメージを使用しないようにするために、元のイメージを削除することはベスト プラクティスです。

Microsoft Azure にデプロイされた Horizon Cloud ポッドの管理

顧客アカウントに最初のクラウド接続のポッドがあり、Active Directory ドメインをすべて登録したら、追加のポッドをデプロイして、Horizon Universal Console を使用して、ポッド フリートを操作することができます。Microsoft Azure にデプロイされたポッドの場合、必要に応じて、キャパシティ制限の監視や保存されているサブスクリプション情報の更新または保存されている未使用のサブスクリプション情報の削除など、それらを管理するタスクを実行できます。また、ポッドを編集して、その設定（ゲートウェイの構成など）を変更することもできます。

ポッドを操作するには、主に [キャパシティ] ページとポッドの個別の詳細ページを使用します。[キャパシティ] ページからポッドの詳細ページに移動します。[キャパシティ] ページの詳細については、3 章 第 1 世代テナント - 第 1 世代 Horizon Cloud がサポートするすべてのポッド タイプのクラウド接続ポッドの管理を参照してください。

[キャパシティ] ページ以外に、[ダッシュボード] ページを使用して、ポッド全体の健全性、割り当てられたキャパシティと使用率、およびユーザー アクティビティのスナップショット ビューを取得できます。第 1 世代のテナント - 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を参照してください。

IT またはセキュリティ組織で、Horizon Cloud on Microsoft Azure 環境のサブスクリプションでの Azure Marketplace オファーの使用またはマーケットプレイスでの購入に制限がある場合、または環境で Azure China を使用している場合

このドキュメント ページでは、Horizon Cloud on Microsoft Azure のデプロイおよびアップグレード プロセスでの Azure Marketplace の使用に関連する要件、およびサポート リクエストで VMware のサポートによるトラブルシューティング ジャンプ ボックスのデプロイが必要な場合について説明します。

この情報は、ユーザーまたはユーザーの IT 組織またはセキュリティ組織が Horizon Cloud on Microsoft Azure 環境のサブスクリプションに Azure Marketplace オファーまたは Azure Marketplace の注文の使用に関する制限を設定している場合に関係します。

また、Azure China に Horizon Cloud on Microsoft Azure 環境がある場合は、このページの Azure China - 特別な考慮事項セクションで説明されているように、VMware のサポート チームによるサポートが必要になる場合があります。

簡単な紹介

2022 年初頭から、このサービスは、Azure Marketplace で提供される VMware オファーをプログラムで使用するための Horizon Cloud on Microsoft Azure デプロイヤとアップグレード コードを強化しました。

この機能強化により、最初のデプロイ プロセスとアップグレード プロセスがより迅速に実行され、ポッド マネージャ インスタンスと Unified Access Gateway インスタンスのダウンタイムがほぼゼロのアップグレードが実現されます。

また、この機能強化により、追加のストレージ アカウントを使用せずに、App Volumes 機能に使用される 1 つのストレージ アカウントだけでデプロイとアップグレードを実行することもできます。

Azure Marketplace とデプロイ、アップグレード、およびサポート ジャンプ ボックスの関係

デプロイおよびアップグレード中に、デプロイヤとアップグレード コードは、API 呼び出しによって、プログラムで、`vmware-inc` という名前の VMware の publisherID に対応する Azure Marketplace での VMware オファーの条件に同意しようとします。

関連エンティティ	publisherID	offerID	planID
ポッド マネージャ	vmware-inc	euc-hcs-podmgr	euc-hcs-podmgr
Unified Access Gateway	vmware-inc	euc-hcs-uag	euc-hcs-uag
ジャンプ ボックス（トラブルシューティングを行うために VMware のサポートで必要な場合）	vmware-inc	euc-hcs-jumpbox	euc-hcs-jumpbox

注： Azure ポータルを使用して Azure Marketplace に移動してこれらのオファーを表示することはサポートされていません。VMware は、API 呼び出しを使用したプログラムによるアクセスのためにこれらのオファーを公開します。

サービスの API 呼び出しの要件

このプログラムによる方法が成功するには、Horizon Cloud on Microsoft Azure 環境の Azure サブスクリプションは以下のセクションで説明する要件を満たす必要があります。

これらの項目は、上記の表に記載されている VMware の publisherID、offerID、および planID に対応する Azure Marketplace での VMware オファーの条件に同意するために、デプロイヤおよびアップグレード API 呼び出しに提供されます。

これらの要件は、ポッド マネージャ インスタンスで使用されるサブスクリプションと、Unified Access Gateway インスタンスが独自のサブスクリプションにデプロイするときに使用するサブスクリプションの両方に適用されます。

Azure サブスクリプションで次の項目が満たされていない場合、オファー条件に同意するためのデプロイヤとアップグレード コードの API 呼び出しが失敗し、次の結果になります。

- そのサブスクリプションに関連する新しいデプロイに失敗する。
- そのサブスクリプションにすでにデプロイされているポッド マネージャと Unified Access Gateway インスタンスのアップグレードに失敗する。
- VMware のサポートによるサポート リクエストのトラブルシューティングに必要なトラブルシューティング ジャンプ ボックスをそのサブスクリプションにデプロイできない。

1 つの特別な状況は、Azure China に配置された Horizon Cloud on Microsoft Azure 環境のシナリオです。Azure China では、Microsoft はサービスの API 呼び出しに必要な Microsoft.Marketplace.Ordering リソース タイプを提供しません。Horizon Cloud on Microsoft Azure 環境が Azure China にある場合は、Azure China - 特別な考慮事項セクションのガイダンスをお読みください。

環境のサービス プリンシパルがカスタム ロールを使用する場合の要件

ここで説明するとおりにカスタム ロールを使用する場合、次の権限をカスタム ロールに含める必要があります。

```
Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read
Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write
```

- ポッド マネージャ インスタンスまたは Unified Access Gateway インスタンスの新しいデプロイの場合、ユーザー インターフェイスのデプロイ ウィザードで、サービス プリンシパルがサブスクリプションでこれらの権限を持っているかどうかを検証します。検証に失敗すると、ユーザー インターフェイスによってデプロイが開始されません。
- アップグレードの場合、システムの事前確認は、サービス プリンシパルがサブスクリプションでこれらの権限を持っているかどうかを確認しようとします。持っていない場合、事前確認で更新をブロックするエラーが報告されます。このエラーを解決するには、これらの権限をカスタム ロールに含めます。
- VMware のサポートがサポート リクエストに対応するためにトラブルシューティング用のジャンプ ボックスをデプロイする必要がある場合、ジャンプ ボックスのデプロイ プロセスは、権限がないことを VMware のサポートに示します。

このシナリオでは、VMware のサポート チームは、「構成済みのサブスクリプションにマーケットプレイスのイメージ オファーを使用するための十分な読み取り権限がないため、アップグレードを続行できませんでした。構成済みのサブスクリプションにマーケットプレイスのイメージ オファーを使用するための十分な書き込み権限がないため、アップグレードを続行できませんでした」のようなパターンでログに記録されたエラー メッセージを確認します。

Azure ポリシーがサブスクリプションで許可される Azure リソース タイプを制限する場合の要件

一部の IT 組織の Azure ポリシーでは、名前で明示的に許可されている特定のリソース タイプを除き、Azure リソース タイプのすべての使用を禁止するように指定されている場合があります。

IT またはセキュリティ組織が、組織の Azure サブスクリプションで許可される Azure リソース タイプを制限する Azure ポリシーを設定している場合、Azure ポリシーの AllowedResourceTypes セットに、リソース タイプ `Microsoft.MarketplaceOrdering/*` を含める必要があります。

サブスクリプションの Azure ポリシーに `Microsoft.MarketplaceOrdering/*` が含まれていない場合、VMware のサポート チームは、「**検証エラーのため、**`PublisherId: 'vmware-inc'`**、**`OfferId: 'euc-hcs-xxxxx'` **のオファーを購入できません。**`IT` **管理者が設定したポリシーに従って、発行者** `'vmware-inc'` **のオファー** `'euc-hcs-xxxxxx'` **の** `Sku 'euc-hcs-xxxxxx'` **は利用できません**」のようなパターンでログに記録されたエラー メッセージを確認します。ここで `xxxxx` は前述の表の planIDs のいずれかに対応します。

`Microsoft.MarketplaceOrdering/*` リソース タイプへのアクセスを許可すると、デプロイヤとアップグレード コードは、デプロイヤとアップグレード コードが使用する Azure Marketplace の VMware Horizon Cloud on Microsoft Azure オファーを受け入れる API 呼び出しを行うことができます。

IT チームまたはセキュリティ チームがサブスクリプションでこのリソース タイプの許可を拒否した場合、次のセクション**エンタープライズの Azure プライベート ストア コレクションへの VMware オファーの追加**で説明するアクションを実行して、VMware オファー SKU をエンタープライズの Azure プライベート ストアに追加するオプションを使用できます。その後、サービスの API 呼び出しは、そこから VMware オファーを取得できます。

エンタープライズ管理者が Azure Enterprise テナントの Azure Marketplace 購入をオフに切り替えた場合の要件

Microsoft Azure のドキュメントで説明されているように、エンタープライズ管理者は、エンタープライズ Azure テナントのすべての Azure サブスクリプションの Azure Marketplace 購入をオフに切り替えることができます。

この操作を行うと、Azure Marketplace の購入が Microsoft の発行元からのオファーに制限されます。この制限付き購入により、サービスの API 呼び出しがブロックされ、vmware-inc publisherID から VMware オファーが取得されなくなり、その結果、これらの API 呼び出しを必要とするデプロイおよびアップグレード プロセスが妨げられます。

このシナリオでは、VMware のサポート チームに「**このサブスクリプションの登録ではマーケットプレイス有料製品の購入が許可されていないため、購入を完了できません。**`Azure` **登録管理者がマーケットプレイス有料製品の購入を有効にすることができます**」のようなパターンでログに記録されたエラー メッセージが表示されます。

この状況を解決するには、エンタープライズ管理者にプライベート Azure Marketplace コレクションを作成および管理し、**エンタープライズの Azure プライベート ストア コレクションへの VMware オファーの追加**のアクションを実行して VMware オファーを追加するよう依頼します。

エンタープライズの Azure プライベート ストア コレクションへの VMware オファーの追加

Microsoft Azure は、サブスクリプションで使用するプライベート Azure Marketplace コレクションを作成および管理する機能を提供します。**プライベート Azure Marketplace の作成と管理**で説明されているように、この機能により、IT 管理者は、ユーザーがグローバル Azure Marketplace から使用できるサードパーティ ソリューションを事前に承認、キュレート、および制御できます。前の文でリンクされている Microsoft のドキュメント ページで説明されているように、プライベート ストアを管理する管理者に Marketplace 管理者ロールを割り当てる必要があります。

エンタープライズ Azure テナント用にプライベート ストアが作成されると、Marketplace 管理者ロールを持つ管理者は、プライベート ストア コレクションに VMware オファーを追加できます。テナントのプライベート ストアに VMware オファーを追加すると、サービスの API 呼び出しで、デプロイおよびアップグレードに使用される VMware オファーを取得できます。

Microsoft は、特定の発行者オファーをプライベート ストア コレクションに追加するための PowerShell コマンドを提供します。

プライベート マーケットプレイスにオファーを追加するにある PowerShell コマンドを実行するための前提条件に関する Microsoft のドキュメント参照に従います。この Microsoft ページでは、Microsoft がこの目的のために提供する PowerShell コマンドについても説明されています。

次の例は、コマンドを実行するための前提条件が満たされた後に、そのプライベート ストアに VMware オファーを追加するために使用する Microsoft PowerShell コマンドを示しています。まず、`Get-AzMarketplacePrivateStore` を使用して Azure テナントの `privateStoreId` を取得します。次に、`Set-AzMarketplacePrivateStoreOffer` を使用して、VMware オファーをそのプライベート ストアに追加します。

```
Get-AzMarketplacePrivateStore
```

1 `Get-AzMarketplacePrivateStore` を使用して、次のコマンド セットで使用する Azure テナントの `privateStoreId` を取得します。

```
Get-AzMarketplacePrivateStore
```

2 返された `privateStoreId` を `Set-AzMarketplacePrivateStoreOffer` コマンドで使用して、`euc-hcs-podmgr`、`euc-hcs-uag`、および `euc-hcs-jumpbox` の VMware オファーを追加します。

- ポッド マネージャ インスタンスのオファーを追加します。

```
Set-AzMarketplacePrivateStoreOffer -privateStoreId your-tenant-privateStoreID -offerId
vmware-inc.euc-hcs-podmgr -SpecificPlanIdsLimitation @("euc-hcs-podmgr")
```

- Unified Access Gateway インスタンスのオファーを追加します。

```
Set-AzMarketplacePrivateStoreOffer -privateStoreId your-tenant-privateStoreID -offerId
vmware-inc.euc-hcs-uag -SpecificPlanIdsLimitation @("euc-hcs-uag")
```

- トラブルシューティング用ジャンプ ボックス インスタンスのオファーを追加します。

```
Set-AzMarketplacePrivateStoreOffer -privateStoreId your-tenant-privateStoreID -offerId
vmware-inc.euc-hcs-jumpbox -SpecificPlanIdsLimitation @("euc-hcs-jumpbox")
```

3 VMware オファーがテナントのプライベート ストアに表示されていることを確認します。

```
Get-AzMarketplacePrivateStoreOffer -PrivateStoreId your-tenant-privateStoreID
```

Azure China - 特別な考慮事項

Microsoft は Azure China で Microsoft.Marketplace.Ordering リソース タイプを提供していないため、Azure Marketplace で VMware オファーへの API 呼び出しを使用するサービスの機能はサポートされません。Microsoft.Marketplace.Ordering タイプは、Azure China リソース プロバイダ向けのこの Microsoft ドキュメント参照に記載されていません。

したがって、Horizon Cloud on Microsoft Azure 環境向けに Azure China のサブスクリプションを使用している場合は、次の特別な考慮事項に注意してください。

- Azure China の既存の Horizon Cloud on Microsoft Azure 環境の場合、その環境をアップグレードする前に、VMware のサポートからサポートを受け、Azure Marketplace への API 呼び出しなしで、以前のアップグレード方法を使用するように Horizon Cloud テナントを構成します。
- Azure China へのデプロイを計画する場合は、そのデプロイを開始する前に、VMware のサポートからサポートを受けて、Azure Marketplace への API 呼び出しなしでデプロイヤが以前のデプロイ方法を使用するように Horizon Cloud テナントを構成します。
- VMware のサポートが Azure China にある環境のトラブルシューティングのために一時的なジャンプ ボックスをデプロイする必要がある場合、VMware のサポートは、サービスの Azure Marketplace への API 呼び出しなしで一時的なジャンプ ボックスをサブスクリプションにデプロイできるように、Horizon Cloud テナントを一時的に構成できます。トラブルシューティングのために一時的なジャンプ ボックスをデプロイした後、テナントで Azure China に加えて、複数のリージョンにあるサブスクリプションにポッドがデプロイされている場合に備えて、VMware のサポートはサービスの API 呼び出しの機能を再度有効にできます。

Azure Marketplace を使用しないデプロイとアップグレードの完了には時間がかかります。また、このようなデプロイとアップグレードでは、一時的なジャンプ ボックスを使用して、デプロイとアップグレードのプロセスとサブスクリプション内のストレージ アカウントの使用を調整し、サービスの API 呼び出しが Azure Marketplace で提供される VMware オファーを使用する代わりに、Horizon Cloud 制御プレーンから取得するイメージを保持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

Microsoft Azure にデプロイされた Horizon Cloud ポッドにゲートウェイ構成がある場合、CNAME レコードを DNS サーバに作成する必要があります。この CNAME レコードにより、そのゲートウェイ構成でサービスが構成した完全修飾ドメイン名 (FQDN) が、ポッドのゲートウェイのデプロイされた Azure ロード バランサの情報にマッピングされます。Horizon Universal Console（コンソール）のポッドの詳細ページから、簡単に Azure ロード バランサの情報を取得できます。

この CNAME マッピングでは、Horizon Client および Horizon HTML Access（Web クライアント）で必要とされる名前解決と、エンド ユーザーに使用資格が付与されたポッドプロビジョニングされたリソースに到達するための接続がサポートされています。このマッピングに必要な情報はポッドの詳細ページに表示され、コンソールのキャパシティ ページを使用して移動できます。

適切なマッピングが設定されている場合、Horizon Client と Web クライアントは、エンド ユーザーに使用資格が付与されたポッドプロビジョニングされたリソースに接続するためにドメイン名を解決する必要があるときに、それらを正常に解決できます。

- Universal Broker で構成された環境では、エンド ユーザーはクライアントの Universal Broker 仲介 FQDN を Horizon Client または Web クライアントのサーバ アドレスとして使用します。クライアントは認証のために Universal Broker に接続し、エンド ユーザーの資格を取得します。続いて、認証されたクライアントで、ユーザーが特定の資格のあるデスクトップまたはリモート アプリケーションにアクセスするためにクリックすると、クライアントはポッドのゲートウェイ構成でサービスが構成した FQDN、ポッドのデプロイ ウィザードまたはゲートウェイのデプロイ ウィザードで指定された FQDN にリダイレクトされます。
- シングルポッド仲介を使用して構成された環境では、Horizon Client または Web クライアントのサーバ アドレスに対して、エンド ユーザーはポッドのゲートウェイのポッド デプロイ ウィザードで指定した FQDN を使用します。この FQDN は、Horizon Client と Horizon HTML Access（Web クライアント）が、ポッドから資格のある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使用するものです。クライアントは、認証のために特定のゲートウェイとポッドに接続し、エンド ユーザーの使用資格を取得して、使用資格が付与されたデスクトップまたはリモート アプリケーションにアクセスします。

サービスのデプロイヤ コードがゲートウェイ構成を構成すると、ウィザードのゲートウェイ構成フィールドで指定された、`ourOrg.example.com` や `ourApps.ourOrg.example.com` などの完全修飾ドメイン名 (FQDN) が使用されます。ゲートウェイ構成が外部ゲートウェイ構成の場合、その FQDN はパブリックに解決可能な FQDN である必要があります。Horizon Cloud 制御プレーンは、外部ゲートウェイのデプロイ用に入力された FQDN に関する情報を保存し、その FQDN とインターネット経由で通信します。その結果、Horizon Cloud 制御プレーンはその名前を解決して、そのアドレスに接続できる必要があります。この要件は、テナント環境が Universal Broker で構成されている場合に特に重要となり、満たす必要があります。このような環境では、Horizon Cloud 制御プレーンがその FQDN に接続して、外部ゲートウェイ構成内の Unified Access Gateway インスタンスから認証情報を取得する必要があります。サービスはこの情報を使用して、ゲートウェイ構成の Unified Access Gateway インスタンスで構成された 2 要素認証設定が、参加しているポッド内の Universal Broker 構成およびその他すべての Unified Access Gateway インスタンスの設定と一致することを検証します。

[パブリック IP アドレスを有効にする] トグルをオンにしてデプロイされた外部ゲートウェイ構成（デフォルト）

ポッドのデプロイ ウィザードまたは外部ゲートウェイのデプロイ ウィザードで外部ゲートウェイ構成のパブリック IP アドレスを有効にすることを指定した場合、サービスは、パブリック IP アドレスと自動生成されたパブリック FQDN を持つ Azure ロード バランサ リソースを使用して、デプロイされた Unified Access Gateway インスタンスを構成します。自動生成されるパブリック FQDN の形式は、パターン `vmw-hcs-`*`ID`*`-uag.`*`region`*`.cloudapp.azure.com` です。ここで `vmw-hcs-`*`ID`* は Unified Access Gateway インスタンスが存在するリソース グループの名前のパターンと一致し、*region* は、ポッドが配置されている Microsoft Azure リージョンです。このタイプのデプロイでは、DNS サーバで、デプロイ ウィザードで入力した FQDN を自動生成されたパブリック FQDN にマッピングします。

[パブリック IP アドレスを有効にする] トグルを無効化、オフにしてデプロイされた外部ゲートウェイ構成

プライベート ロード バランサの IP アドレスを使用してポッドの外部ゲートウェイ構成をデプロイするこのシナリオは、外部ゲートウェイ構成の Unified Access Gateway アプライアンスへのアクセスを許可する前に、インターネット ベースのトラフィックを制御する目的でファイアウォールまたは NAT を外部ゲートウェイ構成の Azure ロード バランサの前に構成している場合に使用します。ポッドのデプロイ ウィザードまたは外部ゲートウェイのデプロイ ウィザードで [パブリック IP アドレスを有効にする] トグルをオフに切り替えると、サ

ービスは、プライベート IP アドレスを持つ Azure ロード バランサ リソースを使用して、デプロイされた Unified Access Gateway インスタンスを構成します。DNS サーバで、デプロイ ウィザードに入力した FQDN を、ゲートウェイの Azure 内部ロード バランサ リソースのプライベート IP アドレスにマッピングします。DNS サーバでの CNAME マッピングに加えて、ファイアウォールまたは NAT のセットアップでパブリック IP アドレスが提供されていることと、同じ FQDN がそのファイアウォールまたは NAT によって提供されるパブリック IP アドレスに対してパブリックに解決可能であることを確認する必要があります。

内部ゲートウェイ構成

内部ゲートウェイのデプロイの場合、サービスは、プライベート IP アドレスを持つ Azure ロード バランサ リソースを使用して、デプロイされた Unified Access Gateway インスタンスを構成します。DNS サーバは、ポッドのデプロイ ウィザードまたは内部ゲートウェイのデプロイ ウィザードで内部ゲートウェイ構成に指定された FQDN を、デプロイされた Azure ロード バランサのプライベート IP アドレスにマッピングします。

ポッドの詳細ページには、このマッピングに必要な情報が一覧表示されています。これらの手順を使用して、ポッドの詳細ページで適切な情報を探してください。

前提条件

Microsoft Azure へのポッドの自動デプロイを実行するに記載されているポッドのデプロイ手順に従って、Microsoft Azure 環境にポッドを正常にデプロイする必要があります。

手順

1 コンソールで [設定] - [キャパシティ] に移動し、ポッドをクリックしてその詳細ページを開きます。

2 [サマリ] タブで、ページの一番下までスクロール ダウンし、[Internal UAG（内部 UAG)] および [External UAG（外部 UAG)] というラベルの付いたセクションを探します。

注： ポッドに対応するゲートウェイが構成されているときにのみ、ページにセクションが含まれます。ポッドに内部ゲートウェイのみが設定されている場合、[内部 UAG] セクションのみが表示され、外部のセクションは表示されません。ポッドに両方の構成が設定されている場合、両方のセクションがページに表示されます。

次のスクリーンショットは、内部/外部の両方のタイプの構成が設定されているポッドのページの一部を示しています。

3 ポッドに設定されている各構成で、[ロード バランサの FQDN] フィールドを見つけて、そこに表示されている値をコピーします。

オプション	説明
内部	表示された値は、ゲートウェイ構成における Microsoft Azure ロード バランサ リソースのプライベート IP アドレスです。この数値の IP アドレスは、ポッドのデスクトップ サブネットからゲートウェイのロード バランサ リソースに割り当てられます。
パブリック ロード バランサ IP アドレスがある外部	表示される値は Microsoft Azure ロード バランサ リソースのパブリック FQDN で、`vmw-hcs-`*`podID`*`-uag.`*`region`*`.cloudapp.azure.com` の形式で自動生成されます。region は Microsoft Azure のリージョン、*podID* はポッドの ID 値を表します。そのポッド ID は詳細ページに表示されます。
プライベート ロード バランサ IP アドレスがある外部	表示された値は、Microsoft Azure ロード バランサ リソースのプライベート IP アドレスです。この数値の IP アドレスは、ポッドの DMZ サブネットからロード バランサ リソースに割り当てられます。

4 DNS サーバで、そのロード バランサの FQDN の値をポッドのデプロイ時にウィザードから提供された FQDN にマッピングします。

オプション	説明
内部	`ourApps.ourOrg.example.com  Azure-load-balancer-private-IP`
パブリック ロード バランサ IP アドレスがある外部	`ourApps.ourOrg.example.com  vwm-hcs-`*`ID`*`-uag.`*`region`*`.cloudapp.azure.com`
プライベート ロード バランサ IP アドレスがある外部	`ourApps.ourOrg.example.com  Azure-load-balancer-private-IP`

次のステップ

ポッドの外部ゲートウェイ構成の Azure ロード バランサの前に構成されたファイアウォールまたは NAT を使用してポッドが構成されている場合は、ファイアウォールまたは NAT のセットアップでパブリック IP アドレスが提供されていることと、同じ FQDN がそのファイアウォールまたは NAT によって提供されるパブリック IP アドレスに対してパブリックに解決可能であることを確認する必要があります。

Microsoft Azure でデプロイされた Horizon Cloud ポッドのゲートウェイ関連項目の変更

デプロイされたポッドのゲートウェイ構成は、さまざまな方法で変更できます。これらの変更は、Horizon Universal Console でのポッドの詳細ページを使用して行います。コンソールは動的です。ユーザーが使用できるのは、ポッドにすでに存在するゲートウェイ構成に基づいて実行することが適切なアクションのみです。

Microsoft Azure への Horizon Cloud ポッドのデプロイのドキュメント トピックで説明しているように、外部または内部ゲートウェイ構成のいずれかまたは両方でポッドをデプロイできます。デプロイされたポッドには、そのゲートウェイ構成のいずれか 1 つまたは両方に 2 要素認証を設定することも、まったく設定しないこともできます。ポッドの詳細ページから、デプロイされたポッドについて、次のゲートウェイに関連する項目を変更できます。

- ポッドにゲートウェイ構成を追加する。ポッドにゲートウェイ構成がない場合は、いずれかまたは両方のタイプを追加できます。ポッドに 1 つのタイプのゲートウェイがある場合は、存在しないタイプのゲートウェイを追加できます。
- ポッドからゲートウェイ構成を削除する。
- 既存のゲートウェイ構成を編集して、そのゲートウェイの 2 要素認証設定を追加、変更、または無効にする。
- ゲートウェイ構成の Unified Access Gateway ソフトウェア設定変更します。

注： 現在、ゲートウェイのデプロイの仕様に関連する項目は、そのゲートウェイ構成をサブスクリプション環境にデプロイするときにのみ設定できます。[ポッドの編集] ワークフローを使用してゲートウェイのソフトウェア構成をいつでも更新できる場合でも、コンソールはまだ [ポッドの編集] ワークフローを使用してゲートウェイのデプロイ構成を更新する方法を提供していません。[ポッドの編集] ワークフローを使用して変更できないこれらの項目の例として、Unified Access Gateway インスタンスで使用される仮想マシン モデル、ネットワーク関連の設定、およびゲートウェイのリソース グループの Microsoft Azure リソース タグがあります。既存のゲートウェイのデプロイ構成に関連する項目を変更する場合は、最初にポッドから既存のゲートウェイ構成を削除し、[ポッドの編集] ワークフローを使用して、必要な新しい設定を使用してポッドのゲートウェイ構成を再デプロイする必要があります。

デプロイ済みの Horizon Cloud ポッドへのゲートウェイ構成の追加

最初にゲートウェイなしで、または 1 つのタイプのゲートウェイのみを使用して Horizon Cloud ポッドを Microsoft Azure にデプロイした場合、[ポッドの編集] ワークフローを使用して、後からゲートウェイ構成をポッドに追加できます。このワークフローは、ポッドの詳細ページから起動します。

ヒント: コンソールは動的です。ポッドの現在の構成や環境全体の構成に基づいて、意味のある適切なワークフローおよびトグルやフィールドのみが、ユーザー インターフェイスで利用できるようになります。

6 章 ユーザーの Horizon Cloud on Microsoft Azure 環境に記載されているように、ポッドには内部/外部のゲートウェイ構成のどちらか 1 つまたは両方を設定できます。このワークフローを使用して、ポッドにまだないタイプを追加できます。ポッドを編集してゲートウェイ構成を追加するのと同時に、そのゲートウェイに対して 2 要素認証設定を指定することもできます。

重要： これらの手順を使用してポッドを変更するときは、次の点に注意してください。

- 外部ゲートウェイ構成を最初に設定した後は、外部ゲートウェイのロード バランサの IP 設定を変更できないことに注意してください。外部ゲートウェイ構成を追加するときに、ゲートウェイのロード バランサ用にパブリック IP アドレスではなくプライベート IP アドレスを使用するように選択できます。デフォルトでは、パブリック IP アドレスを使用します。
- テナントが Universal Broker を使用するように構成され、ブローカ設定で 2 要素認証が有効になっている場合、フリート内のすべてのポッドの外部ゲートウェイで同じ 2 要素認証タイプを設定する必要があります。
- システムがポッドの構成を変更している場合、変更が完了するまでは次の制限が適用されます。
  - ポッドでは管理タスクを実行できません。
  - ポッドによってサービスが提供される、デスクトップまたはリモート アプリケーションにセッションを接続していないエンド ユーザーは、接続を試みると失敗します。
  - ポッドによってサービスが提供されるセッションを接続しているエンド ユーザーに対して、それらのアクティブなセッションが切断されることになります。データの損失は発生しません。構成の変更が完了した後に、これらのユーザーは再接続できます。

前提条件

注： ポッドの高可用性が有効になっていて、ポッド マネージャ仮想マシンの 1 つがオフラインの場合、システムによってポッドへのゲートウェイの追加が妨げられます。[保存して終了] をクリックすると、このメッセージが表示されます。ゲートウェイを追加するには、Microsoft Azure ポータルを使用してオフラインのポッド マネージャ仮想マシンをオンラインに戻す必要があります。

Microsoft Azure の既存のポッドにゲートウェイ構成を追加するときに、[ポッドの編集] ウィザードのフィールドの入力を完了するには、Unified Access Gateway 構成の前提条件に記載されている情報を入力する必要があります。ゲートウェイを追加しているときと同時に 2 要素認証の設定も行う場合は、2 要素認証構成でデプロイする際の前提条件に記載されている情報を入力する必要があります。外部ゲートウェイ構成を追加し、独自のサブスクリプションを使用する場合はそのサブスクリプション情報も必要です。追加するゲートウェイに使用する VNet が VNet の要件を満たしていることを確認します。これらの VNet 要件については、Microsoft Azure で必要な仮想ネットワークを構成するを参照してください。

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。

手順

1 コンソールで [設定] - [キャパシティ] に移動し、ポッドの名前をクリックしてその詳細ページを開きます。

2 ポッドの詳細ページで、[編集] をクリックします。

3 [サブスクリプション] の手順で、外部ゲートウェイ構成を追加し、ポッドとは別のサブスクリプションを使用する場合は、[外部ゲートウェイに別のサブスクリプションを使用] を有効にして、サブスクリプション情報を入力します。

4 [ゲートウェイ設定] の手順に到達するまで [次へ] をクリックします。

この手順には、外部ゲートウェイ構成のセクションと、内部ゲートウェイ構成のセクションが含まれています。ユーザー インターフェイスには、ポッドの現在の構成と、すでに存在するゲートウェイ設定が反映されます。

5 外部ゲートウェイを追加するには、[外部 UAG を有効にしますか?] トグルをオンに切り替えて、[外部 UAG] セクションのフィールドに入力します。

オプション	説明
[外部ゲートウェイを有効にしますか?]	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。 **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。 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。
[FQDN]	`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。 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。 **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。
[DNS アドレス]	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。 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。 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 サーバと通信できる必要があります。 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。 [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。

オプション	説明
[ルート]	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。 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。 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`）。
[ポッドの NTP サーバの継承]	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。 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。 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。
[仮想マシン モデル]	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。 **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。
[証明書]	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。
[Blast Extreme TCP ポート]	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。 **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。
[暗号スイート]	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。 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。

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?]	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。 **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。 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。
[Horizon FQDN のパブリック IP アドレス]	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。デプロイヤは、この IP アドレスを Unified Access Gateway 構成の設定で構成します。

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]	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。 **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。 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。
[別の仮想ネットワークを使用] - オフ	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。 ■ [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。 **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。 ■ [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	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。 **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。 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。 ■ 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。

6 （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。

7 内部ゲートウェイを追加するには、[内部 UAG を有効にしますか?] トグルをオンに切り替えて、[内部 UAG] セクションの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 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 バランサは、プライベート IP アドレスで構成されます。
[FQDN]	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。 **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。
[DNS アドレス]	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。 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。 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 サーバと通信できる必要があります。 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。 [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。
[ルート]	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。 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。 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`）。
[ポッドの NTP サーバの継承]	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。 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。

オプション	説明
[仮想マシン モデル]	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。 **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。
[証明書]	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。
[Blast Extreme TCP ポート]	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。 **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。
[暗号スイート]	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。 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。

8 追加しているいずれかのゲートウェイのセクションで、オプションで 2 要素認証を使用するようにエンド ユーザーのデスクトップを構成する場合は、Horizon Cloud ポッドのゲートウェイでの 2 要素認証の有効化の手順に従います。

9 [Azure リソース タグ] セクションで、ポッドの他のリソース グループで指定されているものとは異なるゲートウェイ関連のリソース グループのリソース タグを指定する場合は、[ポッド タグの継承] を無効にして、表示されるフィールドにタグを指定します。

[Azure リソース タグ] フィールドの説明については、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を参照してください。ポッドの両方のタイプのゲートウェイには同じタグのセットが使用されます。

10 [保存して終了] をクリックします。

ワークフローの開始を確認するよう求める確認メッセージが表示されます。

11 [はい] をクリックしてワークフローを開始します。

結果

ゲートウェイの要素をシステムがデプロイ完了するまで、ポッドのサマリ ページにおけるその構成タイプのセクションには、保留中 ステータスが表示されます。また、システムがゲートウェイをデプロイするアクションを完了するまで、追加の [ポッドを編集] ワークフロー関連のアクティビティを実行することはできません。

ワークフローが完了すると、ステータスには 準備完了 と表示され、ロード バランサの FQDN がページに表示されます。

注： Microsoft Azure China のポッドに対してこのワークフローを実行する場合、プロセスが完了するまでに 1 時間以上かかることがあります。このプロセスは地理的なネットワークの問題の影響を受け、バイナリがクラウドの制御プレーンからダウンロードされるときにダウンロードの速度が低下することがあります。

次のステップ

重要： エンド ユーザーが新たに追加されたゲートウェイの使用を開始できるようにするには、次のタスクを実行する必要があります。

- 新しく追加されたゲートウェイ構成の場合、構成でデプロイされるロード バランサをデプロイ ウィザードで入力した FQDN にマッピングする CNAME レコードが DNS サーバにあることを確認します。詳細については、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を参照してください。
- 追加されたゲートウェイに 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 アドレスの取得方法については、必要な Horizon Cloud ポッドの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。

Horizon Cloud ポッドのゲートウェイでの 2 要素認証の有効化

すでにデプロイされているポッドのゲートウェイ設定で 2 要素認証の使用を有効にするには、ポッドの詳細ページで [編集] アクションを使用します。ポッドでのゲートウェイ構成は、Unified Access Gateway 仮想マシンを使用し、エンド ユーザーのデスクトップおよびアプリケーションへのアクセスを提供するように構成されます。これらの 2 要素認証設定は、ポッドの既存のゲートウェイ構成に追加することも、新しいゲートウェイ構成を追加するときに同時に追加することもできます。[ポッドの編集] ワークフローを使用して、ポッドのゲートウェイ構成に 2 要素認証設定を追加します。

注： テナントが Universal Broker を使用するように構成され、ブローカ設定で 2 要素認証が有効になっている場合、フリート内のすべてのポッドの外部ゲートウェイで同じ 2 要素認証タイプを設定する必要があります。このシナリオでは、これらの手順を実行して外部ゲートウェイに 2 要素認証を追加すると、ユーザー インターフェイスによって、ブローカ設定での設定に一致する 2 要素認証タイプの選択が適用されます。

前提条件

2 要素認証を追加するゲートウェイに対して、デプロイ済みの Horizon Cloud ポッドへのゲートウェイ構成の追加であ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、そのゲートウェイの Unified Access Gateway インスタンスがそのオンプレミス サーバへの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入力します。

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]	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。 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。 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`）。

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

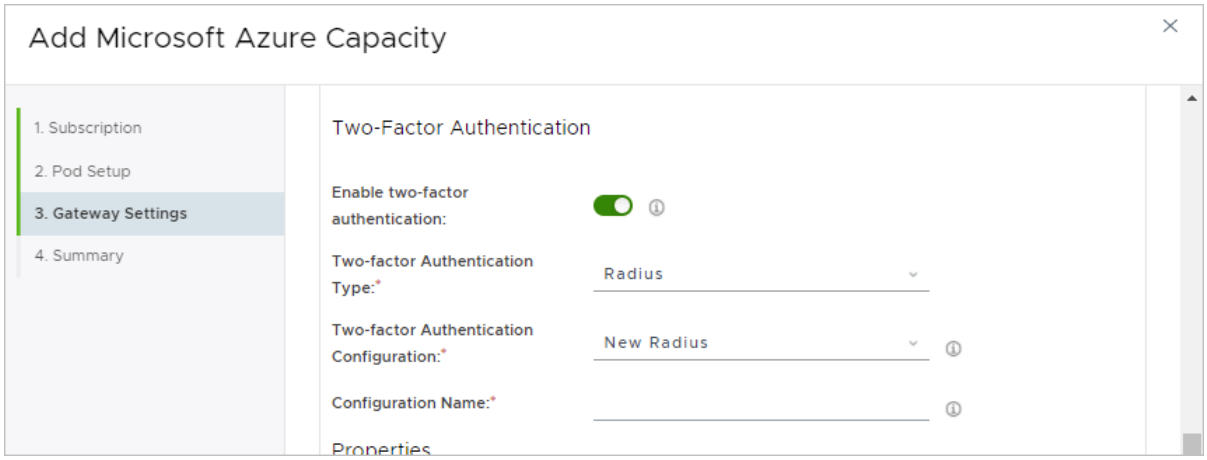
1 [ポッドの編集] ウィンドウの [ゲートウェイ設定] ステップがまだ開いていない場合は、ポッドの詳細ページで [編集] をクリックし、[次へ] をクリックして [ゲートウェイ設定] ステップに移動します。

2 2 要素認証を有効にするゲートウェイ タイプ（外部または内部）のウィンドウに移動します。

3 [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。



4 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。

5 [構成名] フィールドで、この構成の識別名を入力します。

6 [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]	必要に応じて、ユーザーに RADIUS ユーザー名とパスコ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 DisplayHint user name and passcode` としてエンドユーザーに表示されます。ここで、*DisplayHint* はこのフィールドで指定するテキストです。 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。
[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。

オプション	説明
[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]	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： ■ 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。 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。 **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。
[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、アカウンティング 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。
[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。

オプション	説明
[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。

7 必要な設定をすべて完了したら、[保存して終了] をクリックします。

ワークフローの開始を確認するよう求める確認メッセージが表示されます。

8 [はい] をクリックしてワークフローを開始します。

結果

システムがポッドへの新しい構成のデプロイを完了するまで、ポッドのサマリ ページでの 2 要素認証を追加したゲートウェイのセクションに、保留しています ステータスが表示されます。

ワークフローが完了すると、ステータスには 準備完了 と表示され、ゲートウェイの 2 要素認証設定がページに表示されます。

注： Microsoft Azure China のポッドに対してこのワークフローを実行する場合、プロセスが完了するまでに 1 時間以上かかることがあります。このプロセスは地理的なネットワークの問題の影響を受け、バイナリがクラウドの制御プレーンからダウンロードされるときにダウンロードの速度が低下することがあります。

次のステップ

重要： エンド ユーザーが 2 要素認証機能を使用してゲートウェイを使用できるようにするには、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 アドレスの取得方法については、必要な Horizon Cloud ポッドの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。

Horizon Cloud ポッドのゲートウェイでの 2 要素認証設定の変更または無効化

[ポッドの編集] ワークフローを使用して、ポッドのゲートウェイで 2 要素認証設定を変更したり、2 要素認証を完全に無効化したりすることができます。設定を変更する場合、基本的には 2 要素認証設定の新しい名前を入力し、必要な新しい設定を入力して、特定のゲートウェイ用に新しい名前が選択されていることを確認し、保存します。[ポッドの編集] ワークフローを使用して、2 要素認証設定を変更します。

注： テナントが Universal Broker を使用するように構成され、ブローカ設定で 2 要素認証が有効になっている場合、フリート内のすべてのポッドの外部ゲートウェイで同じ 2 要素認証タイプを設定する必要があります。このシナリオでは、これらの手順を実行して外部ゲートウェイに 2 要素認証を追加すると、ユーザー インターフェイスによって、ブローカ設定での設定に一致する 2 要素認証タイプの選択が適用されます。

前提条件

ゲートウェイの 1 つに対して 2 要素認証を有効のままにしておいて、特定の設定を変更している場合は、次の情報があることを確認します。

- 2 要素認証サーバがオンプレミスの場合、ゲートウェイの Unified Access Gateway インスタンスがそのサーバへのルーティングを解決できるように、次のフィールドに関連する情報があることを確認します。

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]	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。 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。 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`）。

- 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 ポッドの詳細ページから [編集] をクリックして、[ポッドの編集] ウィンドウを開きます。

2 [ポッドの編集] ウィンドウで [次へ] をクリックし、[ゲートウェイ設定] の手順に移動します。

この手順には、外部ゲートウェイ構成のセクションと、内部ゲートウェイ構成のセクションが含まれています。ユーザー インターフェイスには、ポッドの現在の構成と、すでに存在するゲートウェイ設定が反映されます。

3 2 要素認証を変更するゲートウェイ タイプ（外部または内部）のウィンドウに移動します。

4 ゲートウェイで 2 要素認証を無効にするには、[2 要素認証を有効にしますか] トグルをオフに切り替えてから、手順 ステップ 9 に移動して変更を保存します。

他のゲートウェイでも 2 要素認証が有効になっていて、それを無効にする場合は、その他のゲートウェイのセクションでトグルをオフにします。

5 ゲートウェイで設定されている特定の 2 要素認証設定を変更するには、次の手順を続行します。

2 要素認証の値の新規セットに新しい名前を作成し、ウィンドウ内のゲートウェイ セクションで選択されたその新しい名前で構成を保存します。

6 [構成名] フィールドで、この構成の識別名を入力します。

7 [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]	必要に応じて、ユーザーに RADIUS ユーザー名とパスコ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 DisplayHint user name and passcode` としてエンドユーザーに表示されます。ここで、*DisplayHint* はこのフィールドで指定するテキストです。 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。
[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]	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： ■ 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。 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。 **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。

オプション	説明
[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、アカウンティング 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。
[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。

8 必要な設定をすべて完了したら、[保存して終了] をクリックします。

ワークフローの開始を確認するよう求める確認メッセージが表示されます。

9 [はい] をクリックしてワークフローを開始します。

結果

システムがポッドへの新しい構成のデプロイを完了するまで、ポッドのサマリ ページでの 2 要素認証を追加したゲートウェイのセクションに、保留しています ステータスが表示されます。

ワークフローが完了すると、ステータスには 準備完了 と表示され、ゲートウェイの 2 要素認証設定がページに表示されます。

注： Microsoft Azure China のポッドに対してこのワークフローを実行する場合、プロセスが完了するまでに 1 時間以上かかることがあります。このプロセスは地理的なネットワークの問題の影響を受け、バイナリがクラウドの制御プレーンからダウンロードされるときにダウンロードの速度が低下することがあります。

次のステップ

重要： ゲートウェイの 2 要素認証設定の値を新しいものに変更する場合は、エンド ユーザーが 2 要素認証の新しい値を持つゲートウェイの使用を再開する前に、次のタスクを完了しておく必要があります。

- 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、ゲートウェイ構成で指定した 2 要素認証サーバが、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していることを確認します。

  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許可された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、2 要素認証サーバが、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構成されていることを確認します。

  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許可された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 アドレスの取得方法については、必要な Horizon Cloud ポッドの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。

デプロイされた Horizon Cloud ポッドのゲートウェイ構成がポッド マネージャ インスタンスと同じ NTP サーバ設定を継承するようにする

このドキュメント ページでは、既存の Horizon Cloud ポッドのゲートウェイ構成が、ポッド マネージャ インスタンスに指定されたものと同じ NTP サーバ設定を継承するようにする方法について説明します。

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。

2022 年 10 月 20 日のサービス更新以降、新しいゲートウェイのデプロイでは、ゲートウェイのデプロイ中に [ポッドの NTP サーバの継承] トグルが手動でオフにされていない限り、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 サーバ設定をデフォルトで継承します。

ゲートウェイが 2022 年 10 月 20 日より前にデプロイされたか、そのトグルをオフにしてデプロイされた場合は、これらの手順を使用して、Unified Access Gateway インスタンスがポッド マネージャに指定されたのと同じ NTP サーバ設定を継承するように設定することができます。

前提条件

次の項目が適切であることを確認します。

- ポッドには、これらの手順を実行するデプロイ済みのゲートウェイ構成があります。
- これらの手順を、ポッドの VNet とは別の専用の VNet にデプロイされた外部ゲートウェイで実行する場合は、ゲートウェイ デプロイの VNet を介してポッドの NTP サーバにアクセスできることを確認します。

手順

1 ポッドの詳細ページから、[編集] をクリックして [ポッドの編集] ウィンドウを開きます。

2 [ポッドの編集] ウィンドウで [次へ] をクリックし、[ゲートウェイ設定] の手順に移動します。

この手順には、外部ゲートウェイ構成のセクションと、内部ゲートウェイ構成のセクションが含まれています。ユーザー インターフェイスには、ポッドの現在の構成と、すでに存在するゲートウェイ設定が反映されます。

3 それぞれのゲートウェイ タイプ（外部または内部）の [ポッドの NTP サーバの継承] トグルを見つけます。

4 [ポッドの NTP サーバの継承] がオンになっていることを確認します。

5 [保存して終了] をクリックします。

結果

システムはデプロイされたゲートウェイの NTP 設定を更新し、それらの設定がポッド マネージャの NTP サーバ設定と一致するようにします。

デプロイされた Horizon Cloud ポッドのゲートウェイ構成でのセッション タイムアウト設定のカスタマイズ

ゲートウェイが Microsoft Azure の Horizon Cloud ポッドで最初に構成されるとき、セッション タイムアウト値は Unified Access Gateway のデフォルト値である 10 時間（3600 万ミリ秒）です。[ポッドの編集] ワーク

フローを使用して、ポッドのゲートウェイ構成を編集し、自分の組織のニーズに合わせてそのタイムアウト値をカスタマイズできます。

前提条件

ポッドには、セッション タイムアウトをカスタマイズするゲートウェイ構成がすでに存在している必要があります。

手順

1 ポッドの詳細ページから、[編集] をクリックして [ポッドの編集] ウィンドウを開きます。

2 [ポッドの編集] ウィンドウで [次へ] をクリックし、[ゲートウェイ設定] の手順に移動します。

この手順には、外部ゲートウェイ構成のセクションと、内部ゲートウェイ構成のセクションが含まれています。ユーザー インターフェイスには、ポッドの現在の構成と、すでに存在するゲートウェイ設定が反映されます。

3 変更するゲートウェイ タイプ（外部または内部のいずれか）の [セッション タイムアウト] フィールドを特定します。

4 [セッション タイムアウト] に新しい値を入力します。

ポッドに別のゲートウェイ タイプがあり、そのセッション タイムアウト値を変更する場合は、この手順をその他のゲートウェイに対して繰り返します。

タイムアウト値は、5 分（30 万ミリ秒）以上にする必要があります。

5 [保存して終了] をクリックします。

結果

システムは、ゲートウェイ構成で入力した値に応じて、ポッドのゲートウェイ構成のセッション タイムアウトを更新します。

デプロイされた Horizon Cloud ポッドのゲートウェイ構成での Blast Extreme TCP ポートを 8443 に設定する

Blast Extreme TCP ポートにポート 8443 が使用されている場合、ポッドの Unified Access Gateway インスタンスへのクライアントの Blast Extreme TCP トラフィックのパフォーマンスが向上します。デプロイされたゲートウェイ構成で Blast Extreme TCP トラフィックにポート 8443 を使用するよう設定されていない場合は、[ポッドの編集] ワークフローを使用して、Blast Extreme TCP ポートにポート 8443 を使用するよう設定できます。

Blast Extreme TCP ポートは、サービスのデプロイヤが Unified Access Gateway 構成の Blast 外部 URL で設定するポートです。たとえば、ゲートウェイ構成が `myuag.hcs.com` として指定された FQDN でデプロイされ、Blast Extreme TCP ポート メニューがデプロイヤ ウィザードで 8443 に設定されている場合、デプロイヤはゲートウェイ構成の Blast 外部 URL を `https://myuag.hcs.com:8443` に設定します。

重要： デプロイヤ ウィザードでは Blast Extreme TCP ポートを 8443 または 443 のいずれかに設定できますが、8443 はエンドユーザー クライアントと Unified Access Gateway インスタンス間のトラフィックに対して最高のパフォーマンスと効率を提供します。ポート 8443 はデプロイヤ ウィザードのデフォルトで、基盤となる Unified Access Gateway インスタンスで CPU 輻輳が発生しないようにするために推奨されます。443 の使用は、組織のセキュリティ チームまたはファイアウォール チームがエンドユーザー クライアントからのトラフィックに対する 8443/TCP の使用をブロックし、443 の使用のみを許可している場合にのみ選択してください。

前提条件

ポッドには、Blast Extreme TCP ポート設定を編集するゲートウェイ構成がすでに存在している必要があります。

手順

1 ポッドの詳細ページから、[編集] をクリックして [ポッドの編集] ウィンドウを開きます。

2 [ポッドの編集] ウィンドウで [次へ] をクリックし、[ゲートウェイ設定] の手順に移動します。

この手順には、外部ゲートウェイ構成のセクションと、内部ゲートウェイ構成のセクションが含まれています。ユーザー インターフェイスには、ポッドの現在の構成と、すでに存在するゲートウェイ設定が反映されます。

3 変更するゲートウェイ タイプ（外部または内部のいずれか）の [Blast Extreme TCP ポート] メニューを特定します。

4 [Blast Extreme TCP ポート] には 8443 を選択します。

ポッドに別のゲートウェイ タイプがあり、その Blast Extreme TCP ポートを変更する場合は、この手順をその他のゲートウェイに対して繰り返します。

5 [保存して終了] をクリックします。

結果

システムは、ポッドのゲートウェイ構成の Blast 外部 URL を更新し、[ポッドの編集] ワークフローで指定された [Blast Extreme TCP ポート] を使用します。

デプロイされた Horizon Cloud ポッドのゲートウェイ構成に使用される暗号スイートの更新

このドキュメント ページでは、ポッドのゲートウェイ構成で暗号スイートを変更する方法について説明します。暗号スイートは、クライアントとポッドの Unified Access Gateway アプライアンス間の TLS 通信を暗号化するために使用される暗号化アルゴリズムです。

ほとんどの場合、デフォルト設定で十分ですが、Unified Access Gateway は暗号スイートを指定するためにこの機能を提供します。

[ポッドの編集] ウィザードには、Horizon Cloud on Microsoft Azure 環境で許可されている暗号スイートのリストが表示されます。画面上のリストから選択します。

前提条件

ポッドには、暗号スイートを更新するゲートウェイ構成がすでに存在している必要があります。

手順

1 ポッドの詳細ページから、[編集] をクリックして [ポッドの編集] ウィンドウを開きます。

2 [ポッドの編集] ウィンドウで [次へ] をクリックし、[ゲートウェイ設定] の手順に移動します。

この手順には、外部ゲートウェイ構成のセクションと、内部ゲートウェイ構成のセクションが含まれています。ユーザー インターフェイスには、ポッドの現在の構成と、すでに存在するゲートウェイ設定が反映されます。

3 暗号スイートを変更するゲートウェイ タイプ（外部または内部のいずれか）の [暗号スイート] を特定します。

選択内容を目的の選択に更新します。

ポッドに別のゲートウェイ タイプがあり、そこで使用する暗号スイートを変更する場合は、この手順をその他のゲートウェイに対して繰り返します。

4 [保存して終了] をクリックします。

結果

システムは、このワークフローで選択した暗号スイートを使用するように、ポッドのゲートウェイ構成内の暗号スイートのセットを更新します。

Microsoft Azure の Horizon Cloud ポッドで、ゲートウェイの SSL 証明書を新しいバージョンに置き換える（新しい有効期限や別の FQDN を使用するなど）

このワークフローを使用して、ポッドにデプロイされているいずれかのタイプのゲートウェイ構成に配置されている SSL 証明書を置き換えます。また、必要に応じて、このワークフローを使用して、ゲートウェイで構成されている完全修飾ドメイン名 (FQDN) を置き換えることもできます。SSL 証明書を置き換える理由の 1 つとして、ゲートウェイ構成に現在配置されている SSL 証明書の有効期限が近づいていることが考えられます。次の手順を実行するには、Horizon Universal Console のポッドの編集ウィザードを使用します。

重要： このユースケースに該当する場合：

- 環境には、Microsoft Azure のポッド用のシングルポッド 仲介が構成されており、[ブローカ] ページに示されています。
- また、ポッドは、シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure の環境の Horizon Cloud ポッドと Workspace ONE Access の統合 の説明に従って Workspace ONE Access と統合されています。
- これは、ポッドとの通信時に Workspace ONE Access Connector によって使用される SSL 証明書を置き換えることを目的としています。

その場合、このユースケースでは、さまざまな手順を実行する必要があります。Workspace ONE Access Connector とポッドを統合する場合は、以下の手順は実行しないでください。これらの手順は、以下の手順とはまったく異なります。Workspace ONE Access Connector の統合とそのニーズの概要については、シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure で関連する Workspace ONE Access テナント情報を使用して Horizon Cloud ポッドを構成する手順を参照してください。また、デプロイが、エンド ユーザーのクライアントとブラウザをポッド マネージャ アプライアンスに直接接続するというまれで一般的ではないシナリオである場合は、以下の手順を実行して、これらのまれなシナリオで使用される SSL 証明書を置き換えないでください。Workspace ONE Access Connector の使用事例、およびまれで一般的ではないシナリオの使用事例に適用される証明書の構成の説明については、代わりに Horizon Cloud ポッドのマネージャ仮想マシンでの SSL 証明書の構成の概要（主にシングルポッド ブローカ環境でポッドを使用する Workspace ONE Access Connector で使用）を参照してください。

ポッドのゲートウェイが最初にポッドにデプロイされてから時間が経過した後に、ポッドのゲートウェイで構成されている SSL 証明書を置き換えるか、ゲートウェイで構成されている FQDN を置き換えるか、またはその両方を行う必要がある場合があります。通常は、エンド ユーザーに対して、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ために、Horizon Client またはブラウザで使用する FQDN を指定します。ブラウザを使用したデスクトップおよび RDS ベースのリモート アプリケーションへのログインと Horizon Client を使用したデスクトップまたは RDS ベースのリモート アプリケーションへのログインのトピックで説明したように、一部のエンド ユーザー

はブラウザを開いてその FQDN を入力しますが、他のエンド ユーザーは Horizon Client の 1 つを使用する場合があります。エンド ユーザーにクライアントとブラウザを指定するように指示するゲートウェイで構成された SSL 証明書により、それらのクライアントとブラウザはそのゲートウェイへの接続を信頼できるようになります。デプロイされた Horizon Cloud ポッド に記載されているように、ポッドには外部の Unified Access Gateway 構成、内部のタイプ、またはその両方を設定できます。Unified Gateway 構成のいずれかのタイプで、Unified Access Gateway インスタンスは、FQDN および SSL 証明書情報で構成されます。

ポッドのゲートウェイで構成されている SSL 証明書と FQDN をさまざまな理由で置き換えることができます。理由の 1 つは、ゲートウェイで構成されたインプレース SSL 証明書の証明書チェーンに有効期限があり、そのカレンダーの日付と時刻が間もなく近づいているためである可能性があります。そのような状況では、現在の有効期限に達する前に SSL 証明書を置き換えて、エンド ユーザーのクライアントまたはブラウザがゲートウェイに接続しようとするときに証明書の信頼の問題が発生しないようにする必要があります。SSL 証明書を置き換えるもう 1 つの理由として、エンド ユーザーがクライアントとブラウザで別の FQDN の使用を開始する必要がある場合です。SSL 証明書は FQDN と連携するため、FQDN を別の FQDN に変更する場合は、通常、SSL 証明書を新しい FQDN に基づく証明書に置き換えます。

注： システムが構成を変更している間、エンド ユーザーの接続セッションがポッドによって提供されている場合、それらのアクティブなセッションは切断されます。データの損失は発生しません。構成の変更が完了した後に、これらのユーザーは再接続できます。

前提条件

このワークフローを完了するには、以下が必要です。

- 次の条件を満たす置き換え用 SSL 証明書。この証明書では、エンド ユーザーがクライアントおよびブラウザで使用する FQDN を使用して、使用資格が付与されたリソースにアクセスするためにポッドのゲートウェイに接続する必要があります。
- 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。

- 当該 SSL 証明書に対応する FQDN。この FQDN は、エンド ユーザーのクライアントとブラウザでポッドのゲートウェイに接続するために使用されるものです。SSL 証明書を置き換える理由が、ユーザーのクライアントの

有効期限の問題を回避するためである場合は、ゲートウェイですでに構成されている FQDN を保持して、ウィザードに表示される可能性があります。また、FQDN を新しいものに変更する場合は、このポッドに固有の FQDN を使用する必要があります。他のポッドに対してすでに設定されている FQDN を再使用することはできません。

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。

手順

1 コンソールで [設定] - [キャパシティ] に移動し、ポッドの名前をクリックしてその詳細ページを開きます。

2 ポッドの詳細ページで、[編集] をクリックします。

3 [ポッドの編集] ウィンドウで [次へ] をクリックし、[ゲートウェイ設定] の手順に移動します。

4 ゲートウェイ構成で実行する必要がある変更に応じて、[外部 UAG] セクションまたは [内部 UAG] セクションのいずれかで、関連する手順を実行します。

   a [FQDN] の値を新しい値に置き換えます。

   b 新しい証明書をアップロードするには、[変更] をクリックして、SSL 証明書を置き換えます。

   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、指定した 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。

5 [保存して終了] をクリックします。

FQDN または証明書を更新すると既存のユーザー接続が切断されるという内容の確認メッセージが表示され、ワークフローの開始を確認するよう求められます。

6 [はい] をクリックしてワークフローを開始します。

重要： 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、[更新ステータス] には [更新に失敗しました] と表示されます。この表示になっている場合は、証明書ファイルを確認し、すべての証明書の有効期間が終了していないか確認します。

次のステップ

どの Unified Access Gateway 構成を変更した場合でも、前の設定とは異なる FQDN に変更した場合は、DNS サーバの CNAME レコードを更新して、構成のロード バランサの FQDN を新しい FQDN にマッピングするようにします。詳細については、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 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 形式に変換した後には、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。

必要な Horizon Cloud ポッドのゲートウェイ情報での 2 要素認証システムの更新

Horizon Cloud ポッドのゲートウェイ構成で 2 要素認証設定を構成した後、特定のゲートウェイ関連の IP アドレスから受信した認証要求を許可するように対応する 2 要素認証システムの構成も設定する必要があります。

ゲートウェイの Unified Access Gateway インスタンスは、特定の IP アドレスから 2 要素認証サーバと通信することを試みます。ネットワーク管理者が、ポッドの Azure 仮想ネットワーク (VNet) および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。そのネットワークの可視性とポッド ゲートウェイ タイプ (外部または内部) の組み合わせによって、2 要素認証サーバ構成で構成してその通信を許可する必要がある特定のゲートウェイ関連 IP アドレスが決まります。

重要： 使用している 2 要素認証システムに適したドキュメントに従う必要があります。

RADIUS 2 要素認証システムは、許可された RADIUS クライアントの概念を使用します。たとえば、FreeRADIUS クライアント構成のための FreeRADIUS Wiki に記載されているように、`/etc/raddb/clients.conf` ファイルには RADIUS クライアントの定義が次のように含まれています。

```
client NAME {
  ipaddr = IPADDRESS
  secret = SECRET
}
```

RSA SecurID 2 要素認証システムは、RSA Authentication Manager と通信するために登録された認証エージェントの概念を使用します。たとえば、SecurID Authentication Manager のドキュメント - 認証エージェントの追加で説明するように、RSA Authentication Manager のセキュリティ コンソールを使用して、必要な IP アドレスをその内部データベースに追加します。

このトピックでは、ポッドのゲートウェイとの間の通信を有効にするために、また、各ポッドの更新後にその通信の復元力を維持するために、2 要素認証サーバで使用する必要がある Horizon Cloud ポッドの情報について説明します。

ゲートウェイ構成の Unified Access Gateway インスタンスからの通信を受け入れるには、2 要素認証サーバで適切な IP アドレスからの通信を許可する必要があります。

通常、ネットワーク管理者は、2 要素認証サーバがデプロイされたポッドに接続されている VNet およびサブネットに対して持つネットワーク アクセスを決定します。2 要素認証サーバとの通信時に Unified Access Gateway インスタンスが使用する特定の送信元 IP アドレスは、次の条件に依存します。

- ゲートウェイ構成で RADIUS と RSA SecurID のどちらのタイプを構成したか
- ゲートウェイ構成が内部であるか外部であるか
- ネットワーク管理者が、2 要素認証サーバをポッドの VNet 内からアクセス可能として構成しているか、または VNet の外部に配置しているか
- ポッドの VNet 内で 2 要素認証サーバにアクセスできる場合、その VNet 内のどのポッドのサブネットから、ネットワーク管理者が 2 要素認証サーバへのアクセスを構成したか

RSA SecurID - 外部と内部の両方のゲートウェイ構成

RSA Authentication Manager サーバには、個々の Unified Access Gateway インスタンスの NIC からの通信が表示されます。RSA Authentication Manager 構成で、次の NIC IP アドレスを認証エージェントとして登録します。

- 外部ゲートウェイの場合、ゲートウェイの `dmz` サブネット上の 4 つの NIC

- 内部ゲートウェイの場合、ゲートウェイの `tenant` サブネット上の 4 つの NIC

RADIUS - 内部ゲートウェイ構成

内部ゲートウェイ構成用にデプロイされた Unified Access Gateway インスタンスは、自身の NIC のプライベート IP アドレスを使用して、その 2 要素認証サーバに通信します。2 要素認証サーバは、NIC のプライベート IP アドレスである送信元 IP アドレスから受信した要求を認識します。ネットワーク管理者は、ポッドの管理またはテナント サブネットの IP アドレス範囲にそのサーバがアクセス可能かどうかを構成しています。Microsoft Azure の内部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 つの NIC はアイドル状態で、ポッド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接続をサポートするには、サーバに対して可視性のあるサブネットに対応する、Microsoft Azure での内部ゲートウェイのリソース グループにある 4 つの NIC の IP アドレスからのクライアント接続を許可するようにサーバを構成する必要があります。以下のポッド ゲートウェイ NIC の IP アドレスからの通信を許可するセクションを参照してください。

注： 内部ゲートウェイで構成された RSA SecurID タイプの場合は、テナント サブネット上の 4 つの NIC の NIC IP アドレスを追加します。

RADIUS - 外部ゲートウェイ構成と、ポッドの VNet の内部でアクセス可能な 2 要素認証サーバ

ネットワーク管理者が、ポッドと同じ VNet で 2 要素認証サーバがアクセス可能になるように構成している場合、Unified Access Gateway インスタンスは NIC のプライベート IP アドレスを使用して、そのサーバと通信します。2 要素認証サーバは、NIC のプライベート IP アドレスである送信元 IP アドレスから受信した要求を認識します。ネットワーク管理者は、ポッドの管理、テナント、または DMZ サブネットの IP アドレス範囲にサーバがアクセス可能かどうかを構成しています。Microsoft Azure の外部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接続をサポートするには、サーバに対して可視性のあるサブネットに対応する、Microsoft Azure での外部ゲートウェイのリソース グループにある 4 つの NIC の IP アドレスからのクライアント接続を許可するようにサーバを構成する必要があります。以下のポッド ゲートウェイ NIC の IP アドレスからの通信を許可するセクションを参照してください。

RADIUS - 外部ゲートウェイ構成と、ポッドの VNet の外部でアクセス可能な 2 要素認証サーバ

ネットワーク管理者がポッドの VNet の外部に 2 要素認証サーバを構成している場合、外部ゲートウェイ構成の Unified Access Gateway インスタンスは、外部ゲートウェイの Azure ロード バランサ リソースの IP アドレスを使用して、そのサーバに接続します。外部ゲートウェイのロード バランサ リソースの IP アドレスからのクライアント接続を許可するように、サーバを構成する必要があります。以下の RADIUS 2 要素認証 - 外部ゲートウェイのロード バランサからの通信を許可するセクションを参照してください。

ポッド ゲートウェイ NIC の IP アドレスからの通信を許可する

ポッドがデプロイされると、ポッド デプロイヤは Microsoft Azure サブスクリプションのゲートウェイのリソース グループに NIC のセットを作成します。次のスクリーンショットは、内部ゲートウェイ タイプと外部ゲートウェイ タイプの NIC の例です。ポッド ID がこれらのスクリーンショットでピクセル化されている場合でも、デプロイヤが NIC の名前に `-management`、`-tenant`、`-dmz` を付けているパターンを確認することができます。ポッドのリソース グループの名前については、第 1 世代テナント - 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。

2 要素認証サーバに対するネットワーク可視性を持つサブネットに対応する、2 要素認証設定を有効にしたゲートウェイ構成の NIC の IP アドレスを取得して、それらの IP アドレスを 2 要素認証サーバの構成で許可されたクライアントとして指定する必要があります。

重要： 更新後に 2 要素認証サーバとポッドとの間の接続が中断されないようにするには、2 要素認証設定を使用して構成した各ゲートウェイで、以下に記載されている 4 つの NIC の IP アドレスが、確実に 2 要素認証サーバの構成で許可されたクライアントとして指定されているようにします。実行中のポッド操作の間は、NIC の半数のみがアクティブになっていますが、これらはポッドの更新後に切り替わります。ポッドを更新した後、NIC の残り半分がアクティブになり、更新前の NIC は再び切り替えられることになる次回のポッドの更新まで、アイドル状態になります。アクティブおよびアイドル状態の両方の NIC の IP アドレスを 2 要素認証サーバ構成に追加していない場合、2 要素認証サーバは、ポッドの更新後の現在アクティブの NIC セットからの接続要求を拒否し、そのゲートウェイを使用するエンド ユーザーのログイン プロセスは停止します。

2 要素認証サーバ構成に追加するゲートウェイの NIC の IP アドレスを取得するには、次の操作を行います。

1 ネットワーク管理者から、ポッドのどのサブネットに 2 要素認証サーバに対するネットワーク可視性があるかについての情報を取得します（管理、テナント、または DMZ）。

2 サブスクリプションの Microsoft Azure ポータルにログインし、ゲートウェイのリソース グループを特定します。

3 ネットワーク管理者によって 2 要素認証サーバに対する可視性があると言われているサブネットに対応する NIC について、各 NIC をクリックして、その IP アドレスをコピーします。

4 使用している 2 要素認証システムのドキュメントに従って、それらの IP アドレスを追加し、2 要素認証サーバがそれらの NIC からの通信を受け入れるようにします。

RADIUS 2 要素認証サーバを使用する場合にゲートウェイの NIC IP アドレスを追加する例

次のコードブロックは、ポッドと同じ VNet 内で、ポッドのテナント サブネットからのアクセスが可能である RADIUS サーバがネットワーク管理者によって構成されている内部ゲートウェイについて、ポッドのテナント サブネットの IP アドレスを持つ NIC のクライアント構成行の一部を示しています。このポッドがデプロイされたとき、ポッドのテナント サブネットは 192.168.25.0/22 として構成されました。ポッドが最初にデプロイされるときに、NIC1 と NIC2 はアクティブになり、NIC3 と NIC4 はアイドル状態になります。ただし、これら 4 つの NIC はすべて RADIUS サーバ構成に追加されており、ポッドの更新後に、NIC3 と NIC4 がアクティブになり、NIC1 と NIC2 がアイドル状態になると、RADIUS サーバはこのゲートウェイからの接続を受け入れ続けます。RADIUS サーバに固有の適切な構文を使用する必要があることに注意してください。

```
client UAGTENANTNIC1 {
  ipaddr = 192.168.25.5
  secret = myradiussecret
}
client UAGTENANTNIC2 {
  ipaddr = 192.168.25.6
  secret = myradiussecret
}
client UAGTENANTNIC3 {
  ipaddr = 192.168.25.7
  secret = myradiussecret
}
client UAGTENANTNIC4 {
  ipaddr = 192.168.25.8
  secret = myradiussecret
}
```

RADIUS 2 要素認証 - 外部ゲートウェイのロード バランサからの通信を許可する

2 要素認証サーバがポッドの VNet の外部に配置されている場合は、そのサーバを指定した外部ゲートウェイに対して、外部ゲートウェイの Azure ロード バランサ リソースのパブリック IP アドレスを 2 要素認証サーバの構成で許可されたクライアントとして追加する必要があります。Microsoft Azure ポータルを使用し、ゲートウェイのリソース グループでロード バランサ リソースを特定することによって、このロード バランサの IP アドレスを取得できます。

1 サブスクリプションの Microsoft Azure ポータルにログインし、ゲートウェイのリソース グループを特定します。

2 ゲートウェイのリソース グループで、ロード バランサ リソースをクリックします。これには、vmw-hcs-*podID*-uag-lb というパターンの名前が付いています。その IP アドレスが概要情報にリストされます。

3 使用している 2 要素認証システムのドキュメントに従って、ゲートウェイのロード バランサ IP アドレスを追加し、2 要素認証サーバがその IP アドレスからの通信を受け入れるようにします。

RADIUS 2 要素認証サーバを使用する場合に外部ゲートウェイのロード バランサ IP アドレスを追加する例

次のコードブロックに例を示します。RADIUS サーバに固有の適切な構文を使用する必要があることに注意してください。

```
client MYPODUAGEXTLBIP {
  ipaddr = 52.191.236.223
  secret = myradiussecret
}
```

Horizon Cloud ポッドからのゲートウェイ構成の削除

Microsoft Azure にデプロイされた Horizon Cloud ポッドからゲートウェイ構成を削除するには、ポッドの詳細ページで [削除] アクションを使用します。たとえば、ポッドがデプロイされた後、そのゲートウェイ タイプを新しい構成で再度設定し直すことが必要になる場合があります。このシナリオでは、まずポッドから既存のゲートウェイ構成を削除し、それからポッドを編集してゲートウェイを再度設定します。

注意：

- ゲートウェイ構成を削除すると、そのゲートウェイに接続されているすべてのユーザー セッションが直ちに終了します。
- ゲートウェイを削除することは、元に戻せないアクションです。特定の削除されたゲートウェイ構成を復元することはできません。後でポッドを編集して、削除された構成に代わるものとして新しいゲートウェイ構成を追加できます。

Horizon Cloud ポッドには、外部ゲートウェイ構成、内部ゲートウェイ構成、またはその両方が含まれる場合があります。削除する特定のタイプを [削除] アクションから選択します。ポッドから両方のゲートウェイ構成を削除する場合は、一度に 1 つずつ削除する必要があります。

重要： システムがポッドの構成を変更している場合、変更が完了するまでは次の制限が適用されます。

- ポッドでは管理タスクを実行できません。一例として、ポッドへの変更が完了するまで、ポッドの詳細ページの [編集] ボタンは使用できなくなります。
- ポッドによってサービスが提供される、デスクトップまたはリモート アプリケーションにセッションを接続していないエンド ユーザーは、接続を試みると失敗します。
- ポッド上の削除していないゲートウェイによってサービスが提供されているセッションを接続しているエンド ユーザーは、それらのアクティブなセッションを切断されることになります。データの損失は発生しません。構成の変更が完了した後に、これらのユーザーはその残りのゲートウェイを使用して再接続できます。

ヒント: コンソールは動的です。ポッドの現在の構成や環境全体の構成に基づいて、意味のある適切なワークフローおよびトグルやフィールドのみが、ユーザー インターフェイスで利用できるようになります。

手順

1 コンソールで [キャパシティ] ページに移動し、ポッドをクリックしてその詳細ページを開きます。

2 ポッドから削除するゲートウェイ タイプに対して適切なアクションをクリックします。

- [削除] - [外部 UAG] では、ポッドの外部ゲートウェイ構成を削除します。
- [削除] - [内部 UAG] では、ポッドの内部ゲートウェイ構成を削除します。

3 本当に削除してよいか確認します。

結果

システムによって、Microsoft Azure でゲートウェイのリソースを削除するプロセスが開始されます。

注： 作成したリソース グループにデプロイされた外部の Unified Access Gateway 構成を削除すると、削除プロセスが完了したときに、一部のポッド以外のアーティファクトがリソース グループに残る場合があります。必要に応じて、削除プロセスの完了後にこれらのアーティファクトを手動で削除することができます。

ファーム用および VDI 割り当て用 Horizon Cloud ポッドでの複数のテナント サブネットの使用の概要

追加のテナント サブネットをポッドに構成することにより、そのサブネットをファーム用や VDI 割り当て用に指定することができます。ファームとデスクトップ仮想マシンをすべてポッドのテナント サブネットに接続するのではなく、ファームと VDI 割り当てごとに、その仮想マシンの接続先にする特定のサブネットを 1 つ以上指定できます。追加の仮想マシン サブネットがポッドに構成されていないと、デフォルトでは、ファームと VDI デスクトップ仮想マシンがすべてポッドのテナント サブネットに接続されます。ポッドを編集して複数のテナント サブネットを追加するこの機能は、2298.0 以降のポッド マニフェストで使用できます。この機能は、Universal Broker を使用するように構成されたテナント環境およびシングルポッド仲介用に構成されたテナント環境で使用できます。

注： このようなテナント サブネットは、仮想マシン サブネットともいいます。ドキュメントと Horizon Universal Console では、いずれの名前でも言及されています。

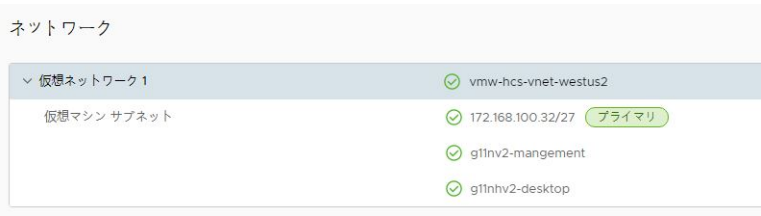
追加の仮想マシン サブネットは、ポッド（ポッド マネージャ仮想マシン）と同じ VNet に含めることも、コア ポッドが配置されている VNet とピアリングされる別の VNet に配置することもできます。ピアリングされた VNet を使用する場合は、ポッドと同じサブスクリプションおよび Microsoft Azure リージョンにある必要があります。

重要： これらの追加の仮想マシン サブネットをポッドに追加する場合は、Microsoft Azure ポータルを使用してネットワーク セキュリティ グループ (NSG) を追加し、ネットワークの分離を行う必要があります。Horizon Cloud ポッドの編集ワークフローでは、このような NSG は作成されません。

ポッド デプロイヤを使用してポッドを初めて作成する場合、ポッド デプロイ ウィザードでテナント サブネットを指定します。このテナント サブネットは、プライマリ仮想マシン サブネットといいます。コンソールでは、ポッドの詳細ページの [ネットワーク] セクションにポッドのテナント サブネット（プライマリと追加の両方）に関する情報が含まれています。以下のスクリーンショットは、追加のテナント サブネットがまだ追加されていないポッドを示し

ています。この場合、ポッドは名前付きサブネットを使用してデプロイされています。ポッド デプロイ ウィザードで、tenant という名前のサブネットがポッドのプライマリ仮想マシン サブネットに選択されています。コア ポッド仮想マシン、ゲートウェイ仮想マシン、基本イメージ仮想マシンはすべて、このプライマリ仮想マシン サブネットへの接続があります。

次のスクリーンショットは、2 つの仮想マシン サブネット（tenant5 と tenant6）が追加された後の同じポッドを示しています。

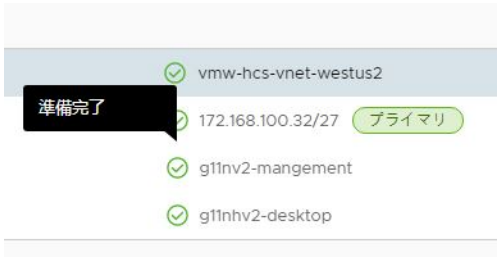


追加の仮想マシン サブネットを追加するには、[ポッドの編集] ワークフローを使用します。ファームおよび VDI デスクトップ割り当てに対して複数のテナント サブネットを使用するように Horizon Cloud ポッドを編集を参照してください。ポッドには仮想マシン サブネットを最大 40 個構成できます。プライマリ仮想マシン サブネットと追加の仮想マシン サブネット 39 個の計 40 個です。

追加のサブネットが追加されると発生する操作

[ポッドの編集] ワークフローで [保存して終了] をクリックして、選択したサブネットを追加すると、ポッド マネージャ仮想マシンとゲートウェイ仮想マシンを更新するバックグラウンド タスクが実行されるので、追加したサブネットに最終的に接続されるファーム仮想マシンとデスクトップ仮想マシンとは、当該サブネット経由で通信できるようになります。更新がエラーなしで完了した場合、追加したサブネットは 準備完了 状態に設定されます。エラーが発生した場合、当該サブネットは エラー 状態に設定されます。

次のスクリーンショットは、追加したサブネットが 準備完了 状態になっていることを示しています。



サブネットが エラー と表示されている場合は、[失敗したネットワークの再デプロイ] アクションを使用してシステム タスクを再試行します。ポッドの詳細ページで、[...] - [失敗したネットワークの再デプロイ] - [ ] をクリックします。

追加した仮想マシン サブネットをポッドの構成から削除する

ポッドの構成で設定されている仮想マシン サブネットを使用する必要がなくなった場合は、[ポッドの編集] ワークフローを使用して、ポッドの構成からそのサブネットを削除できます。このワークフローを実行して仮想マシン サブネットを削除するのは、そのサブネットを使用するファームまたは VDI デスクトップ割り当てがなくなった場合のみにしてください。[ポッドの編集] ワークフローを開始し、表示されるリストで削除するサブネットを選択解除して、変更内容を保存します。

重要：

- ファームまたは VDI デスクトップ割り当てによって使用されている仮想マシン サブネットを削除しようとすると、[ポッドの編集] ウィザードで変更を保存できても、そのようなサブネットはポッドの構成から削除されません。この状況では、コンソールの [監視] - [アクティビティ] - [監査ログ] を使用して、このようなサブネットに関する情報を確認できます。
- ポッドからのプライマリ仮想マシン サブネットの削除はサポートされていません。そのサブネットは、ポッドに必要なテナント サブネットです。

ファームおよび VDI 割り当てへの仮想マシン サブネットの使用について

サブネットは、準備完了 状態にある場合、ファームおよび VDI デスクトップ割り当ての定義で使用できます。ファーム仮想マシンと VDI デスクトップ仮想マシンは、定義で指定するサブネットに接続されます。

- ファームと VDI デスクトップ割り当ての作成時にも編集時にもこれらの仮想マシン サブネットを指定できます。
- 1 つのファームまたは VDI デスクトップ割り当てに複数の仮想マシン サブネットを指定すると、そのファームの仮想マシンや割り当ての仮想マシンは指定のサブネット全体にわたってロード バランシングされます。

  注： これらの仮想マシン サブネットを使用してファームまたはデスクトップ割り当てを作成する際、追加した仮想マシン サブネットに加え、ポッドのプライマリ仮想マシン サブネット（ポッドのテナント サブネット）が選択できます。

- 現在のリリースでは、ファームまたはデスクトップ割り当てにサブネットを割り当てた後に、そのサブネットをファームまたはデスクトップ割り当てから割り当て解除することはできません。

仮想マシン サブネットのステータス

ポッドの詳細ページで色が付いているアイコンは、そのサブネットのステータスを示します。コンソールで、アイコンの上にカーソルを置くと、ステータス ラベルが表示されます。

ステータス	説明
保留中	[ポッドの編集] ワークフローを実行して新しいテナント サブネットを追加すると、システムのバックグラウンド タスクが進行する間、サブネットは 保留しています ステータスで開始されます。通常、このステータスの時間は短くなります。
準備完了	テナント サブネットに関連するすべての操作が正常に行われると、インジケータは 準備完了 ステータスを表示します。
エラー	サブネットに関連するいずれかの操作が失敗すると、インジケータは エラー ステータスを表示します。
削除中	[ポッドの編集] ワークフローを実行してテナント サブネットを削除すると、システムのバックグラウンド タスクが進行する間、インジケータは 削除中 ステータスを表示します。

ファームおよび VDI デスクトップ割り当てに対して複数のテナント サブネットを使用するように Horizon Cloud ポッドを編集

ポッドに複数のテナント サブネットを構成するには、[ポッドの編集] ワークフローを使用します。これらのサブネットは、仮想マシンのサブネットとも呼ばれます。Microsoft Azure のポッドで複数のテナント サブネットを使用できるこの機能は、2298.0 以降のポッド マニフェストで使用できます。これらのサブネットをポッドの構成に追加して、ファーム内の仮想マシンおよび VDI デスクトップ割り当てで使用できるようにします。

複数のテナント サブネット機能の概要については、ファーム用および VDI 割り当て用 Horizon Cloud ポッドでの複数のテナント サブネットの使用の概要 を参照してください。

注： ポッドへの追加がサポートされている追加のテナント サブネットの最大数は 39 です。したがって、ポッドに対してサポートされているテナント サブネットの数は、40（1 つのプライマリ テナント サブネットと 39 の追加サブネット）になります。

前提条件

ポッドに追加するテナント サブネットが Microsoft Azure ポータルですでに作成されていることを確認します。これらのサブネットは、ポッドと同じ VNet（ポッド マネージャ仮想マシン）に配置することも、別の VNet に配置することもできます。異なる VNet にある場合、それらの VNet はポッドの VNet とピアリングされている必要があります。ピアリングされた VNet を使用する場合は、ポッドと同じサブスクリプションおよび Microsoft Azure リージョンにある必要があります。

テナント サブネットが空であることを確認します。他のリソースがこれらのサブネットに接続されていないことを確認します。

重要： これらの追加の仮想マシン サブネットをポッドに追加する場合は、Microsoft Azure ポータルを使用してネットワーク セキュリティ グループ (NSG) を追加し、ネットワークの分離を行う必要があります。Horizon Cloud ポッドの編集ワークフローでは、このような NSG は作成されません。

手順

1 ポッドの詳細ページから [編集] をクリックして、ポッドの編集ワークフローを開始します。

2 [ポッドの詳細] の手順に移動して、[ネットワーク] セクションを探します。

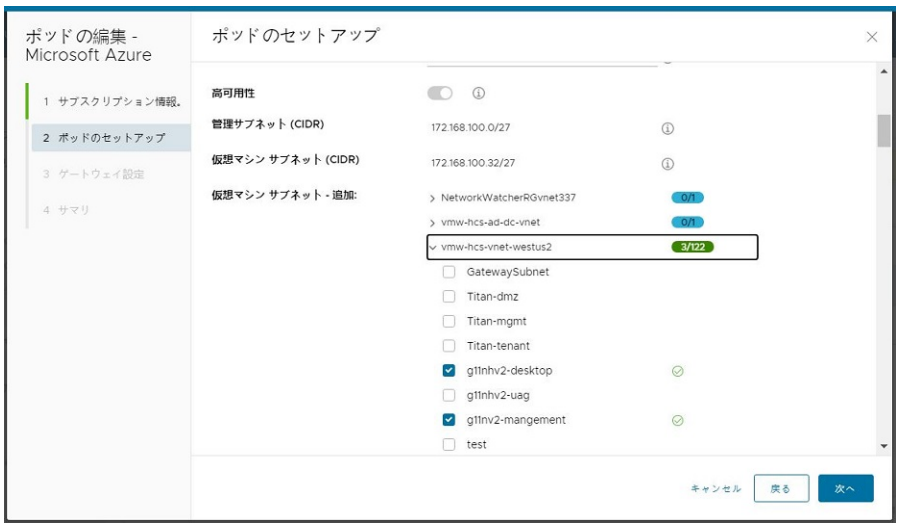
このセクションには、ポッドの現在のネットワーク構成が表示されます。[仮想マシンのサブネット - 追加] 領域には、ポッドのサブスクリプションで見つかった VNet が表示されます。各 VNet の横にあるアイコンは、ポッドにすでに接続されているサブネットの数を示しています。

3 ポッドに追加するサブネットを持つ VNet を展開します。

VNet 内のサブネットのセットが表示されます。ポッドでも使用されている VNet を展開すると、ポッドのプライマリ仮想マシンのサブネットには、その仮想マシンの横にインジケータが表示され、すでに選択されています。

4 追加するサブネットを選択します。

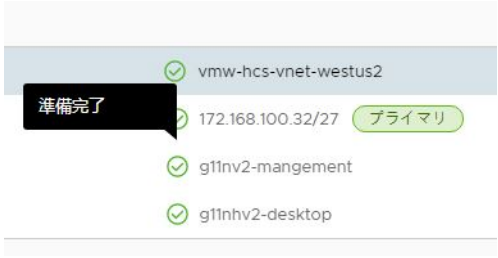
次のスクリーンショットは、`tenant` という名前のサブネットがポッドのプライマリ テナント サブネットであり、ポッドに追加するために 2 つの追加のサブネットが選択されていることを示しています（`tenant5` および `tenant6`）。



5 [保存して終了] をクリックします。

結果

ファーム用および VDI 割り当て用 Horizon Cloud ポッドでの複数のテナント サブネットの使用の概要 で説明するように、システムのバックグラウンド タスクは、必要なポッド構成の変更を行うために実行されます。これらのタスクが正常に完了すると、サブネットがポッドの詳細ページに READY 状態で表示されます。



次のステップ

- Microsoft Azure ポータルを使用して、これらのサブネットにネットワーク セキュリティ グループ (NSG) を追加し、これらのサブネットにネットワークの分離を提供します。Horizon Cloud ポッドの編集ワークフローでは、このような NSG は作成されません。
- 仮想マシンのサブネットがポッドに正常に追加された場合は、ファームおよび VDI デスクトップ割り当てで使用を開始できます。

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

このページでは、Horizon Universal Console の [サブスクリプションの管理] ワークフローを使用して、Horizon Cloud 環境に保存されているサブスクリプション情報を変更、修正、または更新する方法を説明します。このワーク

フローの使用事例の 1 つとして、サブスクリプションのキーの有効期限が近づいていて、Azure ポータルで新しいキーを作成した場合に、そのサブスクリプション内のポッドでその新しいキーを使用するようにすることです。

重要： システムの既知の問題により、この手順は設計どおりに機能しません。この問題により、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、各仮想マシンで管理サービスが再起動されるまで、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。その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。

この既知の問題は、Horizon Cloud - 既知の問題ページに記載されています。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 (SR) を開いて、Horizon Cloud オペレーション チームに各ポッド マネージャ仮想マシンの管理サービスの再起動を依頼してください。SR で、既知の問題と内部問題番号 2979394 および 3017415 を参照してください。

簡単な紹介

状況によっては、これらのサブスクリプションにデプロイされたポッドに関連付けられている Microsoft Azure サブスクリプション情報を変更、修正、または更新する必要がある場合があります。

同様に、この機能を使用して、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を使用して外部ゲートウェイをデプロイする場合は、サブスクリプション情報の変更が必要になる場合があります。

[サブスクリプションの管理] ワークフローは、新しいサブスクリプション情報を環境に追加するためにも使用されます。また、ポッドに関連付けられていないサブスクリプション情報を完全に削除して、Horizon Cloud に表示されないようにすることもできます。

典型的な使用事例

デプロイされたポッドに関連付けられている Microsoft Azure サブスクリプション情報を変更、変更、または更新する必要があるかどうかをどのようにして確認できますか。

サブスクリプションのアプリケーション キーを作成して有効期限を 1 年にし、現在、360 日目が近づいているとします。

最終の 365 日目が経過して、キーの有効期限が切れる前に、まず Microsoft Azure ポータルを使用してサブスクリプションの新しいキーを作成し、Horizon Universal Console に保存されているサブスクリプション情報をすぐに変更して新しいキーの使用を開始する必要があります。

Microsoft Azure ポータル側と Horizon Universal Console 側の両側のサブスクリプション情報が一致すると、Horizon Cloud 環境に保存されているサブスクリプション情報は、そのサブスクリプションにすでにデプロイされているポッドで使用できます。

これらの手順のコンソールの場所

ポッドまたはその外部ゲートウェイ（そのゲートウェイが別のサブスクリプションでデプロイされている場合）で使用されるサブスクリプション情報を [キャパシティ] ページの [リソース] タブから更新します。サブスクリプション情報フィールドの説明については、第 1 世代テナント - Microsoft Azure 上の Horizon Cloud ポッド - 第 1 世代 Horizon Universal Console の [キャパシティ] ページを使用した、ポッド フリートへのポッドの追加ページを参照してください。

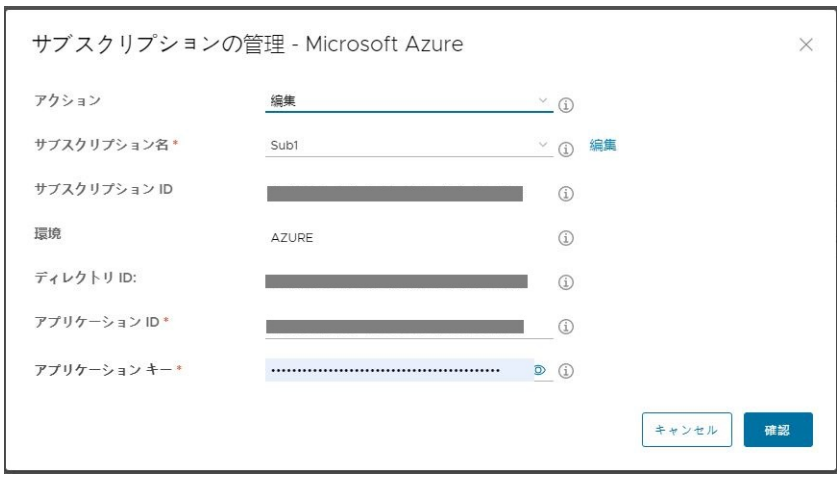
手順

1 コンソールで、[キャパシティ] ページに移動して、[リソース] をクリックします。

次のスクリーンショットは、2 つの名前付きサブスクリプションが一覧表示された [リソース] タブを示しています。それぞれの名前はハイパーリンクです。ハイパーリンク名をクリックすると、保存されている情報を変更できるウィンドウが開きます。

2 表示されたサブスクリプション名をクリックして、新しい値を使用するように変更します。

Microsoft Azure サブスクリプション情報のセットのハイパーテキスト名をクリックすると、[サブスクリプションの管理] ウィンドウが開き、デフォルトでは [編集] アクションが選択されています。



3 Microsoft Azure ポータルでサブスクリプションに設定した値と一致するように変更する新しい値を入力します。

[サブスクリプション名]、[アプリケーション ID]、および [アプリケーション キー] を変更することができます。[アプリケーション キー] フィールドにキーを表示するためのアイコンがある場合でも、キーは非表示のままになります。新しいサブスクリプション名を入力するには、[サブスクリプションの管理] ウィンドウの [サブスクリプション名] メニューの横にある [編集] をクリックします。

注： [環境]、[サブスクリプション ID]、および [ディレクトリ ID] の値を更新することはできません。

4 [確認] をクリックします。

次のステップ

変更が [アプリケーション キー]（クライアント プライベート キー）の更新のみである場合は、既知の問題のため、このページの上部にある重要な通知のガイダンスに従う必要があります。

ここでは、クライアント プライベート キーを変更したときに、ユースケースにおけるその重要性を誤って見落とさないようにするために、ページの下部に重要な通知が繰り返し表示されています。

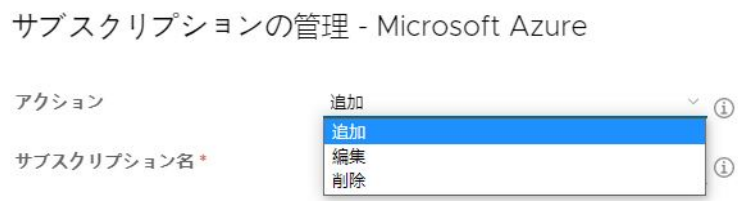
重要： システムの既知の問題により、この手順は設計どおりに機能しません。この問題により、コンソールの [サブスクリプションの管理] ウィンドウで [アプリケーション キー] 設定を編集して保存した後、各仮想マシンで管理サービスが再起動されるまで、新しく入力したプライベート キーがポッド マネージャ仮想マシンで有効になりません。そのサービスが再起動されない場合、サービスがサブスクリプション内のリソースを操作するために使用する API 呼び出しが失敗し始めます。

この既知の問題は、Horizon Cloud - 既知の問題ページに記載されています。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 (SR) を開いて、Horizon Cloud オペレーション チームに各ポッド マネージャ仮想マシンの管理サービスの再起動を依頼してください。SR で、既知の問題と内部問題番号 2979394 および 3017415 を参照してください。

Horizon Cloud：Microsoft Azure サブスクリプション情報の削除、編集、および追加

Horizon Universal Console の [サブスクリプションの管理] ワークフローを使用して、Horizon Cloud 環境に保存されている Microsoft Azure サブスクリプション情報を編集または削除します。また、このワークフローを使用して、そのサブスクリプションのキャパシティにポッドをデプロイする前に、Horizon Cloud に保存する Microsoft Azure サブスクリプション情報を追加することもできます。

ポッドのデプロイ プロセスで Microsoft Azure サブスクリプション情報を使用することに加えて、Horizon Cloud は Microsoft Azure サブスクリプション情報を使用して、Microsoft Azure クラウドのサブスクリプションのキャパシティにデプロイしたポッドを実行および管理する必要があります。ポッドのデプロイ ウィザードで指定したサブスクリプション情報は Horizon Cloud 環境に保存されます。情報は、指定した名前を使用して、構成設定として保存されます。[サブスクリプションの管理] ワークフローを使用すると、これらの保存されたサブスクリプション構成を追加、編集、および削除できます。



注： 既存の Microsoft Azure サブスクリプションが保存されていない場合は、[アクション] メニューの [追加] オプションのみを利用できます。

[サブスクリプションの管理] ワークフローを起動する方法

[サブスクリプションの管理] ワークフロー全体は、コンソールの [キャパシティ] ページの [リソース] タブの [管理] アクションまたは [はじめに] ページから起動できます。次のスクリーンショットは、[キャパシティ] ページの [管理] アクションの場所を示しています。

[リソース] タブに一覧表示されているサブスクリプションの名前をクリックして、ワークフローを起動することもできます。特定の名前をクリックすると、[サブスクリプション名] フィールドにデフォルトで選択されている名前の [サブスクリプションの管理] ウィンドウが開き、その名前で保存されている情報が事前に入力されたその他のフィールドが表示されます。

注： 特定の名前をクリックして [サブスクリプションの管理] を開くと、[アクション] メニューで [編集] オプションが事前に選択されています。システムは、特定の項目をクリックしたときに、その特定の構成を更新することを想定しています。

既存のサブスクリプションの編集

Horizon Cloud がデプロイしたポッドとともに使用することに依存する Microsoft Azure ポータルのサブスクリプション情報を変更した場合は、Horizon Cloud に保存されている構成の対応する情報を更新する必要があります。Microsoft Azure ポータル側と Horizon Universal Console 側の両側のサブスクリプション情報が一致する場合のみ、Horizon Cloud 環境に保存されているサブスクリプション情報は、そのサブスクリプションにすでにデプロイされているポッドで使用できます。たとえば、Microsoft Azure 側でサブスクリプションのアプリケーション ID を変更する場合、Horizon Cloud にログインし、[サブスクリプションの管理] ワークフローの [編集] アクションを使用して、保存された構成の [アプリケーション ID] フィールドを一致するように更新します。

編集手順については、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、更新を参照してください。

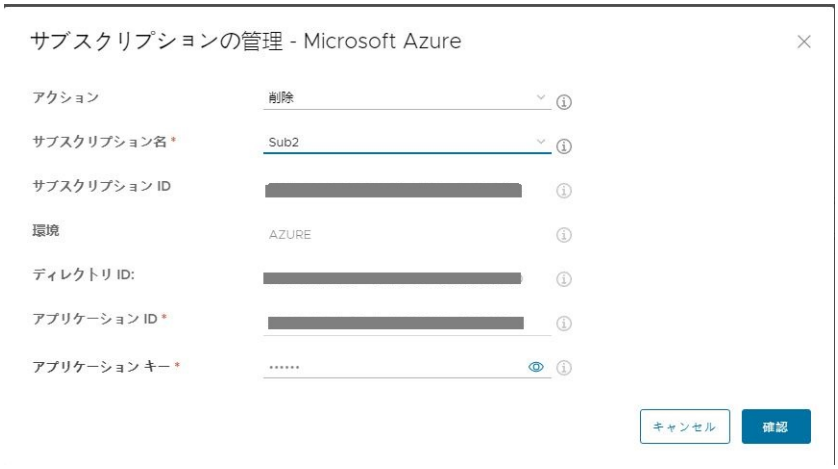
既存のサブスクリプションの削除

編集のほかに、このワークフローでは、そのサブスクリプション名に関連付けられたすべてのポッドが削除されたときに、保存済みの構成を削除することもできます。保存済みの構成を削除すると、次回ポッドのデプロイを開始したときに、そのサブスクリプション名がポッド デプロイ ウィザードに表示されなくなります。このように使用されなくなったサブスクリプション名を削除することは、新しいポッドを繰り返しデプロイしてから削除した後再デプロイし、さらに以前のデプロイから保存されたサブスクリプション情報を削除しようとする Horizon Cloud 環境からトライアルや事前検証 (POC) を実行している場合に役立ちます。

指定されたサブスクリプション情報のセットを削除するには、次の手順を実行します。

1 [キャパシティ] ページの [リソース] タブで、Horizon Cloud から削除するサブスクリプションの名前をクリックします。次のスクリーンショットは、クリック可能な名前 `sub1` と `sub2` を示しています。

2 表示される [サブスクリプションの管理] ウィンドウで、クリックしたサブスクリプション名が削除対象であることを確認し、[アクション] メニューの [削除] を選択します。次のスクリーンショットは、名前 `sub2` の下に保存されたサブスクリプション情報の [削除] アクションの選択を示しています。



注： サブスクリプション名に関連付けられているポッドがある場合は、削除できないというメッセージが表示されます。ゼロ ポッドが関連付けられているサブスクリプション名のみを削除できます。

3 [確認] をクリックします。

Microsoft Azure クラウドにデプロイしたすべてのポッドを削除し、保存されているすべてのサブスクリプション情報を削除する使用事例では、[はじめに] ページに移動し、そのポッドの [管理] - [サブスクリプションの管理] ウィンドウを開いて、指定された情報のセットを削除します。

新しいサブスクリプション情報の追加

[サブスクリプションの管理] ワークフローでは、サブスクリプション情報の新しいセットを追加し、ポッドのデプロイ ウィザードの外部にある Horizon Cloud 環境に保存することもできます。この使用事例は、チームの 1 人が特定のバージョンを使用してすべてのサブスクリプション情報を追加するときに、チームの別の担当者が実際にポッドを展開する責任を負うなど、チームのメンバーに明確な責任がある場合に役立ちます。最初の担当者は、ポッドのデプロイ プロセスの前に、すべての情報を Horizon Cloud に追加できます。

重要： 新しい情報を入力する場合は、入力するサブスクリプション情報が第 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述されるサブスクリプション要件を満たしていることを確認する必要があります。特に、サービス プリンシパルに必要な役割の権限が付与されていることを確認してください。情報がサブスクリプション要件を満たしていない場合、新しいポッドを展開するワークフローでこの指定されたサブスクリプション情報のセットを選択すると、ワークフローが失敗することがあります。

新しいサブスクリプション情報のセットを追加して Horizon Cloud に保存するには、次の手順を実行します。

1 [キャパシティ] ページの [リソース] タブで、[管理] をクリックします。

注： [はじめに] ページで新しいサブスクリプションを追加する場合は、[管理] - [サブスクリプションの管理] の順にクリックします。

2 [サブスクリプションの管理] ウィンドウで、[アクション] が [追加] に設定されていることを確認します。

3 [サブスクリプション名] に、保存されているサブスクリプション情報のセットに使用する名前を入力します。コンソールは、ページでこの名前を使用し、サブスクリプションに関連するワークフローを使用します。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。

4 Microsoft Azure サブスクリプション情報を指定します。

オプション	説明
[環境]	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。 ■ [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。

オプション	説明
[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。

5 [確認] をクリックします。

Horizon Universal Console を使用して、サブスクリプションによる Microsoft Azure 制限の現在の使用率を調べる

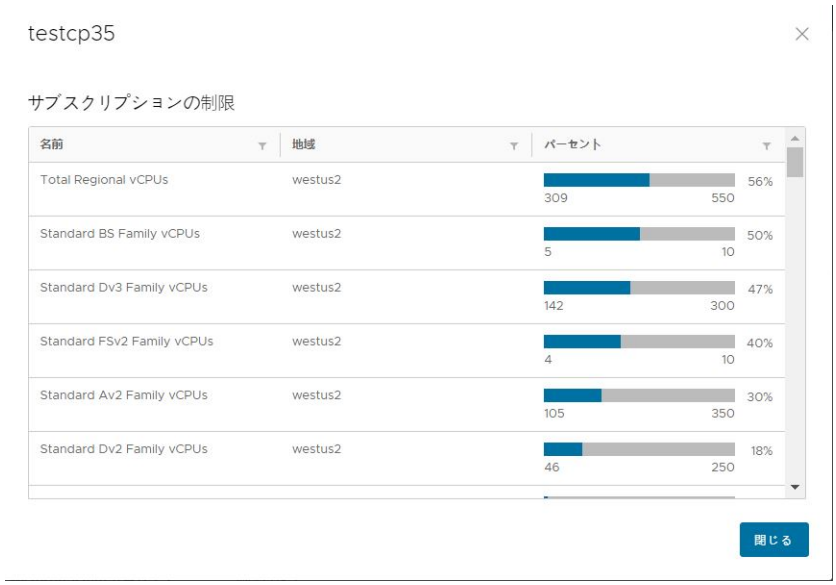
Horizon Cloud はポッドでのサブスクリプションの制限の使用率を監視します。Microsoft Azure の制限は、クォータとも呼ばれます。[ダッシュボード] ページでは、使用率がサブスクリプションで許可される上限に近づくと、健全性に関する警告情報が表示されます。特定のサブスクリプションの現在の使用状況は、そのサブスクリプションのポッドのポッドの詳細ページで確認できます。

Microsoft Azure のサブスクリプションに登録するときは、Microsoft Azure の制限について特定のキャパシティをサインアップします。これらの制限のタイプは、サブスクリプションごとの仮想マシンやサブスクリプションごとのコアのようなものです。各ポッドは、ポッドに関連付けられたサブスクリプションの Microsoft Azure の制限からクォータを使用します。

手順

1 コンソールで [設定] - [キャパシティ] の順に移動し、そのサブスクリプション内のポッドの詳細ページを開きます。

2 ポッドの詳細ページで、[サブスクリプションの制限] フィールドに移動し、ハイパーリンクされた値をクリックして、サブスクリプションによるさまざまな Microsoft Azure 制限の使用率を確認します。



結果

サブスクリプションについて制限に到達している割合が高いことが報告されていて、さまざまな種類でコアまたは仮想マシンの最大数に近づいていることが示されている場合、Microsoft Azure のサブスクリプションで割り当てられているコアの数を増やすことができます。Microsoft Azure 環境のさまざまなリソースのサブスクリプションのクオータを増やすには、Microsoft Azure ポータルを使用します。ポータルにログインして、[サブスクリプション] に移動します。サブスクリプションの名前を選択し、[使用量 + クォータ] をクリックしてサブスクリプションの使用量レベルを表示します。そのページで、[増加を要求] をクリックすると、そのサブスクリプションのより高いクォータを取得します。

Horizon Cloud ポッド - メンテナンスと更新

このドキュメント ページでは、デプロイされた Horizon Cloud ポッドを構成する VMware ソフトウェア コンポーネントのメンテナンスに関する重要な事項について説明します。

簡単な紹介

システムのメンテナンス アクティビティには、ポッドのソフトウェア コンポーネントの自動更新が含まれており、サービスのサポート性と回復性の修正と改善、新機能も含まれます。

ほぼダウンタイムなしでポッドおよびゲートウェイ アプライアンスの更新を完了するために、システムはエンドユーザー セッションの数を使用します。アクティブなセッションで環境に接続しているユーザーの数が少ない場合、システムはセッション数を使用して更新を完了する最適なタイミングを決定します。

既存のポッドを新しいマニフェストに更新するメンテナンス アクティビティは、クラウド プレーンからシステムによって開始され、システムによって決定された日時に実行されます。

このようなシステム メンテナンス アクティビティを特定の時間と曜日に開始することを希望する場合は、コンソールを使用して、各ポッドの優先メンテナンス ウィンドウを指定します。

コンソールで優先メンテナンス ウィンドウが指定されていないポッドは、VMware がいつでも都合の良い時にそのポッドのメンテナンスをスケジューリングできると解釈されます。

注： IT またはセキュリティ組織で、Horizon Cloud on Microsoft Azure 環境のサブスクリプションでの Azure Marketplace オファーの使用またはマーケットプレイスでの購入に制限がある場合、または環境で Azure China を使用している場合説明されているように、2022 年初頭から、サービスは、Azure Marketplace で提供される VMware オファーをプログラムで使用するようにアップグレード コードを強化しました。アップグレードの事前確認で、サブスクリプションでこれらの VMware オファーのプログラムによる使用が禁止されていると判断された場合は、そのドキュメント ページに記載されているアクションを完了して更新をブロックするエラーを解決する必要があります。

たとえば、ポッドとそのゲートウェイ構成に使用されるサブスクリプションに関連付けられている Horizon Cloud サービス プリンシパルがカスタム ロール（非定型）を使用している場合、カスタム ロールにこれらの 2 つの権限が含まれていることを確認してください。拡張されたアップグレード API コードは、これらの権限に依存してマーケットプレイスからオファー リストを取得し、VMware オファーを取得します。カスタム ロールにこれらの 2 つの権限がまだ含まれていない場合は、ポッドとゲートウェイのアップグレード プロセスが実行される前に、それらをカスタム ロールに追加してください。

```
Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read
Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write
```

デプロイされたポッドで使用されるソフトウェア コンポーネントが新しいバージョンに更新されると、ポッドのマニフェスト番号は 2632.0 などのより高いバージョン番号に増加します。ポッドのサービス性とサポート業務で重要と考えられる改善点がある場合、VMware は 2632.1 などのポイント バージョンの新しいマニフェストを作成できます。コンソールの [キャパシティ] ページにポッドのマニフェストが表示されます。

3328 より前のマニフェストからのポッドの更新に関する重要な情報

2022 年 2 月以降、ポッド マネージャ仮想マシンの NIC は、Unified Access Gateway 仮想マシンの NIC と同じインフラストラクチャ設計パターンに従います。

その時点で開始された新しいポッドのデプロイ、およびマニフェスト 3328 より前のマニフェストからのポッドの更新では、デプロイヤは、ポッドの実行とその後の更新をサポートするために必要なすべてのネットワークをインスタンス化します。ポッドのリソース グループに次の 8 つの NIC が追加されます。

- ポッドの管理サブネットから 4 つの IP アドレスを予約する 4 つの NIC。
- ポッドのプライマリ仮想マシン サブネット（旧称テナント サブネット）から 4 つの IP アドレスを予約する 4 つの NIC。

これらの 8 つのポッド NIC は持続し、割り当てられた IP アドレスをポッドの存続期間中予約し続けます。

この設計では、より高速で回復力の高いポッドの更新がサポートされます。この設計より前は、ポッドの更新では、Green ポッドのビルドアウトの一部として新しい NIC を作成し、更新時にポッドのサブネットからそれらの NIC の IP アドレスを取得する必要がありました。その設計では、Azure でタイムアウトが発生し、更新プロセスが中断される可能性があります。

デプロイヤが必要なすべてのネットワークを前もってインスタンス化するこの設計では、管理および仮想マシン（テナント）サブネットの NIC とその IP アドレスが保持され、後続のポッドの更新で使用されます。この設計は、Unified Access Gateway インスタンスで使用されるパターンに従います。

ポッドのリソース グループに 8 つの NIC がまだ存在せず、ポッドがマニフェスト 3328 以降に更新されるようにスケジュール設定されている場合は、次のアクションを実行する必要があります。

そのポッドを更新する前に、ポッドの管理サブネットの IP アドレスとプライマリ仮想マシン（テナント）サブネットの IP アドレスが、Horizon Cloud on Microsoft Azure が作成および構成するアイテムによってのみ取得されることを確認してください。

- 管理サブネット - ポッド デプロイヤが作成および構成した、Horizon Cloud on Microsoft Azure デプロイの特定の NIC のみが、ポッドの管理サブネットからの IP アドレスを使用する必要があります。これらの NIC は、ポッド マネージャの NIC と、ポッドの Unified Access Gateway インスタンスの NIC です。ポッドの管理サブネットには、ポッドがデプロイされていないリソースまたはアイテムを接続したり、ポッドから IP アドレスを取得したりすることはできません。
- テナント サブネット - ポッド デプロイヤが作成および構成した、Horizon Cloud on Microsoft Azure デプロイの特定の NIC およびロード バランサのみが、ポッドのテナント サブネットからの IP アドレスを使用する必要があります。ポッドのテナント サブネットには、デプロイ以外のリソースまたはアイテムを接続したり、ポッドから IP アドレスを取得したりすることはできません。

『デプロイ ガイド』には、ポッドで使用されるサブネットには、ポッド デプロイのリソース以外に追加のリソースを接続する必要はないと正確に記載されています。手動でリソースを作成し、ポッドの管理またはテナント サブネットからそのような追加のリソースに IP アドレスを割り当てた場合は、ポッドの更新を実行する前にそれらのリソースからそれらの IP アドレスを削除する必要があります。そうしないと、ポッドの更新に失敗し、VMware のサポートが必要になります。

ポッドを更新した後、更新前に設定したファイアウォール ルールに、ポッドのリソース グループ内のデプロイヤが作成した NIC によって予約されたすべての IP アドレスを追加します。

ポッド マネージャ仮想マシンの NIC の IP アドレスからのトラフィックを制御する既存のファイアウォール ルールがある場合があります。ポッドの更新後も更新前と同様にトラフィック通信が機能するようにするには、ポッドのリソース グループ内の NIC によって予約された 8 つの IP アドレスすべてが、更新後にファイアウォール ルールに反映されるようにする必要があります。

ポッドのメンテナンスに関する情報

デプロイされた Horizon Cloud ポッドを構成する VMware ソフトウェア コンポーネントのメンテナンスは、そのポッドによって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の正常性と安定性を維持するために必要な操作です。VMware Horizon Cloud Service - 追加のサービスの詳細 (KB87894) で説明したように、VMware には、ポッドに常駐し、制御プレーンからそのポッドにダウンロードされるソフトウェア コンポーネントを管理する責任があります。このナレッジベースの記事に添付されている『VMware Horizon Cloud Service - 追加のサービスの詳細』PDF には、次の情報が記載されています。

- ポッドにダウンロードされるソフトウェア コンポーネントの正常性を維持するための変更管理手順に関する VMware の役割と責任。メンテナンス アクティビティには、ポッドのソフトウェア コンポーネントの更新が含まれます。

- スケジュールされたメンテナンスや緊急メンテナンスが必要な場合の VMware との連携を含めた変更管理手順に関するユーザーの役割と責任。

『VMware Horizon Cloud Service - 追加のサービスの詳細』ドキュメントには、スケジュール設定されたメンテナンス、メンテナンス期間、および緊急メンテナンスの定義が含まれます。これらの詳細については、該当ドキュメントを参照してください。このドキュメント ページの内容と『VMware Horizon Cloud Service - 追加のサービスの詳細』ドキュメントの内容に相違がある場合は、『VMware Horizon Cloud Service - 追加のサービスの詳細』ドキュメントが優先されます。

注目: ポッドを更新する前に、ポッドのイメージ仮想マシン、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、ポッドで使用できる最新のエージェントがすべて含まれていることを確認する必要があります。ポッドを更新する前に最新のエージェントに更新しないと、ポッドの更新後に互換性のないエージェント バージョンが実行され、ポッドがサポートされていない状態になる可能性があります。更新する必要があるエージェントがあるかどうかを、どうすれば確認できますか。コンソールで、イメージまたは割り当ての横に青いドットが表示されているのを確認します。青いドットが表示されている場合は、ポッドを更新する前に、コンソールからすべての青いドットを消します。Horizon Cloud ポッドの更新：エージェントの互換性とサポートを継続するための手順を参照してください。

ポッドの優先メンテナンス ウィンドウの指定

ポッドのメンテナンス アクティビティを特定の時間と曜日に開始したい場合は、コンソールを使用して、そのポッドの優先メンテナンス ウィンドウと呼ばれる時間を指定します。[キャパシティ] ページで、ポッドの詳細ページの [メンテナンス] タブに移動します。[優先メンテナンス時間] というラベルを探し、画面上のコントロールに従って、その日の曜日名と時間 (UTC) を選択します。表示されるシステムで事前定義されたデフォルト値からのみ選択できます。

コンソールの各ポッドの詳細ページで、各ポッドの優先メンテナンス時間を個別に指定します。

注： コンソールで優先メンテナンス ウィンドウが指定されていないポッドは、VMware がいつでも都合の良い時にそのポッドのメンテナンスをスケジュール設定できると解釈されます。

システムは、コンソールで指定した曜日と時刻を読み取り、そのデータをスケジューリング アルゴリズムに組み込みます。クラウド プレーンで新しいポッド マニフェストがデフォルトとして設定されている場合、システムのスケジューラは、ポッド フリートの各ポッドで更新が発生する可能性があると判断した実際の更新日時を計算します。システムは、そのポッドの [メンテナンス] タブで指定された優先メンテナンス開始時間に対応できるように最善を尽くしますが、特定の更新操作でこの優先メンテナンス開始時間に対応できる保証はありません。

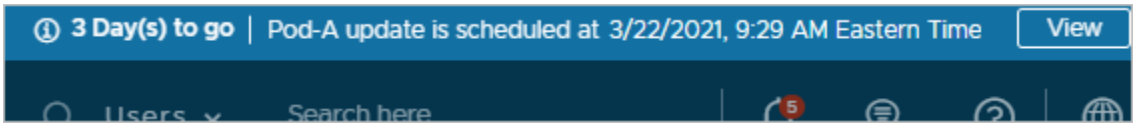
本書の作成時点で、システムのスケジューラは、メンテナンス アクティビティの期間として 4 時間を指定します。一般的なポッドの更新にかかる時間は、この割り当てられた期間よりも短い時間になります。

メンテナンス アラートと通知

システムは、特定のポッドについて特定のメンテナンスが実行されるように指定した特定のカレンダー日時をシステムがスケジュール設定したときに、テナント環境の管理者にアラートと通知を送信します。これらのアラートと通知には、次のものが含まれます。

コンソール内

- コンソールの上部に表示されるパーシステント バナー。バナーの時間は、コンソールを表示しているときの、ブラウザのタイムゾーンに対するローカルなメンテナンス時間です。次のスクリーンショットは、2020 年 7 月 7 日の米国東部時間午後 4 時にポッドの更新がスケジューリングされている例です。[表示] ボタンを使用し、クリックしてポッドの詳細ページに移動し、ポッドの [メンテナンス] タブでスケジューリングされたメンテナンスの詳細を確認します。



- ポッドの [監査ログ] タブおよびコンソールの [アクティビティ] - [監査ログ] で、監査ログにポッドのアップグレードが VMware Operations によってスケジューリングされていることが示されます。監査ログ行には、ポッドの UUID が含まれます。
- ポッドの [メンテナンス] タブで、[スケジューリングされたメンテナンス] セクションに、スケジューリングされたメンテナンスに関する情報が表示されます。

E メール

システムは、ポッドのメンテナンスに関する E メールをテナント環境の管理者（コンソールの [全般設定] - [My VMware アカウント] 設定で指定された管理者）に送信します。E メールには、システムが定期メンテナンスの特定のカレンダー日時を設定したときの E メールが含まれます。このような E メールの例には、スケジューリングされた日時より前の日と週の定期的なリマインダ、メンテナンス アクティビティの開始時、および完了時が含まれます。

注： スケジューリングされたメンテナンスの日時を再スケジューリングする場合は、VMware のサポートにお問い合わせください。

ポッドのメンテナンスを実行する前のシステム事前チェック

ポッドにポッド更新エラーがあることを通知する E メールを受信した場合、またはコンソールがポッドのポッド更新エラーを報告した場合は、状況を修正するためのアクションを実行する必要があります。この問題が発生した場合は、コンソールの画面上のガイダンスまたは E メールの指示に従ってください。このようなエラーの通常の解決策として、一般に、ポッドのサブスクリプション内の Microsoft Azure ポータルで手順を実行する必要があります。一般的なポッドの更新エラーに対する修正の詳細については、Horizon Cloud ポッド：一般的な事前チェックの失敗の対処法を参照してください。

これらの事前チェックの目的は何ですか。ポッドの更新のメンテナンス アクティビティは、ポッドの Microsoft Azure サブスクリプションおよびリソース グループで実行されます。システムが特定のポッドに対する特定の更新について、特定のカレンダー日時をスケジューリングする少し前に、システムは事前チェック操作を実行して、ポッドの更新の成功を妨げる条件が存在するかどうかを判断します。これらの事前チェックの 1 つの例として、システムは、Microsoft Azure サブスクリプションに更新の要件を満たすのに十分な適切な仮想マシン シリーズの vCore があるかどうかを確認します。事前チェックの 1 つが失敗し、条件を修正するためにアクションが必要な場合は、次の処理が発生します。

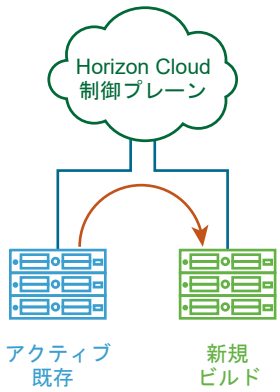
- この事実についてのアラートと、エラーの修正に必要なアクションの詳細を記載した通知 E メールが送信されます。
- コンソールには、そのポッドの事前チェック エラーを修正するために必要なアクションが視覚的アラートで表示されます。

重要： ポッドのアップグレード エラーに関する通知を受け取った場合は、指定したアクションを実行して、ただちにエラーを修正します。時間は重要な問題です。VMware で必要な時間内にこれらのエラーを解決するための操作に失敗すると、ポッドの更新プロセスを修正できなかったために、ポッドがサポートされていない状態になります。

ポッドの更新：概要

メンテナンス アクティビティがポッドの新しいマニフェスト バージョンへの更新である場合、システムはポッドの現在のインフラストラクチャ コンポーネントを適切により高いソフトウェア マニフェスト レベルに移動します。主要なインフラストラクチャ コンポーネントは、ポッド マネージャ仮想マシンと、ポッド用に構成されているすべての Unified Access Gateway 仮想マシンです。たとえば、ポッドのアップデートにはポッド管理ソフトウェア、Unified Access Gateway ソフトウェア、またはそれらの両方のアップデートを含めることができます。

このポッドの更新プロセスは、Blue-Green デプロイとして知られるソフトウェア業界の手法を模したものです。既存の更新対象のポッド コンポーネントは、Blue コンポーネントと見なされます。



ほとんどの場合、ポッドの更新は業界の Blue-Green パターンに従っていますが、標準の Blue-Green 更新とはいくつかの小さな違いがあります。ポッドの更新では、Green のビルドアウト内の Blue のリソースを 100% 複製するわけではありません。Unified Access Gateway の NIC など既存の Blue の一部は、新しい Green のビルドアウトで再利用されます。もう 1 つの違いとして、ポッドの更新プロセスでは、既存のインスタンスのほかに新しいインスタンスが作成されると、新しいインスタンスがパワーオンされ、ポッドが新しいインスタンスへの移行を完了

するまで実行を続けます。また、システムがポッドを Green のビルドアウトに移行し、ポッドが新しいマニフェスト バージョンで正常に実行されていることを検証した後、古い Blue の仮想マシンがリソース グループから削除されます。（通常、正規の Blue-Green の更新では、Green に切り替えた後も古い Blue のアーティファクトが保持され、古いアーティファクトはアイドル状態に保たれます。）

- 既存の更新されるポッド コンポーネント（ポッド マネージャ仮想マシンや仮想マシン Unified Access Gateway など）は、Blue コンポーネントと見なされます。
- サービスは、Microsoft Azure サブスクリプション内のポッドに必要な Green のコンポーネントのセット（新しい Green のポッド マネージャ仮想マシン、Unified Access Gateway 仮想マシン、ゲートウェイ コネクタ仮想マシン）を自動的に構築します（外部ゲートウェイが専用の VNet にデプロイされている場合）。
- Green のビルドアウトの新しく作成されたコンポーネントは、Blue のコンポーネントと一緒に同じリソース グループ内に作成されます。
- Green のビルドアウトを作成するプロセスでは、ダウンタイムやデータ損失は発生しません。また、パラレル仮想マシンはポッドの操作に影響しません。
- Green のセットはパラレル環境であり、Blue から Green に切り替わる、スケジューリングされたメンテナンス アクティビティの準備ができています。システムがポッドでメンテナンス アクティビティをスケジューリングする方法については、前のセクションで説明します。
- これらの Green の仮想マシンが開始され、スケジューリングされたメンテナンス アクティビティ（Blue から Green に移行するメンテナンス アクティビティ）が完了するまで実行され続けます。
- Green のビルドアウトに移行するためのスケジューリングされたメンテナンス アクティビティが完了し、ポッドが新しいインスタンスで正常に実行されると、システムはポッドのリソース グループから Blue の仮想マシンを削除します。Unified Access Gateway インスタンスの NIC など、一部のリソースは次回のポッドの更新に必要な構成の値を保持するために残ります。

注： Microsoft Azure ポータルおよびポッドのサブスクリプションで、Green のコンポーネントからシステムのビルドに影響を与えたり、システムのポッドの更新および保守プロセスに影響を与えるような変更を行わないようにする必要があります。

メンテナンス アクティビティの順序

この手順では、Green のビルドアウトへの移行について説明します。ポッドのアップデートでは、スイッチが Blue から Green に切り替わります。

1 システムは、コンソールで指定したポッドの優先メンテナンス ウィンドウをチェックし、その情報をスケジューラのアルゴリズムで使用して、ポッドのメンテナンス アクティビティの実際のカレンダー日時をスケジューリングします。

2 システムのスケジューラは、メンテナンスが実行される実際のカレンダー日時を選択します。前のセクションで説明したように、コンソールにはスケジューリングされた日時が視覚的に表示され、テナントの管理者に E メールが送信されます。

3 **重要：** スケジューリングされたメンテナンスを実行する前に、次の作業を行います。

- ポッドのイメージ仮想マシン、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、ポッドで使用できる最新のエージェントがすべて含まれていることを確認します。コンソールで青いドットが表示されている場合は、ポッドを更新する前に、コンソールからすべての青いドットを消します。詳細については、Horizon Cloud ポッドの更新：エージェントの互換性とサポートを継続するための手順
- ポッドの仮想マシン (VM) で設定した Microsoft Azure の管理ロックがあればすべて削除します。名前に vmw-hcs-`podID` のような部分（`podID` はポッドの ID 値）を持つすべての仮想マシンはポッドに属します。Microsoft Azure では、Microsoft Azure ポータルを使用してリソースが変更されないようにロックすることができます。このような管理ロックは、リソース グループ全体または個々のリソースに適用できます。ユーザーまたは組織がポッドの仮想マシンに管理ロックを適用した場合、更新を実行する前にそれらのロックを削除する必要があります。そうしないと、更新プロセスは正常に完了しません。ポッドの ID 値は、[キャパシティ] ページからアクセスできるポッドの詳細ページで確認できます。

組織のニーズに応じて、スケジュールリングされたメンテナンス時間より前であればいつでも VMware のサポートに連絡して、別のスケジューリングされたメンテナンス日をリクエストできます。

重要： コンソールに表示されるスケジューリングされた時間は、ブラウザのタイム ゾーンに対してローカルです。

4 スケジュール設定されたメンテナンス時間に、サービスは更新アクティビティを開始します。外部と内部の両方の Unified Access Gateway 構成を持つポッドの場合、完全なプロセスには通常、開始から終了まで 20 ～ 30 分かかります。

注： プロセスが完了するまでの 20 ～ 30 分間は、コンソールによって、更新中のポッドで管理タスクを実行できなくなります。たとえば、ポッド マネージャ アプライアンスがクラウド プレーンに更新が完了したことを通知するまで、ポッドの詳細ページの [編集] アクションをクリックしてそのポッドの特性を変更することができません。

Unified Access Gateway アプライアンスでのエンドユーザー セッションと更新アクティビティについて

エンドユーザー セッションのダウンタイムをゼロに近くするため、システムは、全体的なメンテナンス アクティビティ時間内に、アプライアンス上のエンドユーザー セッションの数を使用して、これらのアプライアンスの更新を完了するための最適なタイミングを決定します。

完了時間は、アクティブなセッションで環境に接続されているユーザーの数が少ない場合に発生するように最適化されています。

このゼロに近い時間枠では、アクティブなセッションを持つエンド ーザーはこれらのセッションが切断されます。数分後には、そのユーザーは再接続できるようになります。

ファームと VDI デスクトップ割り当てのタイムアウト処理に [直ちに実行] オプションを設定したシナリオを除き、データは失われません。そのシナリオでは、タイムアウト処理に [直ちに実行] オプションを使用したアクティブなセッションを持つユーザーはすぐに切断され、その設定に従ってそれらのセッションもすぐにログオフされます。このような状況では、進行中のユーザーの作業はすべて失われます。このシナリオで処理中のエンドユーザーのデータが失われるのを回避するには、メンテナンス アクティビティを開始する前に、ファームおよび VDI デスクトップ割り当ての [切断されたセッションのログオフ] の設定を、ユーザーが作業を保存する時間を確保できる値に変更します。更新が完了したら、設定を元の値に戻すことができます。

また、ゼロに近い時間枠内で、ポッドから仮想デスクトップまたはリモート アプリケーションへのセッションをまだ接続していないエンド ユーザーが、接続を試みると、プロセスが完了するまで接続できなくなります。

5 メンテナンス アクティビティが完了すると、システムは、Green のビルドアウトで再利用されない Blue コンポーネント（たとえばポッド マネージャ仮想マシンや Unified Access Gateway 仮想マシン）など、不要になったコンポーネントを削除します。ポッド マネージャ インスタンスや Unified Access Gateway インスタンスの特定の NIC など、一部のアーティファクトは今後のメンテナンスに必要な構成の値を保持するために残ります。

メンテナンス アクティビティの完了後

メンテナンス アクティビティが完了したら、ポッド上で管理タスクを実行できます。ポッドで現在実行されているソフトウェアのバージョンを表示するには、[設定] - [キャパシティ]を選択して、サマリ ページを表示するポッドをクリックします。ページに現在実行されているソフトウェア バージョンが表示されます。

- ポッドの更新後、既存のすべてのイメージ、ファーム、および VDI 割り当てのエージェントが利用可能な最新バージョンに更新されていることを確認します。これらの仮想マシンにインストールされているエージェントが更新されない場合、ポッドはサポートされていない構成になります。メンテナンス プロセスでは、それらのインストールされているエージェントは自動的に更新されません。コンソールにイメージまたは割り当てに対して青いドットが表示されている場合は、エージェントを更新する必要があります。Horizon Cloud ポッドの更新：エージェントの互換性とサポートを継続するための手順。
- この更新がマニフェスト 3328 より前のマニフェストからのものである場合は、ポッドを更新した後に、ポッドのリソース グループ内にあるデプロイヤが作成した NIC のすべての IP アドレスをファイアウォール ルールに追加してください。ポッド マネージャ仮想マシンの NIC の IP アドレスからのトラフィックを制御する既存のファイアウォール ルールがある場合があります。このポッドの更新後、およびその後のポッドの更新後も更新前と同様にトラフィック通信が機能するようにするには、ポッドのリソース グループ内の NIC によって予約された 8 つの IP アドレスすべてが、更新後にファイアウォール ルールに反映されるようにする必要があります。
- 構成済みの 2 要素認証サーバが同じ VNet にデプロイされている場合は、メンテナンス アクティビティへの移行後に、新しい内部 Unified Access Gateway 仮想マシンの新しいプライベート IP アドレスを受け入れるように 2 要素認証サーバ側の設定を更新する必要があります。これは、ポッドでの最初の更新に対する 1 回限りの要件であり、そのポッドの将来の更新で繰り返す必要はありません。必要な Horizon Cloud ポッドの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。
- 2019 年 9 月の四半期サービス リリース以降、ポッド アーキテクチャは、高可用性 (HA) を保有する機能をサポートするように更新されています。高可用性機能が有効になっていなくても、HA 対応の新しいアーキテクチャにはポッドのマネージャ仮想マシンの前に Microsoft Azure ロード バランサが含まれています。ポッドをマニフェスト 1600 に更新した後、ポッドが直接接続用に構成されていた場合は、更新されたポッドの詳細ページに新たに表示されるポッド マネージャの Azure ロード バランサの IP アドレスをポイントするように、DNS 設定を再マッピングする必要があります。DNS マッピングを更新するまでは、これらの直接ユーザー接続は引き続き機能しますが、アクティブなポッド マネージャ仮想マシンがダウンした場合に、これらの接続では HA 対応ポッドが提供するように設計されている高可用性フェイルオーバーは行われません。このユースケースでは、コネクタがポッド マネージャ仮想マシンへの接続を信頼できるように、Workspace ONE Access コネクタ アプライアンスを Microsoft Azure の Horizon Cloud ポッドと統合する場合には、ポッド マネージャ仮想マシンで SSL 証明書を直接構成します。の説明に従って、ポッドの詳細ページに表示される、[ポッド マネージャのロード バランサの IP アドレス] フィールドの IP アドレスに FQDN をマッピングします。ポッド マニフェスト 1600 以前は、その IP アドレスはテナント サブネット上のポッドのマネージャ仮想マシンの NIC

に割り当てられたものでした。ポッド マニフェスト 1600 以降では、マッピングするポッドの IP アドレスは、ポッドのマネージャ仮想マシンに使用される Microsoft Azure ロード バランサのプライベート IP アドレスになります。このリリースのマニフェスト バージョンに更新された既存のポッドの場合、マニフェスト 1493.1 以前のポッドのテナント アプライアンスの IP アドレスをポイントするように DNS 名を構成した場合は、更新したポッドの詳細ページの [ポッド マネージャのロード バランサの IP アドレス] ラベルに表示される IP アドレスをポイントするように DNS 設定を再マッピングする必要があります。

- 2474.x より前のマニフェストでは、システムは登録済みの Active Directory サーバのクロック スキューを確認しませんでした。2474.x では、クロック スキューのチェックが導入されました。登録済みの Active Directory サーバに時刻同期の問題がある場合（`clockSkew > 4 minutes`）、ポッドが 2474.x 以上にアップグレードされると、そのポッドでこのシステム検証が開始されます。その結果、クロック スキューの問題を解決するまで、Active Directory サーバの検出が失敗します。検出に失敗すると、そのポッドへのエンド ユーザー デスクトップ接続要求に影響が及ぶことがあります。

Horizon Cloud ポッド：一般的な事前チェックの失敗の対処法

このトピックでは、一般的なメンテナンスの事前チェックの失敗に対処する方法について説明します。システムの事前チェックで、ポッドのメンテナンス アクティビティをブロックする条件が明らかになった場合、これらのエラーが Horizon Universal Console に表示されます。このエラーを解決するために必要なアクションを実行できます。

重要： ポッドの更新エラーに関する通知を受け取った場合は、指定したアクションを実行して、ただちにエラーを修正する必要があります。時間は重要な問題です。VMware で必要な時間内にこれらのエラーを解決するための操作に失敗すると、ポッドの更新プロセスを修正できなかったために、ポッドがサポートされていない状態になります。

Horizon Cloud ポッド - メンテナンスと更新で説明されているように、システムは、Microsoft Azure 環境で制御されているメンテナンス ブロック条件があることをユーザーに通知します。対処方法はユーザーが制御するものであり、VMware では解決できないため、コンソールで更新エラーの通知を受け取った場合、またはそのようなエラーに関する通知の E メールを受け取った場合は、アクションを完了してエラーを解決し、VMware サポートに連絡してポッドの更新プロセスを続行する必要があります。

更新をブロックする一般的に発生するエラー

次の更新をブロックするエラーは一般的に発生するもので、Microsoft Azure 環境で解決することができます。

サブスクリプション ポリシーは、`vmware-inc` 発行者からの Azure Marketplace オファーの使用をブロックしています。

IT またはセキュリティ組織で、Horizon Cloud on Microsoft Azure 環境のサブスクリプションでの Azure Marketplace オファーの使用またはマーケットプレイスでの購入に制限がある場合、または環境で Azure China を使用している場合説明されているように、2022 年初頭から、サービスは、Azure Marketplace で提供される VMware オファーをプログラムで使用するようにアップグレード コードを強化しました。アップグレードの事前確認で、サブスクリプションでこれらの VMware オファーのプログラムによる使用が禁止されていると判断された場合は、そのドキュメント ページに記載されているアクションを完了して更新をブロックするエラーを解決する必要があります。

サブスクリプションに、パラレルの仮想マシンのためのすべての仮想マシンをインスタンス化するために使用できる適切なコア (vCPU) や仮想マシン サイズが十分にありません。

Green コンポーネントが構築されると、現在のポッド内の各仮想マシンに対して、別の仮想マシンが作成されます。その結果、Green コンポーネントが構築されるときから、コンソールでスケジューリングした時刻に Blue コンポーネントから Green コンポーネントへの移行が行われるまで、ポッド マネージャ仮想マシンと Unified Access Gateway 仮想マシンの数に重複が生じることになります。これらの仮想マシンの作成に対応するために、関連する Microsoft 仮想マシン ファミリのコア (vCPU) に対するサブスクリプションの割り当てレベルは、パラレルの仮想マシンを、既存の関連付けられたポッドのサブスクリプションですでに使用されている割り当てとともに包含するのに十分なものである必要があります。さまざまな仮想マシン タイプと使用に必要なコアについては、以下の割り当てとコアの表を参照してください。

ポッドは現在オフラインであるか、現在 Horizon Cloud と通信できません。

[キャパシティ] ページで、更新予定のポッドがオンラインのステータスを報告していることを確認します。Microsoft Azure ポータルにログインし、ポッド マネージャ仮想マシンとその Unified Access Gateway 仮想マシン（ポッドにある場合）が実行されているかどうかを確認します。仮想マシンが実行されていない場合は、パワーオンします。これらの仮想マシンが配置されているリソース グループの詳細については、第 1 世代テナント - 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 Microsoft Azure サブスクリプションでは、リソース グループを作成または削除する権限が有効になっていません。

システムの事前チェックでは、このポッドに関連付けられているサービス プリンシパルに、サービスに必要な権限が付与されている必要があります。ポッドのサブスクリプションでリソース グループを作成または削除する権限が有効になっていない場合、その自動化はブロックされます。この状況を解決するには、Microsoft Azure ポータルを使用して必要なアクセス許可を有効にする方法に関する検証のガイダンスメッセージに従います。サービス プリンシパルがサービスに必要な操作を実行するために必要な権限の詳細については、Microsoft Azure サブスクリプションで Horizon Cloud によって要求される操作を参照してください。

Green 仮想マシンのデプロイから、Blue 仮想マシンからの移行が完了するまでに必要な割り当てとコア

使用可能なコアの不足による更新エラーが通知された場合は、次の表を使用して、必要な追加のクォータを確認します。現在の状態のポッドで使用されるさまざまな仮想マシン タイプについて、このトピックの最後の表では、それらのタイプで使用される割り当て、Green ポッド仮想マシンの作成時に必要な追加の割り当て、および Green 仮想マシンが作成されてから Green 仮想マシンへの切り替えが完了するまでに、Blue と Green の両方の仮想マシンを実行するために必要な割り当ての合計について説明します。ポッドで使用される仮想マシン ファミリのタイプとコアの詳細については、『デプロイ ガイド』のポッドに対する仮想マシン要件のドキュメント トピックを参照してください。

仮想マシン タイプとそのコア	説明	Green 仮想マシンへの切り替えが完了するまで、Blue 仮想マシンと Green 仮想マシンを実行するために必要な割り当ての合計
Standard_D4_v3 仮想マシン タイプ、それぞれ 4 コア **注：** Standard_D4_v3 タイプが Microsoft Azure リージョンで使用できない場合、ポッドは通常、Standard_D3_v2 仮想マシン タイプを使用しています。このタイプも 4 個のコアを使用します。	この仮想マシン タイプは、ポッド マネージャ仮想マシンに使用されます。	**単一のマネージャ仮想マシンを持つポッドの場合** 割り当ては既存の (Blue) マネージャ仮想マシンの 4 コアに加えて、パラレルのマネージャ仮想マシン用に追加の 4 コアを許容できる必要があります。この使用量をカバーするには 8 コアが必要です。 **高可用性が有効になっている、2 台のマネージャ仮想マシンを持つポッドの場合** 割り当ては既存の (Blue) マネージャ仮想マシン（それぞれ 4 個のコアを持つ 2 台の仮想マシン）の 8 コアに加えて、パラレルのマネージャ仮想マシン用に追加の 8 コアを許容できる必要があります。この使用量をカバーするには 16 コアが必要です。
ポッドをデプロイするときに選択した内容に応じて、次のようになります。 ■ Standard_A4_v2 仮想マシンタイプ（4 コア） ■ Standard_F8s_v2（8 コア）	この仮想マシン タイプは、ポッドのゲートウェイ構成内の Unified Access Gateway 仮想マシンに使用されます。サブスクリプションでサポートする必要があるコアの数は、ポッドで構成されているゲートウェイ タイプによって異なります。	**外部ゲートウェイのみを持つポッドの場合** この外部ゲートウェイには 2 台の Unified Access Gateway 仮想マシンがあるため、2 台の仮想マシンにそれぞれのコア数を掛けます。設定するには、割り当ては既存の (Blue) Unified Access Gateway 仮想マシンの合計コア数に加えて、パラレルの Green の Unified Access Gateway 仮想マシン用に追加の重複した数のコアを許容できる必要があります。 ■ たとえば、仮想マシンがそれぞれ 4 個のコアを持つ Standard_A4_v2 である場合は、この使用量をカバーするために、2 x 4 x 2 = 16 コアが必要です。 ■ 仮想マシンがそれぞれ 8 コアの仮想マシン サイズである場合は、その使用量をカバーするために、2 x 8 x 2 = 32 コアが必要です。 **内部ゲートウェイのみを持つポッドの場合** このゲートウェイには 2 台の Unified Access Gateway 仮想マシンがあるため、2 台の仮想マシンにそれぞれのコア数を掛けます。設定するには、割り当ては既存の (Blue) Unified Access Gateway 仮想マシンの合計コア数に加えて、パラレルの Green の Unified Access Gateway 仮想マシン用に追加の重複した数のコアを許容できる必要があります。 ■ たとえば、仮想マシンがそれぞれ 4 個のコアを持つ Standard_A4_v2 である場合は、この使用量をカバーするために、2 x 4 x 2 = 16 コアが必要です。 ■ 仮想マシンがそれぞれ 8 コアの仮想マシン サイズである場合は、その使用量をカバーするために、2 x 8 x 2 = 32 コアが必要です。 **両方のタイプのゲートウェイを持つポッドの場合** このゲートウェイには 4 台の Unified Access Gateway 仮想マシンがあるため、4 台の仮想マシンにそれぞれのコア数を掛けます。設定するには、割り当ては既存の (Blue) Unified Access Gateway 仮想マシンのコア数の 4 倍に加えて、パ

仮想マシン タイプとそのコア	説明	Green 仮想マシンへの切り替えが完了するまで、Blue 仮想マシンと Green 仮想マシンを実行するために必要な割り当ての合計
		ラレルの Green の Unified Access Gateway 仮想マシン用にさらに 2 倍のコアを許容できる必要があります。 ■ たとえば、仮想マシンがそれぞれ 4 個のコアを持つ Standard_A4_v2 である場合は、この使用量をカバーするために、4 x 4 x 2 = 32 コアが必要です。 ■ 仮想マシンがそれぞれ 8 コアの仮想マシン サイズである場合は、その使用量をカバーするために、4 x 8 x 2 = 64 コアが必要です。

Horizon Cloud ポッドの更新：エージェントの互換性とサポートを継続するための手順

この記事では、ポッドのイメージ、ファーム、および VDI デスクトップにインストールされているエージェントとポッドのマニフェスト バージョンとの互換性を維持することの重要性と、エージェントに関連する互換性の問題を回避するために実行する必要がある修正方法について説明します。

ポッドの更新を開始する前に、コンソールのすべての青いドット インジケータが消えるまでエージェントを更新する必要があります。ポッドの更新後、コンソールで青いドット インジケータが表示された場合は、それらのエージェントを再度更新する必要があります。

ヒント: この場合は、ポッドの更新前とポッドの更新後に、コンソールに表示される青いドット インジケータをすべて取り除くことが目的となります。

お客様の責任

『Horizon Service Description PDF』で説明されているように、イメージと割り当て仮想マシンの管理およびパッチ適用を継続的に最新のアップデートで行う必要があります。ポッドのイメージ、ファーム、およびデスクトップ割り当て内のエージェントをポッドのバージョンと互換性のある最新のエージェントのバージョンに確実に更新しない場合、ポッドはサポートされていない構成になります。

そのため、ポッドの更新を開始する前に、エージェントを最新バージョンのエージェントに更新する必要があります。また、ポッドの更新が完了した後、コンソールに青いドット インジケータが戻っていないことを確認する必要があります。コンソールのディスプレイに青いドット インジケータが返された場合は、表示された項目のエージェントを再度更新する必要があります。

ポッドの更新のスケジューリングされたメンテナンスの実施前と完了後にすべての青いドットをクリアする

コンソールで、イメージ仮想マシン、ファーム、および VDI デスクトップ割り当てのセットを調べます。青いドットのインジケータが表示されていますか。コンソールには、エージェントが最新ではないイメージおよび専用 VDI デスクトップ割り当ての横に青いドット インジケータが表示されます。この場合は、ポッドが新しいマニフェスト バージョンに更新される前に、すべての青いドットインジケータをクリアすることが目的となります。

次のスクリーンショットは、対象となる青いドットのタイプを示しています。

ポッドの更新が始まる前に、エージェントの更新手順を実行してすべての青いドットをクリアする

青いドットがゼロになるまでエージェントの更新ワークフローを実行します。コンソールでは、ファームの詳細ページと VDI デスクトップ割り当ての詳細ページにある仮想マシンのすべてのリストを調べて、最高の互換エージェント バージョンを使用していることを確認できます。次の各トピックに記載されているすべての手順に従います。

- 青いドットがあるイメージで、[エージェントのアップデート]を実行します。イメージを更新するための具体的な手順については、Horizon Cloud の RDSH イメージのエージェント ソフトウェアをアップデートする、専用 VDI デスクトップ割り当てによって使用されるイメージのエージェント ソフトウェアを更新するおよびフローティング VDI デスクトップ割り当てによって使用されるイメージのエージェント ソフトウェアを更新するを参照してください。
- ファームおよび VDI デスクトップ割り当てを [編集] して、現在のイメージではなく、更新されたイメージを使用します。この手順では、すべてのファーム、フローティング VDI デスクトップ仮想マシン、および未割り当ての専用 VDI デスクトップ仮想マシンを更新し、新しいエージェント バージョンのイメージを使用します。
- 専用 VDI デスクトップ割り当てで、[エージェントのアップデート] を実行して、割り当てられた専用 VDI デスクトップ仮想マシンを新しいエージェント バージョンに更新します。専用 VDI デスクトップ割り当ての [割り当て] ページでエージェント ソフトウェアを更新するを参照してください。

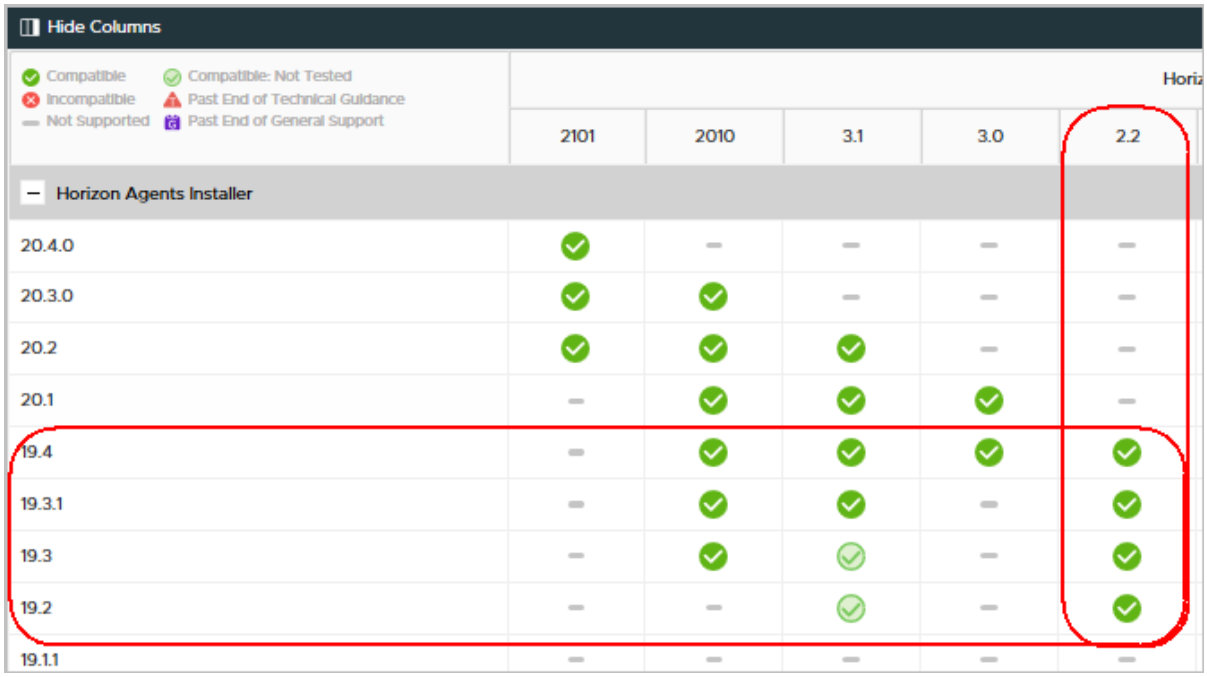
これらの手順を完了した後、ファーム仮想マシン、フローティング VDI デスクトップ割り当てのデスクトップ仮想マシン、および専用 VDI デスクトップ割り当ての割り当てられていないデスクトップ仮想マシンはすべて更新され、互換性のある最も新しいエージェント バージョンを実行しているはずです。コンソールでは、ファームの詳細ページと VDI デスクトップ割り当ての詳細ページにある仮想マシンのすべてのリストを調べて確認できます。

ポッドの更新が完了したら、青いドットがあるか確認します。次に、エージェントの更新手順を実行してすべての青いドットをクリアします

ポッドの更新前に青いドット インジケータをクリアしたのに、ポッドの更新後に青いドット インジケータがコンソールに戻るのはなぜですか? 新しいポッド マニフェストの登場時に、新しいエージェント バージョンも登場するためです。ポッド マニフェストとエージェント バージョンのこの組み合わせは、サポートされているポッド エージェント構成に使用されます。

ただし、既存のポッドをその新しいポッド マニフェスト レベルに引き上げるポッド更新プロセスは、そのポッドの既存のイメージ仮想マシン、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すでにインストールされているエージェントには影響しません。これらのエージェントは、以前にインストールされたバージョンに引き続き存在しますが、そのバージョンは、そのポッド マニフェストと互換性がない場合があります。ファーム仮想マシンとデスクトップ仮想マシンが過去に作成されたバージョンに戻り、ポッドを更新するとポッドがポッドエージェント バージョンの互換性マトリックスを超えるバージョンに移動する場合、ポッドはサポートされていない構成になります。

以下に一例を示します。次のスクリーンショットは、サービスの 2.2 バージョン中にデプロイされたポッドがサービスの 2101 バージョンに更新された場合の例を示しています。そのポッドのデフォルトの最新バージョンであるエージェント バージョン 19.4 は、そのポッドがサービスの 2101 バージョンに更新される際に互換性のない状態（灰色のボックス）になります。



特定のポッド マニフェストで利用可能な最新のエージェント バージョンを特定する方法

ポッド マネージャは、ポッドごとに、イメージ仮想マシン、ファーム仮想マシン、VDI デスクトップ仮想マシン、およびインポートされた仮想マシン（インポートされた仮想マシンでエージェント ペアリング アクションが実行された場合）にインストールされているエージェントとペアリングを行います。このペアリングは、ポッド マネージャとそれらの仮想マシンの間で必要とされる安全な通信の基盤を提供します。エージェントの新しいバージョンは、ポッド マネージャ ソフトウェアの新しいバージョン（マニフェスト）と同時にリリースされ、これらのバージョンは両方とも相互に互換性があります。同時に、ポッド マネージャ ソフトウェアの新しいバージョンはそれぞれ、以前のエージェント バージョンのいくつかと下位互換性を維持することを目的としています。これは、新しいポッド マネージャ ソフトウェアは、特定の時点までの古いエージェントとの通信と相互運用を継続できるということです。新しいポッド マネージャ ソフトウェアと古いエージェントの間の差が大きすぎると、ポッド マネージャとそれらのエージェント間の通信と相互運用性が停止します。

1 つのポッドで、特定のエージェント バージョンと特定のポッド マニフェストとの相互運用性を判断するには、複数のスポットからの各種の情報、すなわちポッド マニフェスト バージョン、そのポッド マニフェスト バージョンがデビューした VMware Horizon Cloud Service on Microsoft Azure という名前の製品のバージョン、および Horizon Agent Installer (HAI) のバージョンを関連付ける必要があります。エージェント ソフトウェアは、HAI ソフトウェアによって、ポッドのインポートされた仮想マシン、イメージ仮想マシン、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インストールされます。

1 まず、[キャパシティ] ページまたはポッドの詳細ページを使用して、ポッドのマニフェスト バージョンを取得します。

2 次に、『Horizon Cloud リリース ノート』を開き、そのマニフェスト バージョンのページ検索を実行して、そのマニフェストがデビューした「新機能」の日付を見つけます。

3 同じ「新機能」の場所で、製品名 VMware Horizon Cloud Service on Microsoft Azure の後に表示されているバージョン番号（2201 など）を見つけます。

4 次に、https://interopmatrix.vmware.com/#/Interoperability の「VMware 製品の相互運用性マトリックス」ページに移動し、Horizon Cloud Service on Microsoft Azure と Horizon Agents Installer の比較を選択します。

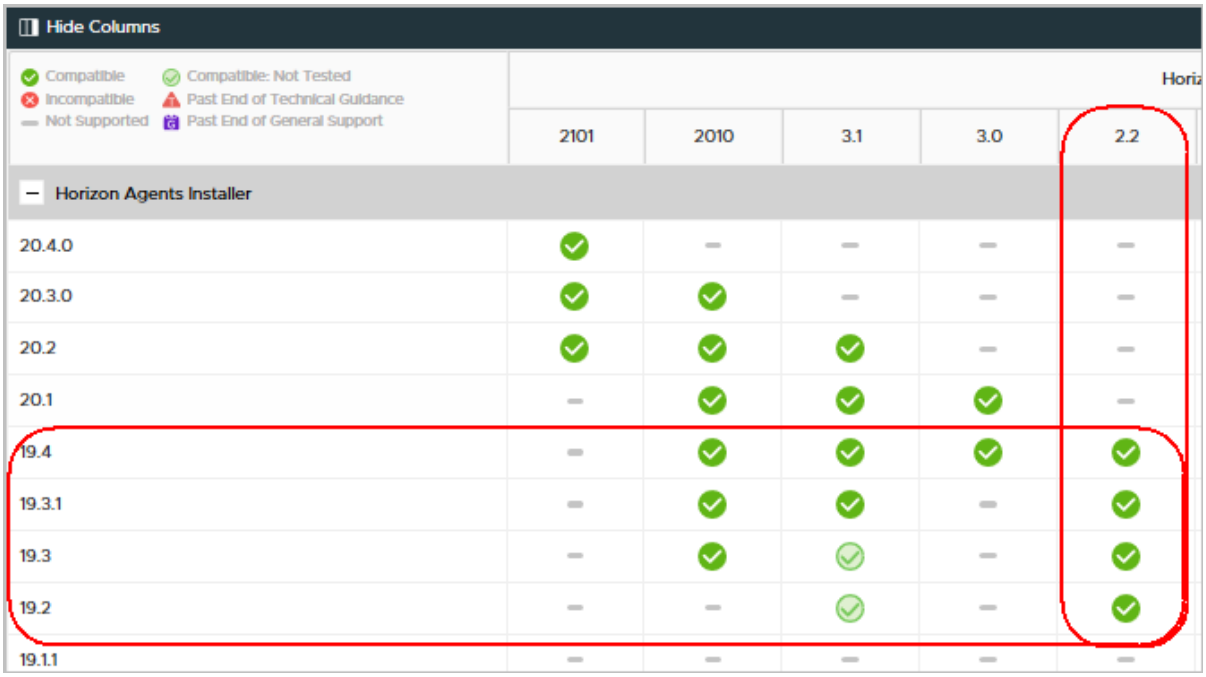
- [比較] セクションには Horizon Cloud Service on Microsoft Azure。
- [比較対象] セクションには Horizon Agents Installer。

マトリックス上のポッド マニフェストとエージェント バージョンの組み合わせが緑色のドットの外側にある場合、それらのエージェント バージョンを実行しているポッド内の仮想マシンで予期しない問題が発生する可能性が高くなります。

例

マニフェスト 1763.x を実行しているポッドがあるとします。リリース ノートによると、最初の 1763.0 マニフェストは VMware Horizon Cloud Service on Microsoft Azure 2.2 でデビューしました。マトリックスは、ポッドがデビューしたエージェント バージョン (19.4) およびそれ以前のエージェント バージョン 19.3.1、19.3、および 19.2 と相互運用することを示しています。リリース ノートの 2019 年 12 月 13 日の新機能によれば、HAI バージョン 19.4 が VMware Horizon Cloud Service on Microsoft Azure 2.2 リリースと同時にデビューしたことがわかります。この例では、1763.x ポッドが操作できる最も古いエージェントは 19.2 エージェントです。最も新しいエージェントは 19.4 エージェントです。1763.x を実行しているポッドを更新する前に、ベスト プラクティスとして、イメージ仮想マシン、ファーム仮想マシン、および VDI デスクトップ仮想マシンのエージェントが、その列に示されている最も新しいエージェント バージョンに更新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、前の段落と 2021 年 2 月 23 日の互換性マトリックスを示しています。



Horizon Cloud on Microsoft Azure デプロイのバックアップとリストア

Horizon Cloud on Microsoft Azure デプロイで失敗のシナリオが発生した場合、サービスはデータを失うことなくデプロイをリストアするための機能を提供します。

Horizon Cloud on Microsoft Azure デプロイのリストアを要求するには、VMware 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。

概要

ユーザー データは、デプロイの Azure Database for PostgreSQL データベースに保存されます。Microsoft Azure PostgreSQL データベースは、Microsoft Azure のマネージド サービスです。

サービス リリース v2111 およびポッド マニフェスト 3139.x 以降、デプロイがその PostgreSQL データベースに接続するために必要な構成情報は、クラウド プレーンに保存されます。

したがって、Horizon Cloud on Microsoft Azure のデプロイのリストアでは、PostgreSQL データベースに接続し、データベースに保存されているユーザー データを取得し、そのデータを使用して再デプロイされた仮想マシンを構成します。そのデータを使用して、デプロイは失敗のシナリオが発生する直前の動作状態にリストアされます。

技術的な詳細

以前は、ポッド デプロイヤはパターン `vmw-hcs-podID-recovery` の名前でリソース グループを作成していました。このリソース グループには、バックアップおよびリストア サービスに関連するストレージ アカウントがありました。

現在のリストア プロセスの実装では、サービスはこのタイプのリソース グループにデータを保持することに依存しません。リストア操作では、デプロイの Azure PostgreSQL データベースに保存されているデータが使用されます。

サービスがマニフェスト 3139.x 以降のリソース グループに依存していない場合、3139.x より前のデプロイへの更新がスケジュール設定され、その Green のビルドアウトが作成されると、既存の `vmw-hcs-podID-recovery` リソース グループはその時点で削除されます。

リストア プロセスでは、Azure PostgreSQL データベースからユーザー データが取得され、再デプロイされた仮想マシンを構成してデプロイを最新の動作状態にリストアするために使用されます。

失敗のシナリオが発生した場合

VMware 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 (SR) を発行し、デプロイのリストア プロセスを開始します。

VMware サポート チームは、このサービス全体の提供の一環として、手順についてアドバイスします。

Horizon Cloud ポッドの NTP 設定を変更する

ポッドの詳細ページで [編集] アクションを使用して、Microsoft Azure にデプロイされたポッドの NTP 設定を変更することができます。

手順

1 コンソールで [設定] - [キャパシティ] に移動し、ポッドの名前をクリックしてその詳細ページを開きます。

2 ポッドの詳細ページで、[編集] をクリックします。

3 [ポッドの編集] ウィンドウで、[NTP サーバ] フィールドの設定を編集します。

4 [保存と終了] をクリックして新しい設定をシステムに保存します。

コネクタがポッド マネージャ仮想マシンへの接続を信頼できるように、Workspace ONE Access コネクタ アプライアンスを Microsoft Azure の Horizon Cloud ポッドと統合する場合には、ポッド マネージャ仮想マシンで SSL 証明書を直接構成します。

このワークフローは、シナリオで、シングルポッド仲介を使用して Horizon Cloud 環境のポッドと Workspace ONE Access Connector アプライアンスを統合する場合に使用します。Horizon Cloud 環境がシングルポッド仲介用に構成されていて、Microsoft Azure のポッドを Workspace ONE Access と統合する場合は、ポッド自体を参照するように Workspace ONE Access Connector アプライアンスを構成します。これにより、アプライアンスがポッドからユーザー資格を同期できるようになります。このワークフローは主にこのタイプの統合のために使用され、それによって Workspace ONE Access Connector はポッド マネージャ仮想マシンへの SSL 接続

を信頼します。まれなシナリオとして、一部の組織でポッド マネージャ仮想マシンに SSL 証明書を直接配置することが必要になる場合がありますが、そのような状況は一般的ではなく、ほとんどの組織では発生しません。

重要： ポッドと統合する Workspace ONE Access Connector がデプロイに含まれておらず、エンド ユーザーによってクライアントとブラウザがポッドのゲートウェイ構成用の FQDN を参照している場合、これらの手順はそのシナリオに適用されません。そのシナリオでは、Microsoft Azure の Horizon Cloud ポッドで、ゲートウェイの SSL 証明書を新しいバージョンに置き換える（新しい有効期限や別の FQDN を使用するなど）。以下の手順を実行しても、ゲートウェイ構成上の SSL 証明書は変更されません。ユースケースに、1 つ以上のポッドのゲートウェイ構成で構成されている SSL 証明書の置き換えが含まれる場合は、代わりに Microsoft Azure の Horizon Cloud ポッドで、ゲートウェイの SSL 証明書を新しいバージョンに置き換える（新しい有効期限や別の FQDN を使用するなど）を参照してください。ポッドの詳細ページのゲートウェイ関連のセクションに表示される FQDN 情報を調べて、クライアントまたはブラウザがゲートウェイ関連の FQDN を参照するようにエンド ユーザーに指示したかどうかを確認できます。

シングルポッドまたはポッド単位の仲介を使用するように環境が構成されている場合、Workspace ONE Access Connector は、それらのアプライアンスの前にある Microsoft Azure ロード バランサを介してポッド マネージャ仮想マシンと通信します。この通信を行うには、Workspace ONE Access Connector がポッド マネージャ仮想マシンへの SSL 接続を信頼できるようにする必要があります。これらのポッド マネージャ仮想マシンに SSL 証明書を配置することで、その信頼された通信が可能になります。

ポッド マネージャ仮想マシンが SSL 証明書を使用して構成されるシナリオについては、Horizon Cloud ポッドのマネージャ仮想マシンでの SSL 証明書の構成の概要（主にシングルポッド ブローカ環境でポッドを使用する Workspace ONE Access Connector で使用）。主なユースケースは、環境がシングルポッド仲介用に構成されていて、ポッドを Workspace ONE Access Connector と統合して、エンド ユーザーが 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アクセスできるようにする場合です。統合ワークフローについては、シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure の環境の Horizon Cloud ポッドと Workspace ONE Access の統合を参照してください。

注： 以下の手順で [保存] をクリックすると Horizon Cloud はこれらの証明書ファイルを使用して仮想マシンに証明書を構成します。このアクティビティの所要時間は 1 分未満です。

以下の手順は Horizon Universal Console で実行されます。

前提条件

このワークフローを開始する前に、Horizon Universal Console コンソールの [ポッド証明書のアップロード] ワークフローを実行して、Horizon Cloud ポッドのマネージャ仮想マシンで SSL 証明書を構成するための前提条件に記載されている必要事項を満たしていることを確認します。特に、コンソールのワークフローで必要な 3 つの証明書ファイルがあり、そのリンク ページに記載されている基準を満たしていることを確認します。

注目: これらの証明書に SHA-1 ハッシュ関数を使用することはサポートされていません。

注意: 不正なまたは不適切な形式の SSL 証明書ファイルをアップロードしてポッドに保存すると、ポッドへのアクセスが失われる可能性があります。ポッドマニフェストが 3139.x より低い場合は、手順を実行する前に VMware サポートに連絡してガイダンスを確認してください。サービスの「Horizon Cloud on Microsoft Azure デプロイのバックアップとリストア」には 3139.x 以降のマニフェストが必要であるため、[ポッド証明書のアップロード] ワークフローを実行する前に、ポッド マニフェストが 3139.x 未満の場合は、VMware のサポートまでお問い合わせください。

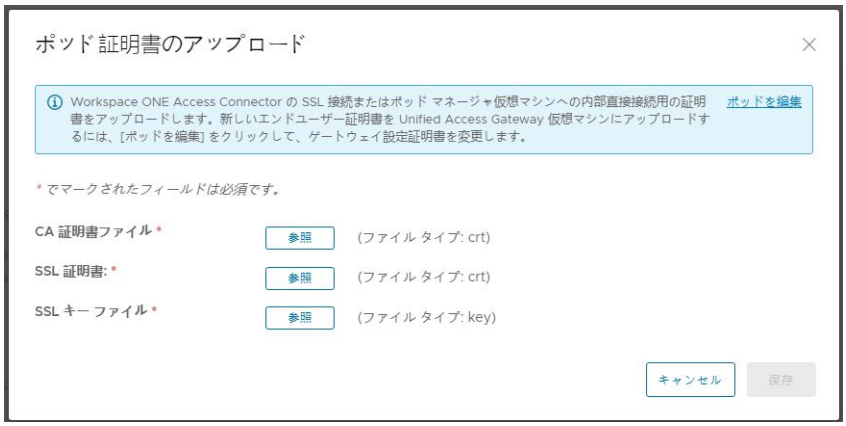
手順

1 [設定] - [キャパシティ] を選択します。

2 ポッドの名前をクリックしてポッドの [サマリ] ページを開きます。

3 [...] - [ポッド証明書のアップロード] の順にクリックします。

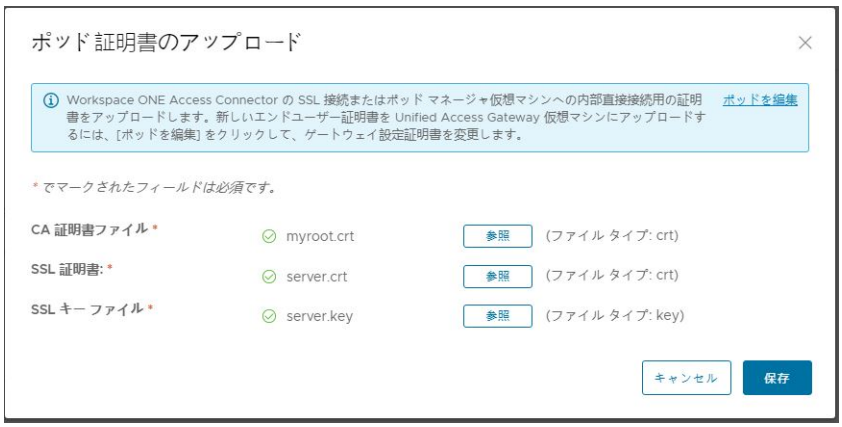
[ポッド証明書のアップロード] ウィンドウが開きます。次のスクリーンショットは、ウィンドウの例です。



4 [ポッド証明書のアップロード] ウィンドウに表示される各証明書ファイルについて、[選択] をクリックして、アップロード可能なファイルの場所に移動します。

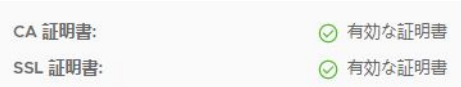
5 すべての証明書ファイルがリストされていることが表示されたら、[保存] をクリックします。

次のスクリーンショットは、システムに保存する前のすべての証明書ファイルが一覧表示されているウィンドウを示します。



結果

Horizon Cloud は、証明書ファイルを使用して、SSL 証明書をポッドのマネージャ仮想マシンに構成します。このアクティビティには数秒間かかります。ポッドの [サマリ] ページでステータスを確認できます。



Horizon Cloud ポッドのマネージャ仮想マシンでの SSL 証明書の構成の概要（主にシングル ポッド ブローカ環境でポッドを使用する Workspace ONE Access Connector で使用）

シングルポッド仲介タイプ用に構成された本番環境システムでは、Horizon Cloud ポッドのマネージャ仮想マシンで SSL 証明書を構成する場合の主な使用事例は、Workspace ONE Access をポッドに統合することです。Workspace ONE Access Connector は、ポッドのマネージャ仮想マシンへの SSL 接続を信頼できる必要があります。これにより、これらのポッドと Workspace ONE Access の統合が機能します。Workspace ONE Access Connector と統合するこの特定の使用事例では、ポッドは SSL 証明書をポッドのマネージャ仮想マシンに直接設定する必要があります。

ご利用のポッドがシングルポッド仲介環境にある場合、Microsoft Azure の Horizon Cloud ポッドと Workspace ONE Access との統合で重要となるのは、ポッドをプロビジョニングしたデスクトップおよびリモート アプリケーションを使用するために Workspace ONE Access で設定した Horizon Cloud 仮想アプリケーションのコレクションを同期させるよう、Workspace ONE Access Connector を構成することです。この同期を実行するには、Workspace ONE Access Connector がポッド マネージャ仮想マシンと通信する必要があります。したがって、ポッドは有効な SSL 証明書を提示して、Workspace ONE Access Connector がその証明書を信頼するようにする必要があります。この統合の詳細については、シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure の環境の Horizon Cloud ポッドと Workspace ONE Access の統合を参照してください。

ポッドの詳細ページの [ポッド マネージャのロード バランサの IP アドレス] フィールドと Workspace ONE Access Connector の SSL 証明書の要件との関係

ポッドの詳細ページの [ポッド マネージャのロード バランサの IP アドレス] ラベルの横に表示される数値の IP アドレスは、ポッド マネージャ仮想マシンで構成可能である、有効な信頼された SSL 証明書を作成するために必要な情報の重要部分です。次のスクリーンショットは、デプロイされたポッドの詳細ページで [ポッド マネージャのロード バランサの IP アドレス] ラベルが表示される場所を示しています。

信頼された SSL 証明書は、そのフィールドに表示される IP アドレスに DNS サーバ内でマッピングする完全修飾ドメイン名 (FQDN) に基づいている必要があります。このマッピングは、その FQDN を使用するように構成されたエンド ユーザーのクライアントがポッドへの信頼された接続を確立できるようにするために必要です。

それでは、その数値の IP アドレスに関連付けられるものは何でしょうか? これはポッドのテナント サブネットからのプライベート IP アドレスであり、ポッドのポッド マネージャ仮想マシンの Azure ロード バランサに関連付けられます。

ポッド マネージャのロード バランサの IP アドレスについて

現在サポートされているすべてのポッド マニフェストの場合、[ポッド マネージャのロード バランサの IP アドレス] ラベルに表示される数値の IP アドレスは、ポッドの Azure ロード バランサ リソースの、数値のプライベート IP アドレスです。ポッド アーキテクチャには、ポッドのテナント サブネットからのプライベート IP アドレスを持つ、ポッドの Azure ロード バランサが含まれています。そのポッドの Azure ロード バランサは、その Azure ロード バランサの背後に存在するポッド マネージャ仮想マシンに対する SSL 通信のポイントとなります。

高可用性が有効なポッドの場合、管理コンソールで [証明書をアップロード] をクリックして SSL 証明書ファイルをアップロードすると、Horizon Cloud はアクティブなポッド マネージャ仮想マシンで構成を実行してから、証明書の構成を他のポッド マネージャ仮想マシンにコピーします。

高可用性が有効になっていないポッドの場合（典型的ではないケース）、そのポッドには Azure ロード バランサの背後に単一のポッド マネージャ仮想マシンがあります。この場合、コンソールで [証明書をアップロード] をクリックすると、Horizon Cloud はそのポッド マネージャ仮想マシンで証明書を構成します。

次のスクリーンショットは、ポッドの Azure ロード バランサのプライベート IP アドレスが、上記の例のコンソールのポッドの詳細ページに表示される [ポッド マネージャのロード バランサの IP アドレス] ラベルの横に表示される IP アドレスと同じであることを示しています。

ポッドのマネージャ仮想マシンでの SSL 証明書の構成方法

管理コンソールを使用して、ポッド マネージャ仮想マシンに SSL 証明書を構成します。詳細な手順については、コネクタがポッド マネージャ仮想マシンへの接続を信頼できるように、Workspace ONE Access コネクタ アプライアンスを Microsoft Azure の Horizon Cloud ポッドと統合する場合には、ポッド マネージャ仮想マシンで SSL 証明書を直接構成します。を参照してください。これらの手順を実行する際の前提条件については、Horizon Universal Console コンソールの [ポッド証明書のアップロード] ワークフローを実行して、Horizon Cloud ポッドのマネージャ仮想マシンで SSL 証明書を構成するための前提条件を参照してください。

ポッドのマネージャ仮想マシンで構成された SSL 証明書が必要となる一般的なシナリオ

これらのシナリオは、事前検証に適している場合がありますが、本番環境では使用しないことを推奨します。本番環境システムでは、ポッドによってプロビジョニングされたリソースへのエンドユーザー接続をサポートする、内部および外部ゲートウェイ構成の Horizon Cloud の機能を活用する必要があります。VPN 経由など、企業のネットワーク内でのエンドユーザー接続の場合は、ポッドに内部 Unified Access Gateway 構成を設定する必要があります。インターネット経由のエンドユーザー接続の場合は、ポッドに外部 Unified Access Gateway 構成を設定する必要があります。これらの構成をポッドに追加する手順については、デプロイ済みの Horizon Cloud ポッドへのゲートウェイ構成の追加を参照してください。

表 6-6. ポッド マネージャ仮想マシンで構成された SSL 証明書が必要となる一般的なシナリオ

シナリオ	説明
外部ゲートウェイ構成のみでデプロイされたポッドで、内部 Unified Access Gateway 構成がない	このシナリオでは、インターネット経由のエンド ユーザーは、デプロイされた外部ゲートウェイ構成を介してポッドによってプロビジョニングされたリソースに到達しますが、企業のネットワークの内部ユーザーは、同様の内部ゲートウェイ構成がないため、ポッドによってプロビジョニングされたリソースに到達するために使用できる手段がありません。内部 Unified Access Gateway 構成がない場合、内部ユーザーは、クライアント接続がポッドに直接到達するようにポイントする必要があります。ポッドに直接アクセスするには、ポッドの詳細ページの [ポッド マネージャのロード バランサの IP アドレス] ラベルの横に表示されている IP アドレスに対して、またはその表示されている IP アドレスに DNS 内でマッピングする FQDN に対して、クライアントをポイントすることになります。
ゲートウェイ構成なしでデプロイされるポッド（Unified Access Gateway 仮想マシンがゼロ）	このシナリオでは、ポッドによってプロビジョニングされたリソースへのすべてのエンドユーザー接続で、オペレーティング システム固有の Horizon Clients のいずれかを使用してポッドに直接アクセスする必要があります。ポッドに直接アクセスするには、ポッドの詳細ページの [ポッド マネージャのロード バランサの IP アドレス] ラベルの横に表示されている IP アドレスに対して、またはその表示されている IP アドレスに DNS 内でマッピングする FQDN に対して、クライアントをポイントすることになります。 **注目:** オペレーティング システム固有の Horizon Clients の 1 つを使用する場合とは異なり、ブラウザをポッドに直接ポイントすると、コンソールで [証明書のアップロード] アクションを使用してポッドのマネージャ仮想マシンでの SSL 証明書を構成した場合でも、そのブラウザ接続は信頼されていない接続として動作します。ポッドの FQDN をブラウザに直接入力すると、ブラウザは HTML Access (Blast) 接続タイプを使用して接続し、また、HTML Access (Blast) の動作により、ブラウザはポッドへの接続を直接行うときに、一般的な信頼されない証明書のエラーが表示されます。信頼されていない証明書のエラーが表示されるのを回避するには、ポッドにゲートウェイを構成し、それらのブラウザ接続が適切なゲートウェイ構成を通過できるようにする必要があります。すなわち、企業ネットワークの外側のエンド ユーザーの場合は外部ゲートウェイ構成、企業ネットワークの内側のエンド ユーザーの場合は内部ゲートウェイ構成です。FQDN をインターネットに公開したくない場合は、内部ゲートウェイ構成を使用します。内部ゲートウェイ構成では、企業のネットワーク内にいるエンド ユーザーが接続できる Microsoft 内部ロード バランサを使用します。デプロイ済みの Horizon Cloud ポッドへのゲートウェイ構成の追加を参照してください。

Horizon Universal Console コンソールの [ポッド証明書のアップロード] ワークフローを実行して、Horizon Cloud ポッドのマネージャ仮想マシンで SSL 証明書を構成するための前提条件

[ポッド証明書のアップロード] ワークフローを実行する前に、これらの前提条件を満たしていることを確認します。[ポッド証明書のアップロード] ウィンドウの条件を満たし、ワークフローを正常に完了するには、以下で説明する証明書関連のファイルが必要です。

注目: これらの証明書に SHA-1 ハッシュ関数を使用することはサポートされていません。

DNS サーバ

DNS サーバで、完全修飾ドメイン名 (FQDN) を、ポッドの詳細ページに表示され、[ポッド マネージャ ロード バランサの IP アドレス] とラベル付けされた IP アドレスにマッピングします。[キャパシティ] ページからポッド名をクリックすると、ポッドの詳細ページに移動できます。

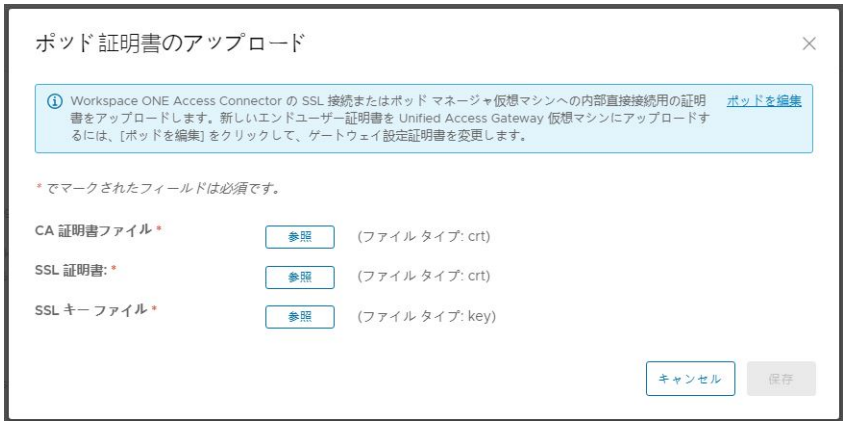
[ポッド マネージャ ロード バランサの IP アドレス] ラベルの横に表示される IP アドレスの意味については、Horizon Cloud ポッドのマネージャ仮想マシンでの SSL 証明書の構成の概要（主にシングルポッド ブローカ環境でポッドを使用する Workspace ONE Access Connector で使用）を参照してください。

この FQDN は、次のセクションで説明するように SSL 証明書ファイルを取得するときに使用します。

SSL 証明書ファイル

コンソールの [ポッド証明書のアップロード] ウィンドウでは、3 つの異なる相互関連ファイルを指定する必要があります。

次のスクリーンショットは、3 つのファイルを指定する [ポッド証明書のアップロード] ウィンドウがどのように表示されるかを示しています。



次のリストでは、上記のように、コンソール ウィンドウで使用されるラベルに関連するファイルについて説明します。

CA 証明書ファイル (CA.crt)

この `CA.crt` ファイルは、認証局 (CA) によって発行されます。このファイルは、以下で説明する他の 2 つのファイルの信頼性を確認するために使用されます。

SSL 証明書ファイル (SSL.crt)

このファイルは、RSA 暗号化アルゴリズムを使用したデータの暗号化に使用されるパブリック キー ファイルです。ポッド マネージャ インスタンスは、シングルポッド ブローカとポッド マネージャと通信する Workspace ONE Access コネクタを使用するシナリオで、この SSL.crt ファイルを使用してポッド マネージャ インスタンスによって送信されるデータを暗号化します。(このユースケースについては、「Horizon Cloud ポッドのマネージャ仮想マシンでの SSL 証明書の構成の概要 (主にシングルポッド ブローカ環境でポッドを使用する Workspace ONE Access Connector で使用)」ページで説明します。)

SSL キー ファイル (.key)

このファイルは、RSA 暗号化アルゴリズムを使用して、上記の `SSL.crt` パブリック キー ファイルによって暗号化されたデータの復号化に使用されるプライベート キー ファイルです。

ファイル要件

ファイルが次の要件を満たしていることを確認します。

- 有効な信頼された SSL 証明書は、DNS サーバでポッド マネージャのロード バランサ IP アドレスにマッピングした FQDN に基づいています。
- このアップロードの CA 証明書ファイル (`CA.crt`) と SSL 証明書ファイル (`SSL.crt`) は PEM 形式です。PEM 形式とは X.509 証明書を BASE64 でエンコードした DER 表現です。どちらも `.crt` 拡張子を持つ必要があります。

  次のブロックは、ファイルの内容がどのように表示されるかの例です。

  ```
  -----BEGIN CERTIFICATE-----
  MIIFejCCA2KgAwIBAgIDAIi/MA0GCSqG
  ..............
  -----END CERTIFICATE-----
  ```

- プライベート キー ファイル (`.key`) にパスワードまたはパスフレーズが関連付けられていないことを確認します。次のブロックは、ファイルの内容がどのように表示されるかの例です。

  ```
  -----BEGIN RSA PRIVATE KEY -----
  MIIEpQIBAAKCAQEAoJmURboiFut+R34CNFibb9fjtI+cpDarUzqe8oGKFzEE/jmj
  ....................
  -----END RSA PRIVATE KEY-----
  ```

- 証明書ファイルは、SHA-1 より新しいハッシュ関数を使用する必要があります。ポッド マネージャ インスタンスでの SHA-1 証明書の使用はサポートされていません。
- CA 証明書ファイルに関連する特別な考慮事項の次のセクションを確認し、CA 証明書ファイルがチェーンルート CA タイプの場合は、説明されている要件が満たされていることを確認します。

CA 証明書ファイル - 特別な考慮事項

CA 証明書ファイルは、信頼できる認証局 (CA) によって発行されている必要があります。

その結果、`CA.crt` ファイルの生成は、使用する CA によって異なります。たとえば、一般的な CA には、DigiCert、Verisign、Google などがあります。

使用する CA によっては、次のいずれかのタイプが提供される場合があります。

単一ルート CA 証明書

このタイプでは、CA は証明書に直接署名します。

チェーンルート CA 証明書

このタイプでは、ルート認証局と一緒に 1 つ以上のサードパーティの修正認証局が関与します。

CA 証明書ファイルに 1 つ以上の中間証明書認証局が含まれている場合は、`CA.crt` ファイルに中間証明書とルート CA が含まれている必要があります。ファイルは、先頭の中間証明書で始まり、ファイルの下部にルート証明書が含まれている必要があります。

次の手順

ポッドのマネージャ仮想マシンで SSL 証明書を構成する手順については、コネクタがポッド マネージャ仮想マシンへの接続を信頼できるように、Workspace ONE Access コネクタ アプライアンスを Microsoft Azure の Horizon Cloud ポッドと統合する場合には、ポッド マネージャ仮想マシンで SSL 証明書を直接構成します。を参照してください。

ポッドマニフェストが 3139.x より低い場合は、手順を実行する前に VMware サポートに連絡してガイダンスを確認してください。不正なまたは不適切な形式の SSL 証明書ファイルをアップロードしてポッドに保存すると、ポッドへのアクセスが失われる可能性があり、サービスの「Horizon Cloud on Microsoft Azure デプロイのバックアップとリストア」には 3139.x 以降のマニフェストが必要であるため、ポッド証明書のアップロード ワークフローを実行する前に、ポッド マニフェストが 3139.x 未満の場合は、VMware のサポートまでお問い合わせください。

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 デプロイヤを機能させるには、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 6-7. 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 デプロイヤは、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 `d1mes20qfad06k.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 6-8. 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	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。 ■ 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	地域別制御プレーンのインスタンス ■ 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.horizo

表 6-8. 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.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.h

表 6-8. 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
					orizon.vmware.com ■ ドイツ：cloud-de.horizon.vmware.com
管理	softwareupdate.vmware.com	443	TCP	はい	VMware ソフトウェア パッケージ サーバ。システムのイメージに関連する操作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 6-8. 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 Gateway 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プ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 6-8. 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、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。	Microsoft ソフトウェア パッケージ サーバ。Microsoft 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 6-8. 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、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。	Ubuntu ソフトウェア パッケージ 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 6-8. 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 パッケージ サーバ。ポッド マネージャと Unified Access Gateway 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 6-8. 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 パッケージ サーバ。ポッド マネージャと Unified Access Gateway 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 6-8. 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 パッケージ サーバ。ポッド マネージャと Unified Access Gateway 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 6-8. 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 パッケージ サーバ。ポッド マネージャと Unified Access Gateway 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 サイトを使用してセキュリティ関連の Ubuntu 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 6-8. 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 パッケージ サーバ。ポッド マネージャと Unified Access Gateway 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 (Common Vulnerabilities and Exposu

表 6-8. 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 6-8. 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	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。 ■ 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	この Web アドレスは通常、アプリケーションによって Microsoft Azure サービスを認証するために使用されます。Microsoft 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 Directory v2.0 および OpenID Connect プロトコル」、および「National Clouds」を参照してください。「National Clouds」のトピックでは、

表 6-8. 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 Microsoft Azure National 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 6-8. 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	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。 ■ 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	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

表 6-8. 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。 ■ 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 Directory (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 Directory (Azure AD) へのポッドによるプログラムアクセスに使用されます。

表 6-8. 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	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。 ■ 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す。この名前は、*.postgres.database.azure.com のパターンに従います。	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 6-8. 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	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。 ■ 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	Universal Broker サービスのリージョン インスタンス ■ 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 6-8. 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
					warehorizon.com ■ 日本：connector-azure-jp.vmwarehorizon.com ■ 英国：connector-azure-uk.vmwarehorizon.com ■ ドイツ：connector-azure-de.vmwarehorizon.com

表 6-8. 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	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。 ■ 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 6-8. 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	■ *.blob.core.windows.net: ■ sauron-jp.horizon.vmware.com	443	TCP	いいえ	*.blob.core.windows.net 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 Microsoft Azure クラウド環境内の Microsoft 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 Microsoft Azure クラウド スペース内で直接行います。 sauron-jp.horizon.vmware.com エンドポイントを使用すると、VMwar

表 6-8. 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
					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。

表 6-8. 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。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 [Marketplace 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 ペアリング 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 6-8. 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 サーバ 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 Microso	App Volumes on Azure 機能に使用されます。ポッド マネージャのリ

表 6-8. 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、Microsoft 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 Volumes AppStack 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で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できる必要があります。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 インスペク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 インスペク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、その後に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 6-9. 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 6-9. 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ヤ ID）や `node` を含む名前が付けられます。

表 6-10. 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 6-11. 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	NTP サービス。NTP の時刻同期を提供するサーバ。 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。 ■ 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。 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。 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。 **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。
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	Blast Extreme デフォルトでは、Blast Extreme を使用する場合、クライアント ドライブ リダイレクト (CDR) トラフィックおよび USB トラフィックはこのポート内でサイド チャネルされます。好みに応じて、CDR トラフィックは TCP 9427 ポート上で、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。

表 6-11. 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 6-12. 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ヤ オプションを選択する場合

デプロイヤは、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. 高可用性が有効で、外部および内部の両方の Unified Access Gateway 構成を持つポッドの Horizon Cloud Pod アーキテクチャの図は、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 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. 高可用性が有効で、外部および内部の両方の Unified Access Gateway 構成を持つポッドの Horizon Cloud Pod アーキテクチャの図は、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 オプションを選択する場合

デプロイヤは、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す。この構成の場合、コネクタがポッド マネージャ仮想マシンへの接続を信頼できるように、Workspace ONE Access コネクタ アプライアンスを Microsoft Azure の Horizon Cloud ポッドと統合する場合には、ポッド マネージャ仮想マシンで SSL 証明書を直接構成します。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 6-13. 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 6-13. 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。デプロイでの設定内容によって異なる	TCP	Horizon Client からのデータ トラフィック用の Unified Access Gateway 上の Blast Secure Gateway 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。 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。 **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。
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 6-13. 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	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。
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。デプロイでの設定内容によって異なる	TCP	Horizon HTML Access クライアント（Web クライアント）からのデータ トラフィック用の Unified Access Gateway 上の Blast Secure Gateway 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、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。 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。 **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。

表 6-14. 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	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。シングルポッド ブローカ - Horizon Cloud ポッドと URL コンテンツ リダイレクト機能を参照してください。
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 6-14. 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。デプロイでの設定内容によって異なる	TCP	Horizon Client からのデータ トラフィック用の Unified Access Gateway 上の Blast Secure Gateway 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。 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。 **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。
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 6-14. 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	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。
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。デプロイでの設定内容によって異なる	TCP	Horizon HTML Access クライアント（Web クライアント）からのデータ トラフィック用の Unified Access Gateway 上の Blast Secure Gateway 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、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。 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。 **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。

表 6-15. 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 6-15. 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	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。 **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。
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 機能で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 6-16. 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 サブネットで、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 6-17. 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	■ 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 マネージャー仮想マシンとその Horizon Agent の間にすでに配置されている通信チャネルを介して、環境のアクティブなポッド マネージャー仮想マシンに 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 - Microsoft Azure にデプロイされた 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

このドキュメント トピックの目的は、第 1 世代の Horizon Cloud 環境を使用して Microsoft Azure サブスクリプションにポッドを作成し、続いて Microsoft Azure ポータルにログインしてポッド デプロイヤが何を作成しているかを確認したときに表示される内容を説明することです。Microsoft Azure へのポッドのデプロイの一環として、自動デプロイ プロセスは一連のネットワーク セキュリティ グループ (NSG) を作成し、それぞれを VMware によって制御されるポッド関連の各仮想マシンにある特定の個別のネットワーク インターフェイス (NIC) に関連付けます。このようなポッド関連の仮想マシンとは、ポッドのマネージャ仮想マシン、およびポッドが Unified Access Gateway で構成されるときにデプロイされる仮想マシンです。

このページを読む前に

このページを読む前に、以下の点を考慮してください。

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。

注： 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、廃止された機能に以前関連していたこのページの情報は、適宜更新されています。

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。

概要

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

ここで説明する NSG は、Horizon Universal Console を使用して作成するときにポッドによってプロビジョニングされるベース仮想マシン、ファーム、および VDI デスクトップに使用される NSG とは異なります。これらの NSG には、異なる使用情報があります。これらの NSG については、以下のトピックを参照してください。

- Horizon Cloud の [Marketplace からの仮想マシンのインポート] ウィザードによって作成されたネットワーク セキュリティ グループ (NSG)
- Horizon Cloud ポッド内のネットワーク セキュリティ グループとファームについて
- Horizon Cloud ポッド内のネットワーク セキュリティ グループと VDI デスクトップについて

注意: ここに記載されているデプロイヤで作成された NSG ルールは、サービスの構成要件です。自動的に作成され、ポッド仮想マシンの NIC に関連付けられている Horizon Cloud NSG を削除または編集しないでください。この指示には、次のようなアクションが含まれます。

- これらの NSG または NSG ルールを Horizon Cloud で使用されるサブネットにコピーまたは移動する
- これらの NSG または NSG ルールを、ポッド仮想マシンに関連付けられている NIC 間でコピーまたは移動する。

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

- クラウド制御プレーンがポッドと通信する機能。
- ポッドのインフラストラクチャの管理
- ポッドのライフサイクルの運用

これらのデプロイヤで作成された NSG はサービスの構成要件であるため、VMware Horizon Service のサービス レベル アグリーメントで説明されているように、それらを変更または移動しようとすると Horizon Cloud のサポートされていない使用および提供サービスの誤用と見なされます。

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

Microsoft Azure ドキュメントで説明するように、ネットワーク セキュリティ グループ (NSG) の目的は、セキュリティ ルールを使用して Microsoft Azure 環境のリソースとの間のネットワーク トラフィックをフィルタリングすることです。各ルールには、NSG が関連付けられているリソースに許可されるトラフィックを決定する、送信元、宛先、ポート、プロトコルなどの一連のプロパティがあります。Horizon Cloud が自動的に作成し、VMware によって制御されるポッドの仮想マシンの NIC と関連付ける NSG には、Horizon Cloud が、サービスのポッドの管理、進行中のポッド操作の正しい実行、およびポッドのライフサイクルの管理に必要と判断した特定のルールが含ま

れています。一般的に、これらの NSG で定義されている各ルールは、エンド ユーザーに仮想デスクトップを提供する VDI のユースケースなど、Horizon Cloud サブスクリプションの標準的なビジネス目的を実現するサービス フルフィルメントの一部であるポッド操作のポート トラフィックを提供することを目的としています。Horizon Cloud ポッドのポートとプロトコルの要件も参照してください。

以下のセクションでは、これらの NSG で Horizon Cloud が定義する NSG ルールが一覧表示されています。

これらの NSG に関する一般的な事実

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

- これらの VMware が作成した NSG は、VMware によって制御されるソフトウェア アプライアンスのセキュリティのためのものです。VMware がサブスクリプションに新しいソフトウェアを追加し、追加のルールが必要になると、それらの新しいルールがこれらの NSG に追加されます。
- Microsoft Azure ポータルでは、NSG の名前にパターン `vmw-hcs-podUUID` が含まれています。ここで *podUUID* はポッドの識別子です。ただし、専用の VNet にデプロイされる外部ゲートウェイ構成用の NSG は除きます。その場合、ゲートウェイに関連する NSG の名前にはパターン `vmw-hcs-ID` が含まれています。ここで *ID* はその外部ゲートウェイのデプロイ ID です。

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

  これらの ID は、管理コンソールの [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て見つけることができます。

  注： ポッドの外部 Unified Access Gateway でカスタム リソース グループを使用することを選択した場合、ゲートウェイ コネクタ仮想マシンのデプロイヤによって作成された NSG の名前には、パターン `vmw-hcs-ID` の代わりにそのカスタム リソース グループの名前が含まれます。たとえば、ポッドの外部ゲートウェイに `ourhcspodgateway` という名前のカスタム リソース グループを使用することを指定した場合、デプロイヤが作成してゲートウェイ仮想マシンの NIC に関連付ける NSG の名前は `ourhcspodgateway-mgmt-nsg` になります。
- NSG は、関連付けられている仮想マシンおよび NIC と同じリソース グループにあります。たとえば、外部ゲートウェイがポッドの VNet にデプロイされ、デプロイヤによって作成されたリソース グループを使用している場合、外部 Unified Access Gateway 仮想マシンの NIC に関連付けられている NSG は、`vmw-hcs-podUUID-uag` というリソース グループにあります。第 1 世代テナント - Microsoft Azure にデプロイされたポッド用に作成されたリソース グループも参照してください。
- Horizon Cloud では、サービスの保守性を維持するために、必要に応じて新しいルールが追加されたり、既存のルールが変更されたりすることがあります。
- ポッドの更新中、NSG とルールは保持されます。それらは削除されません。

- Horizon Cloud ルールは優先度 1000 から始まり、優先度は通常 100 単位で増えます。Horizon Cloud ルールは、優先度 3000 のルールで終了します。
- Microsoft Azure ドキュメントのトピック「IP アドレス 168.63.129.16 について」で説明するとおり、送信元 IP アドレス 168.63.129.16 に対する `AllowAzureInBound` ルールによって、NSG は Microsoft Azure プラットフォームからの受信通信を受け付けます。ポッドに関連するすべての仮想マシンは、Microsoft Azure の仮想マシンです。その Microsoft Azure ドキュメントのトピックで説明されているように、IP アドレス 168.63.129.16 は、Microsoft Azure クラウド プラットフォームがクラウド内のすべての仮想マシンに対して実行するさまざまな仮想マシン管理タスクを容易にします。例として、この IP アドレスを使用すると、仮想マシン内にある仮想マシン エージェントが Microsoft Azure プラットフォームと通信して、仮想マシンが準備完了状態にあることを簡単に通知できます。
- Unified Access Gateway インスタンスの NSG では、PCoIP トラフィックが 4173+ 範囲の可変ポート番号を使用しているため、`AllowPcoipUdpInBound` ルールがすべてのポートに設定され、トラフィックを特定のポートのセットに制限できません。
- Microsoft Azure は、各 NSG が作成されると自動的にいくつかのデフォルトのルールを作成します。作成されるすべての NSG で、Microsoft Azure はいくつかのインバウンド ルールとアウトバウンド ルールを 65000 以上の優先度で作成します。このような Microsoft Azure のデフォルトのルールは、Microsoft Azure によって自動的に作成されるため、このドキュメント トピックでは説明しません。これらのデフォルトのルールの詳細については、Microsoft Azure ドキュメントのデフォルトのセキュリティ ルールトピックを参照してください。
- これらの NSG で定義されている各ルールは、エンド ユーザーに仮想デスクトップを提供する VDI のユースケースなど、Horizon Cloud サブスクリプションの標準的なビジネス目的を実現するサービス フルフィルメントの一部であるポッド操作のポート トラフィックを提供することを目的としています。Horizon Cloud ポッドのポートとプロトコルの要件も参照してください。
- ファームおよび VDI デスクトップ割り当てに対して複数のテナント サブネットを使用するように Horizon Cloud ポッドを編集場合、ポッド マネージャ仮想マシンのテナント サブネットに関連する NSG と Unified Access Gateway の仮想マシンの NIC のルールが更新され、追加のテナント サブネットが含まれるようになります。
- VMware に対してサポート リクエストを発行し、サポート チームがそのリクエストに対応する方法を一時的なジャンプ ボックス仮想マシンのデプロイであると判断した場合、この一時ジャンプ ボックスには一時ジャンプ ボックス リソース グループに NSG があります。この NSG は、サポート チームが終了したときにジャンプ ボックスのリソース グループが削除されると削除されます。

ポッド マネージャ仮想マシンのデプロイヤにより作成される NSG

ポッド マネージャ仮想マシンには 2 つの NIC があり、1 つは管理サブネットに接続され、もう 1 つはテナント サブネットに接続されています。デプロイヤは、これら 2 つの NIC にそれぞれ特定の NSG を作成し、各 NSG を適切な NIC に関連付けます。

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

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

表 6-18. ポッド マネージャ仮想マシンの管理 NIC 上のデプロイヤにより作成された NSG ルール

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	ルールの目的
受信	1000	AllowSshInBound	22	任意	管理サブネット	任意	許可	定常状態の運用中に VMware に対してサポート リクエストを発行し、サポート チームがそのリクエストのトラブルシューティング方法は SSH 通信用のジャンプ ボックス仮想マシンをポッドのマネージャ仮想マシンにデプロイすることであると判断した場合、この NSG ルールはそのユースケースをサポートします。緊急アクセスには、事前にお客様の許可を得る必要があります。有効期間が短いジャンプ ボックス仮想マシンは、ポッド マネージャ仮想マシンのポート 22 への SSH 接続を使用して、この仮想マシンと通信します。日常的なポッド操作では、ポッド マネージャ仮想マ

表 6-18. ポッド マネージャ仮想マシンの管理 NIC 上のデプロイヤにより作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	ルールの目的
								シン上でポート 22 が使用可能である必要はありません。
受信	1100	AllowAzureInBound	任意	任意	168.63.129.16	任意	許可	前の「一般的な事実」セクションおよび Microsoft Azure ドキュメントのトピック IP アドレス 168.63.129.16 について」で説明するように、仮想マシンが Microsoft Azure プラットフォームからの受信通信を受け付けるようにするため。
受信	1200	AllowHttpsInBound	443	任意	管理サブネット	任意	許可	クラウド制御プレーンがポッド マネージャの REST API エンドポイントと安全に通信するため。
受信	1300	AllowApacheGeodeInBound	10334-10336、41000-41002、41100-41102、42000-42002	任意	管理サブネット	任意	許可	これらのポートは、ポッド マネージャ仮想マシン間でユーザー セッションおよび FileShare 関連の情報を複製するために使用されます。

表 6-18. ポッド マネージャ仮想マシンの管理 NIC 上のデプロイヤにより作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	ルールの目的
受信	1400	AllowTelegrafInBound	9172	任意	管理サブネット	任意	許可	廃止されました。この NSG は Horizon インフラストラクチャの監視機能で使用されていましたが、VMware ナレッジベースの記事 KB93762 で説明されているように、この機能は廃止されました。
受信	1500	AllowAgentJmsInBound	4001、4002	任意	管理サブネット	任意	許可	廃止されました。この NSG は Horizon インフラストラクチャの監視機能で使用されていましたが、VMware ナレッジベースの記事 KB93762 で説明されているように、この機能は廃止されました。
受信	3000	DenyAllInBound	任意	任意	任意	任意	拒否	この NIC の受信トラフィックを前の行のアイテムに制限するためにデプロイヤによって追加されました。

表 6-19. ポッド マネージャ仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1000	AllowHttpsInBound	80 443	TCP	VirtualNetwork	任意	許可	このルールは、クライアント接続をポッドの Microsoft Azure ロード バランサにマッピングした FQDN に確立するように（VPN 経由など、企業ネットワークを介して）内部エンドユーザーに指示する、一般的ではないシナリオを提供します。このシナリオは、直接ポッド接続と呼ばれることがあります。ポッド マネージャへのログイン認証要求の場合、Horizon Client と Horizon Web クライアントはポート 443 を使用します。HTTPS ではなく HTTP をクライアントに入力するユーザーのための簡単なリダイレクト方法として、そのトラフィックはポート 80 に送信され、

表 6-19. ポッド マネージャ仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
								自動的にポート 443 にリダイレクトされます。
受信	1100	AllowAgentHttpsInBound	3443 8443	TCP	テナント サブネット	任意	許可	この NIC の受信ポート 3443 は、ベース仮想マシン、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 によって使用され、ポッド マネージャで実行される App Volumes Manager サービスにアクセスします。 この NIC の受信ポート 8443 は、Unified Access Gateway インスタンスがポッド マネージャに確認するために使用されます。ゲートウェイ インスタンスはこのエンドポイントを使用して、ポッド マネージャへの新しいクライアント接続要求の送信を確認します。

表 6-19. ポッド マネージャ仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1110	AllowGatewayBrokeringHttpsInBound	8443	TCP	VirtualNetwork	任意	許可	コードの一貫性とメンテナンスの容易さのために、ポッド デプロイヤは常にこのルールをこの NSG に書き込みます。 ポッドの外部ゲートウェイがポッドとは別の独自の VNet にデプロイされている環境では、このルールは、ポッド マネージャに確認するために外部ゲートウェイの Unified Access Gateway インスタンスからの受信トラフィックをサポートします。ゲートウェイ インスタンスはこのエンドポイントを使用して、ポッド マネージャへの新しいクライアント接続要求の送信を確認します。

表 6-19. ポッド マネージャ仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1120	AllowUagHttpsInBound	8443	TCP	管理サブネット	任意	許可	このルールは、将来のサービス リリースで使用される予定です。

表 6-19. ポッド マネージャ仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1200	AllowAgentJmsInBound	4001 4002	TCP	テナント サブネット	任意	許可	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 仮想マシンの Horizon Agent はこれらのポートを使用します。 ポート 4001 は、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）用です。 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

表 6-19. ポッド マネージャ仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
								用してセキュアな SSL 接続を確立します。 **注：** 定常状態の動作には、4001 と 4002 の両方が必要です。場合によっては、エージェントがポッドに再入力する必要があります。
受信	1210	AllowRouterJmsInBound	4101	TCP	テナント サブネット	任意	許可	ポッドで高可用性 (HA) が有効になっている場合、このトラフィックはポッド マネージャ仮想マシン（node-1 および node-2）間の JMS ルーティングです。

表 6-19. ポッド マネージャ仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1300	AllowAgentUdpInBound	5678	UDP	テナント サブネット	任意	許可	マニフェスト 1600 以降のポッドでは廃止されました。サービスの 2019 年 9 月のリリースでは、DaaS Agent がポッド マニフェスト 1600 時点の Horizon Agent に組み込まれました。以前は、このポート 5678 と UDP プロトコルは、DaaS Agent の使用をサポートするために使用されていました。

表 6-19. ポッド マネージャ仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1400	AllowAzureInBound	任意	任意	168.63.129.16	任意	許可	前の「一般的な事実」セクションおよび Microsoft Azure ドキュメントのトピック IP アドレス 168.63.129.16 について」で説明するように、仮想マシンが Microsoft Azure プラットフォームからの受信通信を受け付けるようにするため。
受信	3000	DenyAllInBound	任意	任意	任意	任意	拒否	この NIC の受信トラフィックを前の行のアイテムに制限するためにデプロイヤによって追加されました。

外部 Unified Access Gateway 仮想マシンのデプロイヤにより作成される NSG

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

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

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

表 6-20. 外部 Unified Access Gateway 仮想マシンの管理 NIC 上のデプロイヤにより作成された NSG ルール

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

表 6-20. 外部 Unified Access Gateway 仮想マシンの管理 NIC 上のデプロイヤにより作成された NSG ルール（続き）

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

表 6-21. 外部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール

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

表 6-21. 外部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-21. 外部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-21. 外部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-21. 外部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-21. 外部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-22. 外部 Unified Access Gateway 仮想マシンの DMZ NIC 上のデプロイヤにより作成された NSG ルール

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

表 6-22. 外部 Unified Access Gateway 仮想マシンの DMZ NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-22. 外部 Unified Access Gateway 仮想マシンの DMZ NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

内部 Unified Access Gateway 仮想マシンのデプロイヤにより作成される NSG

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

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

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

表 6-23. 内部 Unified Access Gateway 仮想マシンの管理 NIC 上のデプロイヤにより作成された NSG ルール

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

表 6-23. 内部 Unified Access Gateway 仮想マシンの管理 NIC 上のデプロイヤにより作成された NSG ルール（続き）

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

表 6-24. 内部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール

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

表 6-24. 内部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-24. 内部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-24. 内部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-24. 内部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-24. 内部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-24. 内部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

表 6-24. 内部 Unified Access Gateway 仮想マシンのテナント NIC 上のデプロイヤにより作成された NSG ルール （続き）

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

外部ゲートウェイが専用の VNet にデプロイされている場合のゲートウェイ コネクタ仮想マシンのデプロイヤが作成した NSG

ゲートウェイ コネクタ仮想マシンには 1 つの NIC があります。この NIC は、外部ゲートウェイの VNet の管理サブネットに接続されています。デプロイヤは単一の NSG を作成し、その NSG を NIC と関連付けます。デフォルトでは、ゲートウェイ コネクタの管理 NIC 用にデプロイヤで作成された NSG には、ポッド マネージャ仮想マシン用にデプロイヤで作成された NSG と同じルールがあります。

表 6-25. 外部ゲートウェイのコネクタ仮想マシンの管理 NIC でデプロイヤが作成した NSG ルール

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1000	AllowSshInBound	22	任意	管理サブネット	任意	許可	定常状態の運用中に VMware に対してサポート リクエストを発行し、サポート チームがそのリクエストのトラブルシューティング方法は SSH 通信用のジャンプ ボックス仮想マシンをゲートウェイ コネクタ仮想マシンにデプロイすることであると判断した場合、この NSG ルールはそのユースケースをサポートします。緊急アクセスには、事前にお客様の許可を得る必要があります。有効期間の短いジャンプ ボックス仮想マシンは、ゲートウェイ コネクタ仮想マシンのポート 22 への SSH 接続を使用して、この仮想マシンと通信します。日常的なポッド操作では、ゲートウェイ コネク

表 6-25. 外部ゲートウェイのコネクタ仮想マシンの管理 NIC でデプロイヤが作成した NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
								タ仮想マシン上でポート 22 が使用可能である必要はありません。
受信	1100	AllowAzureInBound	任意	任意	168.63.129.16	任意	許可	前の「一般的な事実」セクションおよび Microsoft Azure ドキュメントのトピック IP アドレス 168.63.129.16 について」で説明するように、仮想マシンが Microsoft Azure プラットフォームからの受信通信を受け付けるようにするため。
受信	1200	AllowHttpsInBound	443	任意	管理サブネット	任意	許可	クラウド制御プレーンがゲートウェイ コネクタの REST API エンドポイントと安全に通信するため。

表 6-25. 外部ゲートウェイのコネクタ仮想マシンの管理 NIC でデプロイヤが作成した NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1300	AllowApacheGeodeInBound	10334-10336、41000-41002、41100-41102、42000-42002	任意	管理サブネット	任意	許可	これらのポートは、ポッド マネージャ仮想マシンおよびゲートウェイ コネクタ仮想マシン上でユーザー セッションおよび FileShare 関連の情報を複製するために使用されます。
受信	1400	AllowTelegrafInBound	9172	任意	管理サブネット	任意	許可	廃止されました。この NSG は Horizon インフラストラクチャの監視機能で使用されていましたが、VMware ナレッジベースの記事 KB93762 で説明されているように、この機能は廃止されました。

表 6-25. 外部ゲートウェイのコネクタ仮想マシンの管理 NIC でデプロイヤが作成した NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	1500	AllowAgentJmsInBound	4001、4002	任意	管理サブネット	任意	許可	廃止されました。この NSG は Horizon インフラストラクチャの監視機能で使用されていましたが、VMware ナレッジベースの記事 KB93762 で説明されているように、この機能は廃止されました。
受信	3000	DenyAllInBound	任意	任意	任意	任意	拒否	この NIC の受信トラフィックを前の行のアイテムに制限するためにデプロイヤによって追加されました。

一時ジャンプ ボックス仮想マシンのデプロイヤが作成した NSG

VMware に対してサポート リクエストを発行し、サポート チームがそのリクエストに対応する方法を一時的なジャンプ ボックス仮想マシンのデプロイであると判断した場合、この一時ジャンプ ボックスには一時ジャンプ ボックス リソース グループに NSG があります。この NSG は、サポート チームがこのような作業を完了したときにジャンプ ボックスのリソース グループが削除されると削除されます。緊急アクセスには、事前にお客様の許可を得る必要があります。

表 6-26. 一時ジャンプ ボックス仮想マシンの管理 NIC でサービスが作成した NSG ルール

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
受信	100	AllowSSHInBound	22	任意	管理サブネット	管理サブネット	許可	サービス リクエストに対する VMware のサポート チームの調査に関わる VMware 管理対象アプライアンスへの SSH 通信用。一時ジャンプ ボックス仮想マシンは、SSH とポート 22 を使用して通信します。 **注：** クラウド制御プレーンがポッドへのアクセスを失った場合、サポート チームはパブリック IP アドレスを持つ緊急ジャンプ ボックスをデプロイしてポッドへのアクセスを確立する場合があります。このシナリオでは、このルールに Source=Any と Destination=Any が必要です。
送信	100	AllowSSHOutbound	22	TCP	管理サブネット	管理サブネット	許可	ジャンプ ボックス仮想マシンによる指定され

表 6-26. 一時ジャンプ ボックス仮想マシンの管理 NIC でサービスが作成した NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
								た機能の実行用。
送信	101	AllowHttpsOutbound	443	TCP	管理サブネット	任意	許可	ジャンプ ボックス仮想マシンが、Microsoft Azure CLI（コマンド ライン インターフェイス）など、外部に配置された特定のソフトウェア コンポーネントをダウンロードして、設計された機能を実行するため。
送信	102	AllowHttpOutbound	80	TCP	管理サブネット	任意	許可	ジャンプ ボックス仮想マシンが、Ubuntu ソフトウェア アップデートなど、外部に配置された特定のソフトウェア コンポーネントをダウンロードして、設計された機能を実行するため。
送信	103	AllowUagOutbound	9443	TCP	管理サブネット	管理サブネット	許可	ジャンプ ボックス仮想マシンが、ゲートウェイの管理インターフェイスを使用してゲートウェイ管理設定に関連する設計された機能を実行するため。

表 6-26. 一時ジャンプ ボックス仮想マシンの管理 NIC でサービスが作成した NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
送信	104	AllowDns Outbound	53	任意	管理サブネット	任意	許可	ジャンプ ボックス仮想マシンが DNS サービスにアクセスするため。

表 6-26. 一時ジャンプ ボックス仮想マシンの管理 NIC でサービスが作成した NSG ルール （続き）

方向	優先順位	名前	ポート	プロトコル	ソース	送信先	アクション	目的
送信	105	AllowHttpProxyOutbound	任意	TCP	任意	任意	許可	ポッドのデプロイが、プロキシ ポートが 80 以外のプロキシを使用するように構成されている場合、一時的なジャンプ ボックス デプロイヤは、この NSG にこのルールを作成します。このルールは、このようなプロキシ環境で一時的なジャンプ ボックスをサポートします。 ポッド デプロイの構成でプロキシが指定されていないか、プロキシ ポート 80 で指定されている場合、このルールはこの NSG に表示されません。
送信	1000	DenyAllOutBound	任意	TCP	任意	任意	拒否	この TCP を使用する NIC の送信トラフィックを前の行のアイテムに制限します。

第 1 世代テナント - 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

Microsoft Azure のキャパシティを使用して Horizon Cloud ポッドをデプロイするプロセスの一環として、一連のリソース グループが Microsoft Azure サブスクリプションに自動的に作成されます。このトピックでは、それらのリソース グループとその目的について説明します。Microsoft Azure ポータルを使用して Microsoft Azure 環境にログインすると、これらのリソース グループを確認できます。ポッドの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と、そのゲートウェイをサポートするリソース グループがそのサブスクリプションに作成されます。

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情報はこのページから削除されました。

次のセクションの表では、*podID* はポッドの一意の識別子を示します。Horizon Cloud の 3 章 第 1 世代テナント - 第 1 世代 Horizon Cloud がサポートするすべてのポッド タイプのクラウド接続ポッドの管理から移動すると、ポッドの詳細ページにポッドの識別子が表示されます。*poolID* は、ファームまたは VDI デスクトップ割り当ての一意の識別子を示します。*Deployment-ID* は、外部ゲートウェイがポッドの VNet とは別に専用の VNet を使用してデプロイされるときに、その外部ゲートウェイに関連する一意の識別子を参照します。

仮想マシンを含むリソース グループには、仮想マシンのネットワーク インターフェイス (NIC)、ネットワーク セキュリティ グループ (NSG)、および類似のアーティファクトなど、それらの仮想マシンに関連付けられたリソースも含まれています。Microsoft Azure ポータルにログインし、リソース グループに移動して、含まれているアーティファクトを確認します。ポッド デプロイヤがポッド仮想マシンの NIC 用に作成する NSG 内のデフォルト ルールの詳細については、第 1 世代テナント - Microsoft Azure にデプロイされた 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。

一部のリソース グループはポッドごとに異なりますが、それ以外のリソース グループは Microsoft Azure サブスクリプションで作成され、同じ Microsoft Azure サブスクリプションを使用してデプロイされたすべてのポッドで使用されるリソースを含みます。そのようなクロスポッド リソース グループは、そのサブスクリプションを使用して最初のポッドがデプロイされるときに作成されます。

注：

- 2020 年 3 月のサービスのリリースから、Horizon Cloud デプロイヤは、デプロイヤによって自動的に作成されたものではなく、ユーザーが作成する既存のリソース グループに外部 Unified Access Gateway 構成をデプロイすることができます。このオプションは、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にのみ使用できます。このシナリオでは、そのリソース グループの名前付けはユーザーおよびユーザーの組織によって制御され、ここで説明するパターンに従ったものにはなりません。
- 2020 年 10 月のサービス リリース以降、Horizon Cloud デプロイヤは、ポッドのデプロイおよびゲートウェイのデプロイ中にデプロイヤが作成するリソース グループにカスタムの Azure リソース タグを適用するための機能を提供します。この機能は、ワークフローを実行して新しいポッドをデプロイするとき、またはワークフローを実行してポッドを編集し、新しいゲートウェイ構成を追加するときに使用できます。

Horizon Cloud によって作成されるポッドごとのリソース グループ

ポッドのデプロイ ウィザードでカスタムの Azure リソース タグが指定されている場合、デプロイヤは、ポッドのデプロイ中に、指定されたタグを次のリソース グループに適用します。

- `vmw-hcs-podID`
- `vmw-hcs-podID-base-vms`

ゲートウェイ構成をデプロイする場合、オプションで、デプロイヤがポッドに指定されているものと同じ Azure リソース タグを適用するか、異なるカスタム リソース タグを指定するかを選択できます。いずれの場合も、デプロイヤは、両方のタイプのゲートウェイのリソース グループに同じカスタム リソース タグのセットを適用します。

ファームまたは VDI デスクトップ割り当てを作成するときに、カスタムの Azure リソース タグを指定できます。ファームまたは割り当て作成ウィザードで指定された Azure リソース タグは、それらのファームまたは VDI デスクトップ割り当ての作成時にリソース グループに適用されます。

リソース グループ	目的
vmw-hcs-*podID*	ポッド マネージャ仮想マシンとそれらの関連リソースが含まれています。
vmw-hcs-*podID*-uag	ポッドに外部 Unified Access Gateway 設定があるときに作成されます。Unified Access Gateway 仮想マシンとその関連リソースが含まれています。
vmw-hcs-*podID*-uag-internal	ポッドに内部 Unified Access Gateway 設定があるときに作成されます。Unified Access Gateway 仮想マシンとその関連リソースが含まれています。
vmw-hcs-*podID*-base-vms	ポッド単位での Microsoft Azure Marketplace からのベース仮想マシンの自動作成と、Horizon Cloud とのペアリングを実行して、または Microsoft Azure から Horizon Cloud に仮想マシンを手動で構築してインポートするで作成した基本イメージ仮想マシン、およびそれらの仮想マシンの関連リソースが含まれています。イメージ仮想マシンが Horizon Cloud に公開された（イメージのシーリングとも言う）後、仮想マシンは、関連付けられたリソースとともにこのリソース グループに配置されたままになります。
vmw-hcs-*podID*-*poolID*	ファームまたは VDI デスクトップ割り当て用の仮想マシンとそれらの仮想マシンの関連リソースが含まれています。ファームまたは VDI デスクトップの割り当てが作成されるたびに、このリソース グループが作成されます。ポッドのすべてのファームまたは VDI デスクトップ割り当ては、これらのリソース グループの 1 つです。

リソース グループ	目的
vmw-hcs-*podID*-recovery	**注：** サービス リリース v2111 以降、このリソース グループの使用は非推奨となりました。その時点から新しいデプロイの場合、ポッド デプロイヤは Microsoft Azure サブスクリプションにこのリソース グループを作成しなくなります。 サービス リリース v2201 より前のバージョンでは、ポッド デプロイヤはこのリソース グループを作成して、Horizon Cloud の Horizon Cloud on Microsoft Azure デプロイのバックアップとリストアをサポートするストレージ関連およびスナップショット関連のアーティファクトを保持していました。 リストア プロセスの強化により、このリソース グループへの依存関係が削除されました。マニフェスト 3139.x より前のマニフェストでの既存のデプロイの場合、デプロイがマニフェスト 3139.x 以降への Blue-Green の更新に対してスケジュール設定されると、サービスは既存の `vmw-hcs-podID-recovery` リソース グループを自動的に削除します。
vmw-hcs-*podID*-jumpbox	このリソース グループは、お客様が 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に対応する方法として、VMware が管理するアプライアンスとの通信用に一時的なジャンプ ボックス仮想マシンをデプロイすることを決定した場合にのみ、一時的に作成されます。このようなジャンプ ボックスのデプロイについては、お客様に許可を求める必要があります。このリソース グループとそれに関連付けられたリソースは、サポート チームがそのような作業を完了すると削除されます。

専用の VNet にデプロイされた外部ゲートウェイに固有の、Horizon Cloud によって作成されたリソース グループ

ゲートウェイ構成をデプロイする場合、オプションで、デプロイヤがポッドに指定されているものと同じ Azure リソース タグを適用するか、異なるカスタム リソース タグを指定するかを選択できます。外部ゲートウェイが独自の VNet にデプロイされ、Azure リソース タグがデプロイ ウィザードで指定されているこのシナリオでは、デプロイヤは以下を実行します。

- ポッド自体に対して指定されたカスタム Azure リソース タグを `vmw-hcs-Deployment-ID` リソース グループに適用します。
- ポッド自体に対して指定されたリソース タグ、またはゲートウェイに対して指定された別のリソース タグを `vmw-hcs-Deployment-ID-nnnnnnnn-nnnn-uag` リソース グループに適用します。

リソース グループ	目的
vmw-hcs-*Deployment-ID*	ゲートウェイ コネクタ仮想マシンとその関連リソースが含まれています。このゲートウェイ コネクタ仮想マシンは、専用の VNet 上のこの外部ゲートウェイ構成内の Unified Access Gateway インスタンスを、ピアリングされた独自の VNet 内のポッド マネージャ インスタンスと接続するために使用されます。
vmw-hcs-*Deployment-ID*-*nnnnnnnn-nnnn*-uag	ポッドに外部 Unified Access Gateway 設定があるときに作成されます。Unified Access Gateway 仮想マシンとその関連リソースが含まれています。値 *nnnnnnnn-nnnn* は、Horizon Cloud 制御プレーンのゲートウェイ設定 ID と呼ばれるものに対応する一意の識別子です。
vmw-hcs-*Deployment-ID*-jumpbox	このリソース グループは、お客様が 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に対応する方法として、VMware が管理するアプライアンスとの通信用に一時的なジャンプ ボックス仮想マシンをデプロイすることを決定した場合にのみ、一時的に作成されます。このようなジャンプ ボックスのデプロイについては、お客様に許可を求める必要があります。このリソース グループとそれに関連付けられたリソースは、サポート チームがそのような作業を完了すると削除されます。

Horizon Cloud によって作成されるクロスポッドのリソース グループ

これらのクロスポッド リソース グループは、そのサブスクリプションを使用して最初のポッドがデプロイされるときに作成されます。最初のポッドがサブスクリプションにデプロイされるときにカスタムの Azure リソース タグがデプロイ ウィザードで指定されている場合、ポッド デプロイヤは、デプロイヤがリソース グループを作成するときに、それらのリソース グループに同じカスタム タグを適用します。

リソース グループ	目的
vmw-hcs-images-*region*	**注：** 2022 年 2 月のサービス リリース v2201 以降、このリソース グループの使用は非推奨となりました。その時点から新しいデプロイの場合、ポッド デプロイヤは Microsoft Azure サブスクリプションにこのリソース グループを作成しなくなります。 サービス リリース v2201 より前のバージョンでは、ポッドのデプロイがリージョンで初めて実行されたときに、ポッド デプロイヤがそのリージョン固有のリソース グループを作成していました。そのリリースより前にデプロイされたポッドの場合、このリソース グループには、特定の Microsoft Azure リージョン (*region*) にデプロイされたポッドの仮想マシンを構成するために使用される Horizon Cloud の事前構成済み VHD ファイルが含まれます。
vmw-hcs-*diagnostics*	**注：** 2022 年 1 月中旬以降、このリソース グループの使用は非推奨となりました。その時点から新しいポッドのデプロイの場合、ポッド デプロイヤは Microsoft Azure サブスクリプションにこのリソース グループを作成しなくなります。 2022 年 1 月中旬より前は、最初のポッドのデプロイがそのサブスクリプションで完了したときに、ポッド デプロイヤはこのリソース グループをサブスクリプションに作成していました。それ以前にデプロイされたポッドの場合、このリソース グループは、サブスクリプションのポッドのポッド デプロイ ログ ファイルを含む Horizon Cloud 診断ストレージ アカウントに使用されます。

シングル ポッド ブローカから Universal Broker への移行について 7

このトピックでは、Horizon Cloud テナントのブローカ移行プロセスについてと移行を実行して得られるメリットについて紹介します。シングルポッド ブローカと Universal Broker の環境の違い、およびブローカの移行前、移行中、移行後に想定可能な点について説明します。

ブローカ移行プロセスについて

ブローカの移行が完了すると、Horizon Cloud テナント環境でエンドユーザーの割り当てからリソースを仲介する方法が、シングル ポッド仲介から Universal Broker の使用に変わります。新しいテナント全体のブローカとして、Universal Broker が接続要求を管理し、要求された割り当てから利用可能な最適なリソースにルーティングします。

ブローカ移行プロセスにより、エンド ユーザー割り当てに次の変更を行います。

- VDI デスクトップ割り当ては、Universal Broker によって仲介されるマルチクラウド割り当てに変換されます。マルチクラウド割り当てには、複数のポッドの VDI デスクトップを含めることができます。
- セッションベースのデスクトップとアプリケーションの割り当ては変更されません。セッションベースのデスクトップまたはアプリケーションの割り当てには、シングル ポッドからのリソースのみを含めることができますが、割り当ては現在、Universal Broker によって仲介されています。

移行機能は、環境が現在シングル ポッド仲介を使用し、Horizon Cloud - Universal Broker に移行するためのシステム要件に記載されている前提条件を満たす場合にのみ利用できます。

Universal Broker に移行するべき理由

VMware が提供する最新のクラウドベースの仲介テクノロジーである Universal Broker の使用に移行すると、主に次のようなメリットが得られます。

複数のポッドからの VDI デスクトップを使用したエンド ユーザー割り当て

シングル ポッド仲介では、VDI 割り当て内のすべてのデスクトップが同じポッドから取得されている必要があります。デスクトップ仲介はポッドごとに行われます。

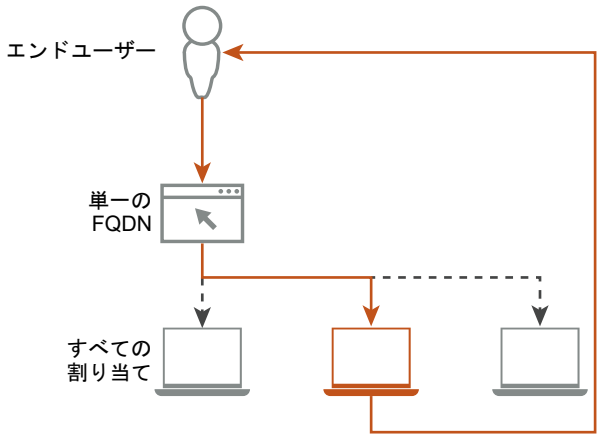
Universal Broker を使用すれば、マルチクラウド割り当てとも呼ばれる複数のポッドからの VDI デスクトップの割り当てを作成できます。エンド ユーザーは割り当てにアクセスし、その割り当てに含まれる任意のポッドからデスクトップを受信できます。詳細については、VMware Horizon Service Universal Broker についておよびそのサブトピックを参照してください。

セッションベースのデスクトップ割り当てとアプリケーション割り当てを引き続き使用できます。違う点は、これらの割り当てからのセッションベースのデスクトップとアプリケーションが、ポッドごとの仲介ではなく Universal Broker によって仲介されることです。

すべてのリモート リソースの単一の接続 FQDN

シングル ポッド仲介を使用する場合、エンド ユーザーは各ポッドの完全修飾ドメイン名 (FQDN) に個別に接続して、そのポッドからの割り当てにアクセスする必要があります。仲介はポッドごとに行われます。

Universal Broker を使用すると、ユーザーは 1 つの FQDN に接続してすべての割り当てにアクセスできます。FQDN は、Universal Broker 設定で定義します。単一の FQDN を介して、ユーザーは環境内の任意のサイトから、参加しているすべてのポッド（Microsoft Azure の Horizon Cloud ポッドと VMware SDDC ベースのプラットフォーム上の Horizon ポッドの両方を含む）の割り当てにアクセスできます。ポッド間の内部ネットワークは必要ありません。



最適なパフォーマンスのためのグローバル ポッド接続と認識

Universal Broker は、マルチクラウド割り当てに参加しているすべてのポッドとの直接接続を維持し、各ポッドの可用性ステータスを引き続き認識します。その結果、Universal Broker はエンド ユーザーの接続要求を管理し、これらのポッドから直接仮想リソースにルーティングできます。パフォーマンスの低下や遅延の問題の原因となる、グローバル サーバ ロード バランシング (GSLB) やポッド間のネットワーク通信を行う必要はありません。

スマート仲介

Universal Broker は、地理的サイトとポッド トポロジの認識に基づいて、最短のネットワーク ルートに沿って割り当てからエンド ユーザーにリソースを仲介できます。

移行しない場合の理由

今回のリリースの Universal Broker には、機能上いくつかの既知の制限があります。ユースケースで、Universal Broker がサポートしていない機能が必要な場合は、Universal Broker がその機能をサポートするまで、シングル ポッド仲介を使用してテナント環境を維持することを検討してください。現在の Universal Broker 制限事項のリストについては、Universal Broker - 機能に関する注意事項と既知の制限を参照してください。

ブローカの移行中に何が起きますか?

移行ワークフローは、いくつかの段階で構成されます。移行を実行する手順の詳細については、シングル ポッド ブローカから Universal Broker への移行をスケジューリングして完了するを参照してください。

移行前と移行中に発生するプロセスの概要を以下に示します。

1 ワークフローを開始するには、まず、移行が実行される日時をスケジューリングする必要があります。このスケジューリング タスクに沿って、移行中に Universal Broker サービスの設定に使用する構成オプションを定義します。

2 スケジュールリングされた開始時刻の少なくとも 15 分前に、コンソールで進行中のすべての操作を完了し、保持する変更をすべて保存します。すべての構成ウィザードとダイアログ ボックスを閉じます。さらに、Microsoft Azure 内のすべてのポッドがオンラインで、健全な準備完了の状態であることを確認します。

3 移行を開始すると、コンソールからログアウトして再度ログインするように求めるプロンプトが表示されます。

4 移行の最初の段階では、次の状態が予測されます。

   - コンソールの編集コントロールにアクセスできません。コンソールには、移行が進行中であることを示すバナーが表示されます。
   - Microsoft Azure のすべてのポッドは、[Default-Site] という名前のサイトに追加されます。
   - VDI デスクトップ割り当ては、Universal Broker によって仲介されるマルチクラウド割り当てに変換されます。デフォルトの割り当て設定では、接続アフィニティは [最も近いサイト] に設定され、範囲は [サイト内] に設定されます。
   - セッションベースのデスクトップとアプリケーションの割り当ては変更されません。移行後、これらの割り当て内のリソースは、Universal Broker によって仲介されます。
   - この間、すべての割り当てはエンドユーザーが引き続き利用でき、すべてのアクティブなユーザーセッションは開いたままで完全に機能します。

   注: 移行のこの段階には通常約 10 分かかりますが、テナント環境に多数の割り当てが含まれている場合は最大 1 時間かかることがあります。

   移行のこの段階が完了すると、コンソールからログアウトして再度ログインするように求めるプロンプトが表示されます。

5 移行の第 2 段階では、Universal Broker サービスがセットアップ プロセスを完了し、完全に有効になります。割り当ての作成と編集を除いた、コンソールのすべての編集操作にアクセスできます。

   注: 移行のこの段階には通常、最大で 30 分かかります。ただし、システムとネットワークの状態、および環境内の割り当ての総数と専用のユーザーからデスクトップへのマッピングによっては、この段階が完了するまでに数時間かかる場合があります。

   移行のこの段階が完了すると、[設定] - [ブローカ] ページに [有効] のステータスが緑色のドットで表示されます。

   この時点で、ブローカ全体の移行が完了します。

ブローカの移行後に想定されることについて

ブローカの移行後にテナント環境に加えられる変更の詳細なリストについては、Universal Broker への移行後のテナント環境の最新情報を参照してください。

移行が完了したら、Universal Broker 環境で提供されるメリットを利用できるようになります。次のリストに、次の手順の概要と詳細ページへのリンクを示します。

- サイトとマルチクラウド VDI 割り当ての設定を変更して、Universal Broker 機能をフル活用します。たとえば、既存の割り当てにポッドを追加したり、サイト設定を調整して、Universal Broker のユーザーへのリソースの割り当て方法を微調整することができます。詳細については、Universal Broker 環境での割り当ての作成および管理および Universal Broker 環境でのサイトの操作を参照してください。
- Horizon Cloud テナントと Workspace ONE Access の間に既存の統合がある場合は、Universal Broker の使用に合わせて統合を更新する必要があります。詳しい手順については、Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合するを参照してください。

  注： VMware Workspace ONE Access 製品チームが確認したように、Universal Broker が Horizon Cloud on Microsoft Azure 展開で使用される場合、VMware Workspace ONE Access 製品の仮想アプリケーションのコレクション機能はその構成でサポートされません。この理由は、Universal Broker が古いスタイルのポッドごとの仲介よりも新しい仲介テクノロジーであるためです。つまり、Universal Broker と Workspace ONE Access の統合は、Horizon Cloud on Microsoft Azure 展開ではレガシーのポッドごとの仮想アプリケーションのコレクションよりも優先して使用されます。したがって、Universal Broker には、Horizon Cloud on Microsoft Azure 展開向けの仮想アプリケーションのコレクションの概念はありません。このため、Universal Broker および Horizon Cloud on Microsoft Azure 構成での仮想アプリケーションのコレクションの使用はサポートされません。

  Universal Broker が Horizon Cloud on Microsoft Azure 展開に構成され、これらの Horizon Cloud on Microsoft Azure 展開で Workspace ONE Access および Intelligent Hub サービスを使用する場合、コンソールの [クリーンアップ] アクションの一部である統合プロセスで、これらの展開に含まれる既存の仮想アプリケーションのコレクションをクリーンアップする必要があります。クリーンアップ アクティビティを完了すると、統合された Universal Broker と Workspace ONE Access および Intelligent Hub サービスの最新機能を使用して、同じアプリケーションが Workspace ONE Access および Intelligent Hub サービスで引き続き機能するようになります。

次のトピックを参照してください。

- Horizon Cloud - Universal Broker に移行するためのシステム要件
- シングル ポッド ブローカから Universal Broker への移行をスケジューリングして完了する
- Universal Broker への移行後のテナント環境の最新情報

Horizon Cloud - Universal Broker に移行するためのシステム要件

この記事では、シングル ポッド仲介の使用から Universal Broker へのテナントの移行をスケジューリングして完了する前に、Horizon Cloud テナント環境が満たす必要のある要件について説明します。また、Universal Broker の新しい接続 FQDN をサポートするための計画および準備の手順についても説明します。

移行後に Universal Broker によって仲介されるマルチクラウド割り当ての移行プロセスと継続的な運用をサポートするには、テナント環境が次の要件を満たしていることを確認します。

注意： テナントのポッド フリートに、Universal Broker をすでに使用している Horizon ポッドとシングル ポッド仲介を使用する Horizon Cloud ポッドが混在している場合は、すでに構成されている Universal Broker 設定の 2 要素認証設定が Horizon Cloud ポッドと一致することを特に注意する必要があります。

- Horizon Cloud ポッドがテナント環境での最小ポッド マニフェストと RSA SecurID オプションの有効化の基準を満たしている場合を除き、これらのポッドは RADIUS 認証のみをサポートします。（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。）
- Horizon Cloud ポッドが外部ゲートウェイで RSA SecurID を構成するための基準を満たしていない場合、フリート内のすべてのポッド（Horizon ポッドと Horizon Cloud ポッドの両方）で 2 要素認証を使用するには、各ポッドに RADIUS 2 要素認証が構成された外部 Unified Access Gateway が必要です。

Horizon Cloud ポッドの要件

Microsoft Azure の Horizon Cloud ポッドが次の要件を満たしていることを確認します。

- テナントに少なくとも 1 つの Horizon Cloud ポッドがあります。Horizon Cloud ポッドは、Microsoft Azure で実行されているポッド マネージャ テクノロジーに基づいています
- テナントのすべての Horizon Cloud ポッドは、ポッド マニフェスト 2298.0 以降で実行されています。特定のユースケースでは、次の要件も適用されます。
  - Horizon Cloud テナントと Workspace ONE Access の間に既存の統合がある場合は、すべてのポッドがマニフェスト 2474.0 以降で実行されている必要があります。ブローカの移行が完了した後、Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合するの説明に従って、Universal Broker の使用に合わせて統合を更新する必要があります。
  - ブローカの移行後にタスク キャンセル機能または削除保護機能を使用する場合は、すべての Horizon Cloud ポッドがマニフェスト 2474.0 以降で実行されている必要があります。ポッドがマニフェスト 2474.0 より前のマニフェストで実行されている場合、これらの機能はサポートされません。

  重要： すべての Horizon Cloud ポッドがオンラインで、健全な準備完了の状態であることを確認します。移行プロセスを完了するために、Universal Broker サービスはポッドとの通信を行い、ポッドでいくつかの構成手順を実行する必要があります。オフラインまたは使用できないポッドがある場合は、移行をスケジューリングできません。移行をスケジュールリングしても、いずれかのポッドが後でオフラインになるか、移行の進行中に使用できなくなると、Universal Broker のセットアップは失敗します。
- 移行と同時にポッドのアップグレードがスケジューリングされることはありません。

- ポッドの場所は、ポッド構成ウィザードのメニュー オプションから有効な場所を選択することによって構成されます。テキスト フィールドに手動で入力してポッドの場所を構成した場合、移行は失敗します。

  注： 手動で入力した場所に関連するこの問題は、2019 年 3 月（サービス リリース 1.9）より前に最初にデプロイされたポッドで発生する可能性が高くなります。2019 年 3 月のリリース以降、場所はシステムの世界の市区町村名データベース内の値からメニューで選択する必要があります。

  ポッドの構成された場所が原因で移行が失敗するシナリオに遭遇する可能性を減らすには、コンソールの [キャパシティ] ページに移動し、各 Horizon Cloud ポッドの [場所] 列の値を調べます。[場所] 列の値が手動で入力した名前のように表示される場合は、ポッドの [編集] アクションを使用して、[ポッドの詳細] 手順に移動し、[場所] フィールドを編集して、その値をシステムの市区町村名の値のいずれかに設定します。

- 移行ワークフローで、テナントにポッド フリート内の Horizon ポッドからの Universal Broker 設定がない場合、コンソールに Universal Broker 設定を求めるプロンプトが表示されます。Universal Broker 設定で 2 要素認証設定を構成する場合は、各ポッドに外部 Unified Access Gateway インスタンスが必要で、そのインスタンスは適切な 2 要素認証タイプで構成されている必要があります。（背景情報については、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。）

  要件は、Horizon Cloud ポッドが外部ゲートウェイで RSA SecurID タイプを構成するための基準を満たしているかどうかによって異なります。

  - Horizon Cloud ポッドが最小ポッド マニフェストおよびテナント環境での RSA SecurID オプションの有効化の条件を満たしている場合は、すべてのポッドにまたがるすべての外部 Unified Access Gateway インスタンスを同じ認証サービスを使用するように構成します。これには、管理対象状態にあるテナントの Horizon ポッドがすべて含まれます。その結果、すべてが一致する認証タイプを使用するようになります（すなわち、すべてが RADIUS またはすべてが RSA SecurID を使用）。
  - Horizon Cloud ポッドが、外部ゲートウェイで RSA SecurID を構成するための条件を満たしていないときに、フリート内のすべてのポッド（Horizon ポッドと Horizon Cloud ポッドの両方）で 2 要素認証を使用する必要がある場合、同じ RADIUS 認証サービスを使用するには、すべてのポッドにまたがるすべての外部 Unified Access Gateway インスタンスを構成する必要があります。これには、管理対象状態にあるテナントの Horizon ポッドがすべて含まれます。

注： ポッドに内部 Unified Access Gateway インスタンスだけが含まれる場合、Universal Broker は [ブローカ] ページの [ネットワーク範囲] タブで定義されたネットワーク ポリシーを上書きし、IP アドレスに関係なく、すべてのユーザーをその Unified Access Gateway インスタンスにルーティングします。

Universal Broker をサポートするための DNS、ポート、およびプロトコル要件

次の要件を確認します。

- 各ポッドが、地域の Universal Broker インスタンスに必要な DNS 名が解決可能であり、アクセス可能であるように構成されていること。Microsoft Azure での Horizon Cloud ポッドの DNS の要件の「ポッドのデプロイと操作に関する DNS の要件」の表を参照してください。
- 各ポッドが必要なポートとプロトコルで構成されている（2019 年 9 月リリースのマニフェスト以降の Horizon Cloud ポッドのポートとプロトコルの要件の「Universal Broker で必要なポートとプロトコル」セクションを参照）。

Universal Broker をサポートするための FQDN 要件

シングル ポッド仲介を使用する場合、エンド ユーザーは各ポッドの完全修飾ドメイン名 (FQDN) に個別に接続して、そのポッドからの割り当てにアクセスします。

Universal Broker への移行後、ユーザーは Universal Broker クラウド サービスの 1 つの FQDN に接続することで、環境内の任意のサイトの任意のポッドから任意の割り当てにアクセスできます。Universal Broker は、要求を処理できる最も適切なポッドの個々の FQDN に各ユーザー要求をルーティングします。

シングル ポッド ブローカから Universal Broker への移行をスケジューリングして完了する の説明に従って、Universal Broker 構成設定で Universal Broker FQDN を指定します。有効なサブドメインを VMware が提供する標準ドメインの前に付けることで FQDN を作成するか、完全にカスタムの FQDN を構成することができます。

注： カスタム FQDN を構成する場合は、この FQDN が自分の会社または組織を表すことに注意してください。カスタム FQDN で指定されたドメイン名の所有者であり、そのドメインを検証する証明書を提供でき、カスタム FQDN を使用するための適切な承認を持っていることを確認してください。Universal Broker のカスタム FQDN は、ポッド内のすべての Unified Access Gateway インスタンスの FQDN とは異なる一意の値でなければなりません。

ブローカ移行の計画と準備

ブローカの移行にはネットワークと割り当てのワークフローへの重要な変更が含まれるため、新しいワークフローに向けて環境とユーザーを準備するために必要なアクションを実行するようにしてください。移行の使用事例に基づく適切な準備と変更管理手順については、次のプランニング ガイドを参照してください。

移行の使用事例	計画と準備の手順
環境が単一のポッドで構成されており、そのポッドの既存の FQDN を Universal Broker の FQDN として使用する	1 シングル ポッド ブローカから Universal Broker への移行をスケジューリングして完了するで、ポッドの既存の FQDN を Universal Broker サービスのカスタム FQDN として指定します。 2 エンドユーザーの割り当てワークロードへの影響を最小限に抑える日時で移行をスケジューリングします。 3 予定された移行に備え、エンド ユーザーに通知して準備します。移行時間が近づくにつれて、作業を保存し、アクティブな接続セッションからログアウトします。 4 移行の直前に、新しい IP アドレスと FQDN をポッドに割り当てます。 5 移行が完了したら、ポッドの以前の FQDN（現在は Universal Broker の FQDN）を使用して接続セッションを再開できることをエンド ユーザーに通知します。
環境が複数のポッドで構成されており、そのポッドの新しい FQDN を Universal Broker の FQDN として構成する	1 移行プロセスの前、移行中、および移行後に実行する必要がある手順を含めるには、手順を更新します。 2 シングル ポッド ブローカから Universal Broker への移行をスケジューリングして完了するで、Universal Broker サービスの新しい FQDN を構成します。 3 エンドユーザーの割り当てワークロードへの影響を最小限に抑える日時で移行をスケジューリングします。ポッドのデプロイの規模に応じて、ユーザー トレーニングとクライアント ソフトウェアの再構成に十分な時間を確保します。 4 予定された移行に備え、エンド ユーザーに通知して準備します。移行時間が近づくにつれて、作業を保存し、アクティブな接続セッションからログアウトします。 5 移行中または移行直後に、ユーザーのクライアント システムの Horizon Client を再構成して、個々のポッドの FQDN ではなく、新しい Universal Broker FQDN に接続します。 6 新しいブローカ接続 FQDN を使用する必要があり、その結果、環境内のすべてのポッドへのユニバーサル アクセスを取得できることをエンド ユーザーに通知します。

シングル ポッド ブローカから Universal Broker への移行をスケジューリングして完了する

このトピックでは、Universal Broker への移行のスケジューリング、準備、完了の手順をご案内します。Universal Broker サービスを設定し、移行の開始日時を定義し、プロセスの各段階を円滑に移動して移行を成功する方法については、次の手順を参照してください。

ブローカの移行をスケジューリングする準備が整っている場合、[スケジュール] ボタンを含む通知バナーが Horizon Universal Console の上部に表示されます。

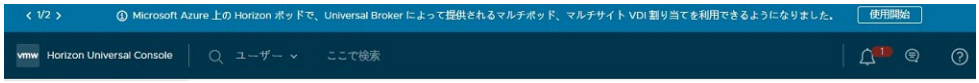
注： バナーにエラー状態が表示され、移行のスケジューリングができない場合は、移行の前提条件の 1 つ以上を満たすことができなかった可能性があります。バナーの [エラーの表示] をクリックし、[ブローカ] ページの [移行が必要です] リンクの横にあるエラー アイコンをクリックして、エラー状態の詳細を表示します。移行をスケジューリングする前に、エラー状態をクリアするための必要な手順を実行する必要があります。

前提条件

テナント環境が Horizon Cloud - Universal Broker に移行するためのシステム要件に概要を記載したすべての前提条件を満たしていることを確認します。

手順

1 ブローカ移行の通知バナーの [スケジュール] をクリックします。



このアクションよって、ブローカ ページへリダイレクトされます。このページは、現在、テナントでシングル ポッド ブローカが有効であることを示し、ブローカ移行をスケジューリングするリンクを提供します。

2 [ブローカ] ページで、[スケジュール] をクリックします。

Universal Broker の構成ウィザードが表示されます。このウィザードの手順を実行して、Microsoft Azure のポッド用の Universal Broker を設定し、Universal Broker への移行をスケジューリングします。

3 ウィザードの [FQDN] ページで、仲介接続の FQDN を構成します。これらの設定は、エンド ユーザーが Universal Broker によって割り当てられるリソースにアクセスするために使用する専用接続アドレスを定義します。

注： サブドメインまたは FQDN 設定を変更すると、すべての DNS サーバで変更が有効になるまでに時間がかかる場合があります。

a [タイプ] には、[VMware が提供] または [カスタム] の完全修飾ドメイン名 (FQDN) を選択します。

b 選択した FQDN タイプの追加設定を指定します。

- [VMware が提供] タイプを選択した場合、次のように設定を指定します。

設定	説明
`Sub Domain`	会社または組織を表すネットワーク構成内の有効なサブドメインの一意の DNS 名を入力します。このサブドメインは、仲介の FQDN を形成するために、VMware が提供するドメインの先頭に付けられます。 **注：** 一部の文字列は、システムによって禁止または予約されています。そのような文字列のカテゴリには、`book` のような一般的な語句、`gmail` のような有名企業が所有している既知の用語、プロトコル、コーディング、オープンソースの用語（たとえば `php` や `sql`）などがあります。またシステムは、`mail0`、`mail1`、`mail2` など、これらの文字列のパターンのカテゴリを禁止します。 ただし、このフィールドに禁止されている名前を入力すると、システムはその時点での入力を検証しません。ウィザードの最終サマリ ステップに到達した時点で初めて、システムはここで入力した名前を検証し、入力が禁止された名前のいずれかに一致した場合はエラーが表示されます。その場合は、より一意の名前をここで入力します。
`Brokering FQDN`	この読み取り専用フィールドには、構成された FQDN が表示されます。FQDN は `https://<your sub-domain>vmwarehorizon.com` の形式を使用します。 この FQDN をエンド ユーザーに提供し、Horizon Client を使用して Universal Broker サービスに接続できるようにします。 Universal Broker は、この FQDN の DNS および SSL 検証を管理します。

- [カスタム] タイプを選択した場合、次のように設定を指定します。

設定	説明
`Brokering FQDN`	エンド ユーザーが Universal Broker サービスへのアクセスに使用するカスタムの FQDN を入力します。カスタム FQDN は、サービスへの接続を完了する自動生成された VMware 提供の FQDN のエイリアスとして機能します。 カスタム FQDN 内で指定されたドメイン名の所有者であること、またそのドメインを検証できる証明書を指定することが必要です。 **注：** カスタム FQDN は、接続 URL とも呼ばれ、会社または組織を表します。このカスタム FQDN を使用するための適切な権限があることを確認します。 **注：** カスタム FQDN は、ポッド内のすべての Unified Access Gateway インスタンスの FQDN とは異なる一意の値でなければなりません。

設定	説明
	重要： カスタム FQDN を Universal Broker サービスの内部接続アドレスを表す VMware 提供の FQDN にマッピングする CNAME レコードを DNS サーバに作成する必要があります。たとえば、レコードは `vdi.examplecompany.com` を *<自動生成文字列>*`.vmwarehorizon.com` にマッピングすることがあります。
`Certificate`	[参照] をクリックして、仲介の FQDN を検証する証明書（パスワード保護された PFX 形式）をアップロードします。証明書は以下の条件をすべて満たす必要があります。 ■ 90 日以上有効である ■ 信頼されている認証局 (CA) によって署名されている ■ 証明書の共通名 (CN) またはそのサブジェクト代替名 (SAN) のいずれかが FQDN と一致している ■ 証明書の内容が標準の X.509 形式に準拠している PFX ファイルに、ドメイン証明書、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。 Universal Broker サービスは、この証明書を使用して、クライアントとの信頼された接続セッションを確立します。
`Password`	PFX 証明書ファイルのパスワードを入力します。
`VMware Provided FQDN`	この読み取り専用フィールドには、仲介サービス用に自動的に作成される VMware 提供の FQDN が表示されます。FQDN は `https://`*`<auto-generated string>`*`.vmwarehorizon.com` の形式を使用します。 VMware 提供の FQDN はエンド ユーザーには表示されず、Universal Broker サービスの内部接続アドレスを表します。カスタム FQDN は、VMware 提供の FQDN のエイリアスとして機能します。 **重要：** カスタム FQDN を VMware 提供の FQDN にマッピングする CNAME レコードを DNS サーバに作成して、エイリアスの関連付けを設定する必要があります。たとえば、レコードは `vdi.examplecompany.com` を *<自動生成文字列>*`.vmwarehorizon.com` にマッピングすることがあります。

c　FQDN 設定の構成が完了したら、[次へ] をクリックしてウィザードの次のページに進みます。

4 （オプション）ウィザードの [認証] ページで、2 要素認証を構成します。

デフォルトでは、Universal Broker は Active Directory のユーザー名とパスワードのみを使用してユーザーを認証します。追加の認証方法を指定することで、2 要素認証を実装できます。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。

重要： Universal Broker に 2 要素認証を使用するには、まず、参加しているすべてのポッドの各外部 Unified Access Gateway インスタンスで適切な認証サービスを構成する必要があります。外部 Unified Access Gateway インスタンスの構成は、参加しているポッド内およびポッド間で同一でなければなりません。

たとえば RADIUS 認証を使用する場合は、参加しているすべての Horizon ポッドおよび Microsoft Azure のポッドにわたって、各外部 Unified Access Gateway インスタンスに RADIUS サービスを構成する必要があります。

参加しているポッド内の Unified Access Gateway インスタンスを削除しないでください。Universal Broker は、Horizon Client と仮想リソース間のプロトコル トラフィックの Unified Access Gateway に依存しているため、参加しているポッドの Unified Access Gateway インスタンスを削除すると、ユーザーはそのポッドからプロビジョニングされたリソースにアクセスできません。

設定	説明
`Two-Factor Authentication`	2 要素認証を使用するには、このトグルを有効にします。 トグルを有効にすると、2 要素認証を構成するための追加オプションが表示されます。
`Maintain User Name`	Universal Broker への認証中にユーザーの Active Directory ユーザー名を維持する場合はこのトグルを有効にします。有効になっている場合： ■ ユーザーは、Universal Broker に対する Active Directory 認証の場合と同じユーザー名認証情報を追加の認証方法でも利用できる必要があります。 ■ ユーザーは、クライアント 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。 このトグルがオフになると、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。

設定	説明
Type	Active Directory のユーザー名とパスワードに加えて、Universal Broker がエンド ユーザーで使用する認証方法を指定します。ユーザー インターフェイスには、[RADIUS] と [RSA SecurID] の 2 つの選択肢が表示されます。 この設定は、テナント全体に適用されます。エンド ユーザー クライアントの動作は、以下のように、テナントのポッド フリートの構成と、ポッドのゲートウェイで構成されている 2 要素認証タイプによって異なります。 **Horizon ポッドのみ** ここで選択するタイプは、クライアントで使用されるタイプです。 **Horizon Cloud ポッドのみ** ■ ポッドの外部ゲートウェイで構成されているタイプと一致するタイプを選択します。 **Horizon ポッドと Horizon Cloud on Microsoft Azure デプロイの混在** 混合フリートでは、ここで [RADIUS] を選択すると、両方のポッド タイプの Unified Access Gateway インスタンスを介してユーザーの RADIUS 認証要求が試行されます。 混合フリートでは、ここで [RSA SecurID] を選択すると、クライアントの動作は、Horizon Cloud on Microsoft Azure デプロイが外部ゲートウェイで RSA SecurID を使用して構成されているかどうかによって異なります。 ■ Horizon Cloud on Microsoft Azure デプロイのゲートウェイで RSA SecurID タイプが構成されていない場合、ここで [RSA SecurID] を選択すると、Horizon ポッドの Unified Access Gateway インスタンスのみを介してユーザーの RSA 認証要求が試行されます。Active Directory のユーザー名とパスワードの認証要求は、Horizon ポッドまたは Horizon Cloud ポッドの Unified Access Gateway インスタンスを通じて試行されます。 ■ Horizon Cloud on Microsoft Azure デプロイで RSA SecurID タイプが構成されている場合、ユーザーの RSA 認証要求は両方のポッド タイプの Unified Access Gateway インスタンスを介して試行されます。
Show Hint Text	このトグルを有効にすると、クライアントのログイン画面に表示されるテキスト文字列を構成して、ユーザーに追加の認証方法に対する認証情報の入力を求めることができます。
Custom Hint Text	クライアントのログイン画面に表示す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 DisplayHint user name and password` としてエンド ユーザーに表示されます。ここで、*DisplayHint* はこのテキスト ボックスで指定するテキスト文字列です。 **注：** Universal Broker のヒント テキストに、**& < > ' "** の文字を含めることはできません。 これらの許可されていない文字のいずれかをヒント テキストに含めると、ユーザーは Universal Broker FQDN への接続に失敗します。 このヒントを参考にして、ユーザーは正しい認証情報を入力することができます。たとえば、**`Company user name and domain password below for`** のようなフレーズを入力すると、`Enter your Company user name and domain password below for user name and password` というプロンプトがエンド ユーザーに表示されます。

設定	説明
Skip Two-Factor Authentication	Universal Broker サービスに接続している内部ネットワーク ユーザーの 2 要素認証をバイパスするには、このトグルを有効にします。Universal Broker の内部ネットワーク範囲の定義の説明に従って、内部ネットワークに属しているパブリック IP アドレス範囲を指定していることを確認します。 ■ このトグルが有効になると、内部ユーザーは、Universal Broker サービスに対して認証するために、Active Directory の認証情報のみを入力する必要があります。外部ユーザーは、Active Directory の認証情報と、追加の認証サービスの認証情報の両方を入力する必要があります。 ■ このトグルがオフになると、内部および外部の両方のユーザーは、Active Directory の認証情報と、追加の認証サービスの認証情報を入力する必要があります。
Public IP Ranges	このフィールドは、[2 要素認証をスキップ] が有効になっている場合に表示されます。 [ブローカ] ページの [ネットワーク範囲] タブで 1 つ以上のパブリック IP アドレス範囲がすでに指定されている場合、このフィールドは読み取り専用で、これらの IP アドレス範囲が一覧表示されます。 [ブローカ] ページの [ネットワーク範囲] タブにパブリック IP アドレス範囲がまだ指定されていない場合は、このフィールドを使用して、内部ネットワークを表すパブリック IP アドレス範囲を指定し、それらの範囲からのトラフィックの 2 要素認証プロンプトをスキップすることができます。Universal Broker は、これらのいずれかの範囲内の IP アドレスから接続しているユーザーを、内部ユーザーと見なします。 これらの範囲を指定する目的の詳細については、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。

2 要素認証の構成が完了したら、[次へ] をクリックしてウィザードの次のページに進みます。

5 構成ウィザードの [設定] ページで、Horizon Client の [期間] 設定を構成します。

これらのタイムアウト設定は、Horizon Client と Universal Broker によって割り当てられた割り当て済みのデスクトップ間の接続セッションに適用されます。これらの設定は、割り当てられたデスクトップのゲスト OS へのユーザーのログイン セッションには適用されません。Universal Broker がこれらの設定で指定されたタイムアウト状態を検出すると、ユーザーの Horizon Client 接続セッションを閉じます。

設定	説明
Client Heartbeat Interval	Horizon Client ハートビートの間隔（分）と、ユーザーの Universal Broker への接続状態を制御します。これらのハートビートは、Horizon Client 接続セッション中に経過したアイドル時間を Universal Broker にレポートします。 Horizon Client を実行しているエンドポイント デバイスとの相互作用が発生しない場合、アイドル時間が測定されます。このアイドル時間は、ユーザーに割り当てられたデスクトップの基盤となるゲスト OS へのログイン セッションがアクティブでない状態であることの影響を受けません。 大規模なデスクトップ デプロイでは、[クライアントのハートビート間隔] を増やすとネットワーク トラフィックが減少し、パフォーマンスが向上する場合があります。
Client Idle User	Horizon Client と Universal Broker 間の接続セッションで許可される最大アイドル時間（分）。 最大時間に達すると、ユーザーの認証期間が期限切れになり、Universal Broker はすべてのアクティブな Horizon Client セッションを閉じます。接続セッションを再度開くには、ユーザーは Universal Broker ログイン画面で認証情報を再入力する必要があります。 **注：** 割り当てられたデスクトップからユーザーが予期せず切断されないようにするには、[クライアントのアイドル ユーザー] タイムアウトを [クライアントのハートビート間隔] の少なくとも 2 倍の値に設定します。

設定	説明
Client Broker Session	ユーザーの認証の有効期限が切れるまでの Horizon Client 接続セッションの最大許容時間（分）。この時間はユーザーが Universal Broker に対して認証されると開始します。セッションのタイムアウトが発生すると、ユーザーは割り当てられたデスクトップで作業を続行できます。ただし、Universal Broker との通信を必要とする設定の変更などのアクションを実行すると、Horizon Client によって Universal Broker の認証情報を再入力するように求められます。 **注：** [Client ブローカ セッション] のタイムアウトは、少なくとも [Client ハートビート間隔] 値と [Client アイドル ユーザー] のタイムアウトの合計値以上にする必要があります。
Client Credential Cache	ユーザーのログイン認証情報をクライアント システム キャッシュに保存するかどうかを制御します。キャッシュにユーザー認証情報を保存するには、**1** と入力します。キャッシュにユーザー認証情報を保存しない場合は、**0** と入力します。

期間設定の構成が完了したら、[次へ] をクリックしてウィザードの次のページに進みます。

6 ウィザードの [スケジュール] ページで、コントロールを使用して、ブローカの移行を行う [日付] および [開始時刻] を指定します。

現在の現地時間より少なくとも 1 時間早く、現在の日付から 3 か月前までの開始時刻をスケジュールリングできます。開始時刻は、正時に発生する必要があります。

開始時刻を設定するときは、移行が中断することなく進行できるよう十分な時間をとってください。

開始時刻の設定が完了したら、[次へ] をクリックして、Universal Broker 構成ウィザードの次の手順に進みます。

注： 指定した開始時刻が使用できないことを示すメッセージがコンソールに表示される場合は、[日付] および [開始時刻] 設定に戻り、移行の別の時間を指定します。

7 [サマリ] ページで設定を確認し、[終了] をクリックして Universal Broker 構成を保存して適用します。

移行が正常にスケジューリングされたことを示すメッセージが表示されます。

移行がスケジューリングされた後：

- [ブローカ] ページには、今後の移行に関する詳細が表示されます。開始時刻が 1 時間以上離れている場合は、[スケジュール] リンクをクリックして移行のスケジュールを変更できます。
- スケジュールリングされた移行をキャンセルする場合、または 1 時間以内に開始する移行のスケジュール変更を行う場合は、VMware のサポートにお問い合わせください。VMware のサポートでは、15 分以内に開始される移行をキャンセルまたは再スケジューリングすることはできませんのでご注意ください。
- 開始時刻に達するまで、コンソールには今後の移行に関する通知バナーが表示されます。[詳細の表示] をクリックすると、[ブローカ] ページにリダイレクトされます。
- 今後の移行に関する通知メッセージとリマインダ メッセージは、テナントに登録されているプライマリ E メール アカウントに送信されます。

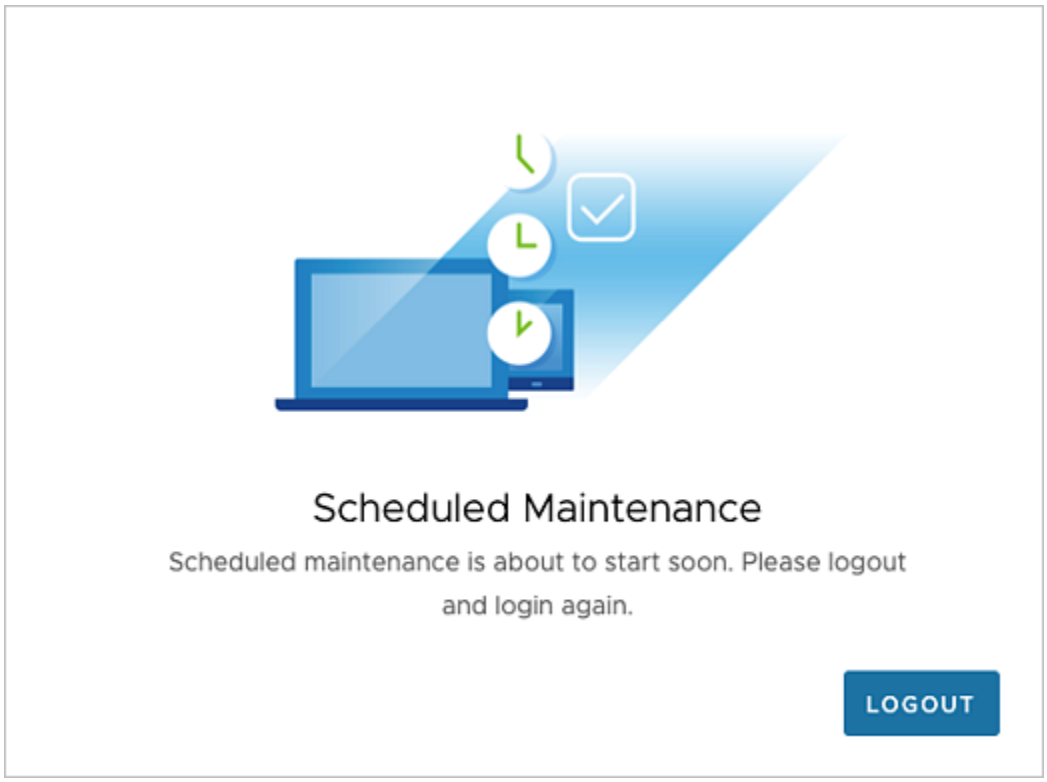
8 移行が開始する少なくとも 15 分前に、次の準備タスクを完了してください。移行中は、コンソールの編集操作にアクセスできません。

- コンソールで進行中のすべての操作を完了し、保持する変更を保存します。
- すべての構成ウィザードとダイアログ ボックスを閉じます。

重要： 移行期間中、Microsoft Azure のすべての Horizon Cloud ポッドがオンラインであり、正常で準備が整った状態であるようにしてください。Universal Broker サービスは、ポッドと通信し、ポッドでいくつかの構成手順を実行して、移行のブローカ有効化段階を完了する必要があります。いずれかのポッドがオフラインまたは使用できない場合、移行は失敗します。

重要： Microsoft Azure の Horizon Cloud ポッドと VMware SDDC ベースのプラットフォームの Horizon ポッドの両方で構成されるハイブリッド環境がある場合、移行中は、Horizon ポッドで Universal Broker サービスを利用できません。また、この間、Horizon ポッドの状態を監視対象から管理対象に変更することはできません。

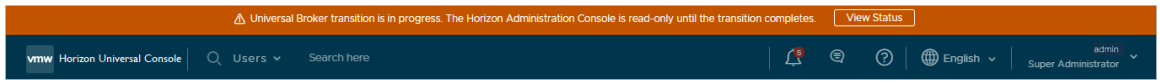
9 移行が始まる少し前に、画面のプロンプトの指示に従ってコンソールからログアウトし、再度ログインします。



10 移行の最初の段階を中断せずに続行できます。

移行のこの段階では、次の条件が発生します。

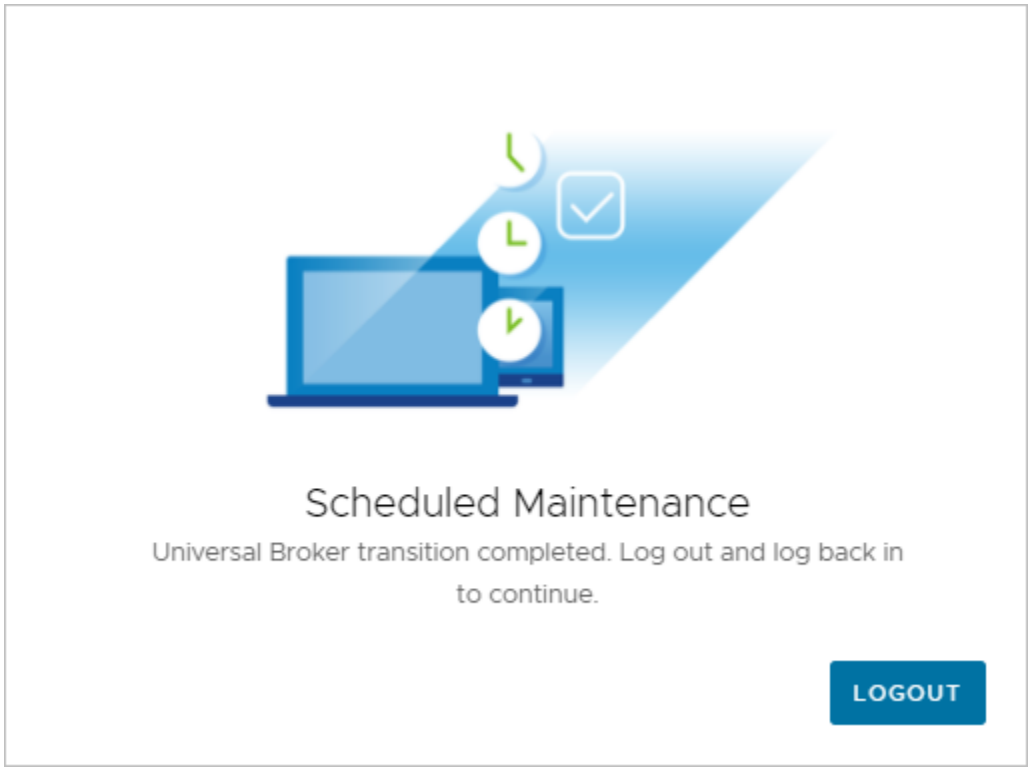
- コンソールの編集コントロールにアクセスできません。コンソールには、移行が進行中であることを示すバナーが表示されます。



- Microsoft Azure のすべてのポッドは、[Default-Site] という名前のサイトに追加されます。
- VDI デスクトップ割り当ては、Universal Broker によって仲介されるマルチクラウド割り当てに変換されます。デフォルトの割り当て設定では、接続アフィニティは [最も近いサイト] に設定され、範囲は [サイト内] に設定されます。
- セッションベースのデスクトップとアプリケーションの割り当ては変更されません。移行後、これらの割り当て内のリソースは、Universal Broker によって仲介されます。
- この間、すべての割り当てはエンドユーザーが引き続き利用でき、すべてのアクティブなユーザーセッションは開いたままで完全に機能します。

注： 移行のこの段階には通常約 10 分かかりますが、テナント環境に多数の割り当てが含まれている場合はさらに長くかかることがあります。進行状況を監視するには、通知バナーの [View のステータス] をクリックします。この段階が 1 時間以内に完了しない場合、移行はタイムアウトになり、障害としてマークされます。

移行のこの段階が完了すると、次のメッセージが表示されます。



注： 移行のこの段階で障害が発生した場合、VMware のサポートが自動通知を受け取り、障害の原因を調査して修正します。詳細について、[ブローカ] ページと、テナントに登録されているプライマリ E メール アカウントに送信される通知メッセージで確認できます。VMware のサポートが原因を修正した後、[ブローカ] ページのリンクを使用して移行を再スケジュールできます。

11 コンソールに再度ログインしたら、Universal Broker サービスがセットアップ プロセスを完了し、完全に有効になります。

すべてのグローバル リージョンの DNS サーバ間で DNS レコードが伝達されるため、通常、構成設定が Universal Broker サービスで完全に有効になるまでに最大 30 分かかります。ただし、システムとネットワークの状態、および環境内の割り当ての総数と専用のユーザーからデスクトップへのマッピングによっては、このプロセスが完了するまでに数時間かかる場合があります。このプロセスが 4 時間以内に完了しない場合、移行はタイムアウトになり、障害としてマークされます。

移行のこの段階では、割り当ての作成と編集を除いた、コンソールのすべての編集操作にアクセスできます。また、割り当ての仲介を行っているこの時間において、Universal Broker サービスを使用することはできません。

セットアップが正常に完了すると、コンソールのベル アイコンの下に通知メッセージが表示され、[設定] - [ブローカ] ページに [有効] ステータスが緑色のドットで表示されます。

これで、割り当ては Universal Broker によって仲介されるようになり、移行が完了します。

重要： Universal Broker のセットアップが失敗した場合、[設定] - [ブローカ] 画面には赤のアラート アイコンで [エラー] ステータスが表示されます。構成エラーを修正し、Universal Broker サービスをセットアップするには、VMware ナレッジベースの記事 KB2006985 の説明に従って、VMware サポートにお問い合わせください。

次のステップ

- Horizon Cloud テナントと Workspace ONE Access の間に既存の統合がある場合は、Universal Broker の使用に合わせて統合を更新する必要があります。詳しい手順については、Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合する を参照してください。
- サイトとマルチクラウド VDI 割り当ての設定を変更して、Universal Broker 機能をフル活用します。たとえば、既存の割り当てにポッドを追加したり、サイト設定を調整して、Universal Broker ブローカの割り当て方法を微調整することができます。詳細については、Horizon Cloud テナント環境でのマルチクラウド割り当ての作成および管理および「Universal Broker 環境でのサイトの操作」を参照してください。

Universal Broker への移行後のテナント環境の最新情報

この記事では、シングルポッド ブローカから Universal Broker への移行が正常に完了した後に、Horizon Cloud テナント環境に表示される変更について説明します。これらの変更には、いくつかの新機能の動作と一部の機能制限が含まれます。

Universal Broker 環境での特定の機能制限の詳細については、Universal Broker - 機能に関する注意事項と既知の制限 を参照してください。

エンド ユーザー割り当ての変更

- Microsoft Azure のすべてのポッドは、[Default-Site] という名前のサイトに追加されます。

- VDI デスクトップ割り当ては、Universal Broker によって仲介されるマルチクラウド割り当てに変換されます。デフォルトの割り当て設定では、接続アフィニティは [最も近いサイト] に設定され、範囲は [サイト内] に設定されます。

  注： 特定のユーザーは、1 つの割り当てに複数のポッドのデスクトップが含まれていても、Universal Broker によって仲介された専用割り当てから最大で 1 つの割り当てられたデスクトップを受信できます。

  重要： ユーザーが以前にシングルポッド ブローカ環境の専用割り当てから複数の割り当てられたデスクトップを受け取った場合、Universal Broker 環境への移行後にこれらのデスクトップにアクセスすることはできません。割り当てられたデスクトップにアクセスするには、ユーザーは Universal Broker の FQDN を使用する代わりにポッドの FQDN に直接接続できます。

- セッション ベースのデスクトップとアプリケーションの割り当ては、Universal Broker によって仲介されるようになりました。

同一名のデスクトップ プールへの変更

ブローカの移行前にポッド全体のデスクトップ プールが同じ名前であった場合は、異なる名前を持つように編集されます。この変更により、異なるポッドから一意の名前のデスクトップ プールを Universal Broker によって仲介される単一の割り当てに追加できるようになります。

たとえば、ブローカ移行の前に次のシナリオを実行したとします。

- Pod1 には、[TestPoolName] という名前のプールが含まれていました。
- Pod2 にも、[TestPoolName] という名前のプールが含まれていました。

移行後、この例のプール名は次のように変更されます。

- Pod1 では、プール名は [TestPoolName] のままです。
- Pod2 では、プール名が [TestPoolName1] に変更されています。

仮想マシン名プリフィックスの変更

移行前のシングルポッド ブローカ環境では、プールの仮想マシン名プリフィックスの最大文字数はカスタマイズ可能な 11 文字です。プール名を形成するには、11 文字のプリフィックスに連続する数字（最大 4 桁）が追加されます。

Universal Broker への移行後、仮想マシン名のプリフィックスは最大 9 文字のカスタマイズ可能な文字で構成できます。以前は 9 文字を超えていた仮想マシン名プリフィックスは、移行後に自動的に切り詰められます。

Universal Broker 環境でプール名を形成するには、9 文字のプリフィックスに次の文字が追加されます：2 つのランダムな英数字またはアルファベット文字とその後に続く連続する数字（最大 4 桁）。

複数の割り当てで同じ仮想マシン名プリフィックスが使用されている場合、割り当ての 1 つを編集しようとするとエラーが発生する場合があります。エラーを解決するには、編集ウィザードで割り当ての仮想マシン名プリフィックスを変更してください。

注： デスクトップ プールの構成で、[デスクトップの最大数] オプションが 0 に設定されている場合、移行後に仮想マシン名のプリフィックスとプール名は変更されずに Horizon Universal Console に表示されます。コンソールを更新して新しい仮想マシン名プリフィックスとプール名を表示するには、編集ウィザードを使用して移行された割り当てを更新します。

移行後の機能に関する考慮事項

以下の考慮事項は、Universal Broker への移行後の特定の機能に該当するものです。

- カスタマイズ割り当て（URL リダイレクト割り当てとも呼ばれる）はサポートされません。
- ポッドがマニフェスト 2474.0 より前のバージョンで実行されている場合、タスクのキャンセル機能はサポートされません。この機能を使用するには、ポッドをマニフェスト 2474.0 以降にアップグレードする必要があります。
- Horizon Cloud on Microsoft Azure 環境に Workspace ONE Access との既存の移行前統合がある場合は、Universal Broker の使用に対応するために、統合を移行後の状態に更新する必要があります。詳しい手順については、Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合するを参照してください。

  この統合を更新する場合は、Horizon Universal Console の [クリーンアップ] ワークフローを使用して、それらの環境に含まれる既存の仮想アプリケーションのコレクションをクリーンアップする必要があることに注意してください。クリーンアップ ワークフローは、レガシーのポッドごとの仮想アプリケーションのコレクション機能ではなく、統合された Universal Broker と Workspace ONE Access および Intelligent Hub サービスの最新機能を使用して、同じアプリケーションが Workspace ONE Access および Intelligent Hub サービスで引き続き機能するようになります。VMware Workspace ONE Access 製品チームが確認したように、Universal Broker が Horizon Cloud on Microsoft Azure 展開で使用される場合、VMware Workspace ONE Access 製品の仮想アプリケーションのコレクション機能はその構成でサポートされません。この理由は、Universal Broker が古いスタイルのポッドごとの仲介よりも新しい仲介テクノロジーであるためです。つまり、Universal Broker と Workspace ONE Access の統合は、レガシーのポッドごとの仮想アプリケーションのコレクションよりも優先して使用されます。したがって、Universal Broker には、Horizon Cloud on Microsoft Azure 環境向けの仮想アプリケーションのコレクションの概念はありません。

重要： ポッドがマニフェスト 2474.0 より前のバージョンで実行されている場合、インベントリ停止の削除保護機能はサポートされません。この機能を使用するには、ポッドをマニフェスト 2474.0 以降にアップグレードする必要があります。

たとえば、ポッドがマニフェスト 2474.0 より前のバージョンで実行され、移行前に削除保護が有効になっている場合、この機能は移行後に機能を停止します。その後、ポッドをマニフェスト 2474.0 以降にアップグレードすると、削除保護機能が再度機能します。

VMware Workspace ONE およびオプションの True SSO 機能を使用した Horizon Cloud 環境の使用について

8

Horizon Cloud テナント環境を Workspace ONE と統合することができます。True SSO 機能は、エンド ユーザーが自分の Horizon Cloud 環境から提供される仮想 Windows デスクトップおよびアプリケーションにシングル サインオンできるようにするための、Workspace ONE Access テナントとともに使用されるオプションの機能です。

Workspace ONE および Horizon Cloud

Horizon Cloud 環境で使用する統合方法は、テナント環境が Universal Broker またはシングルポッド ブローカのどちらを使用するように構成されているかによって異なります。

テナントにどのブローカ タイプが構成されているかを確認するには、Horizon Universal Console の [設定] - [ブローカ] に移動します。[ブローカ] ページには、テナントにシングルポッド ブローカを使用しているものがあるかどうかが示されます。

確認後、そのブローカ タイプに固有の以下のリンク ページ内の統合手順に従います。次のリストのリンクを参照して、ブローカ タイプに一致するリンクを取得してください。

True SSO と Horizon Cloud

Horizon Cloud 環境を VMware Workspace ONE と統合することは、True SSO 機能を使用するための前提条件です。Horizon Cloud 環境で True SSO が構成されている場合、エンドユーザーは、Workspace ONE 環境に関連する URL にログインして認証されます。認証されたら、それらのエンド ユーザーは資格が付与されたデスクトップまたはアプリケーションを、Active Directory 認証情報を求められることなく、起動することができます。

重要： True SSO 構成は、テナント全体の構成です。True SSO 構成は、ポッド フリートのすべての Microsoft Azure の Horizon Cloud ポッドに適用されます。その結果、Horizon Cloud テナントで初めて True SSO を正常に構成した後で、自動ポッド デプロイ ウィザードを使用して追加の Horizon Cloud ポッドを Microsoft Azure サブスクリプションにデプロイすると、システムはそれらすべてのポッドに同じ True SSO 構成を送信し、それらのポッドに対して同じ True SSO 構成を検証しようとします。

次のトピックを参照してください。

- Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合する

- シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure の環境の Horizon Cloud ポッドと Workspace ONE Access の統合
- True SSO を Horizon Cloud 環境で使用するために構成する

Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合する

このトピックでは、Universal Broker を有効にしたときに、VMware Workspace ONE Access と Intelligent Hub サービスを Horizon Cloud 環境に統合する方法について説明します。統合プロセスにより、Horizon Cloud の割り当てが Workspace ONE Intelligent Hub カタログに追加され、使用資格が付与されたユーザーが容易かつ安全にアクセスできるようになります。

Horizon Universal Console は、既存の Workspace ONE Access クラウド テナントと Horizon Cloud テナントを統合するための機能を提供します。

コンソールは、Horizon Cloud テナントで次の要件が満たされている場合にこの統合をサポートします。

- Horizon Cloud テナントに Universal Broker が構成されていること。テナントの現在の構成が、Horizon Universal Console ブローカ ページに表示されます。
- 参加しているすべてのポッドが対応する最小ソフトウェア バージョンを実行していること。
  - Microsoft Azure の Horizon Cloud ポッドの場合、統合はマニフェスト 2474.0 以降でサポートされます。
  - Horizon ポッドの場合、統合は Connection Server 7.13 および Connection Server 2012 (8.1.0) 以降でサポートされます。

注： この機能に関連するその他の考慮事項と制限事項については、Horizon Cloud - 既知の制限事項を参照してください。

用語 - 資格と割り当て

- Workspace ONE では、資格という用語は、Universal Broker サービスから Workspace ONE Intelligent Hub サービスへの同期を表すために使用されます。

- Horizon Cloud では、割り当てはリソースと資格の組み合わせを表します。Horizon Universal Console で、ユーザーを割り当てに追加すると、そのユーザーにポッドでプロビジョニングされた割り当てのリソースの使用資格が付与されます。

手順

1 Horizon Universal Console で、ブローカ ページの [ID とアクセス] タブに移動して、統合ウィザードを開始します。

2 ウィザードの手順 1 で、表示されている [選択] メニューを使用して、Horizon Cloud テナントと統合する Workspace ONE Access クラウド テナントを指定します。

- テナントの URL がドロップダウン メニューのオプションとして表示される場合(シングルポッド ブローカ環境で以前に Horizon Cloud テナントと統合されたテナントなど)、そのオプションを選択します。次に、ドキュメント ページの手順 4 に進みます。
- ドロップダウン メニューにテナントの URL がオプションとして表示されない場合は、[既存のクラウド テナントの追加] を選択して、Workspace ONE Access テナントを統合します。次の手順に進みます。

注： 1 つの Workspace ONE Access テナントのみを Horizon Cloud テナントに統合することができます。

3 [既存のクラウド テナントの追加] で、Workspace ONE Access テナントをこの Horizon Cloud テナントに追加するために必要な詳細を指定します。

a Workspace ONE Access テナントにリモート アプリケーション アクセス クライアントを作成します。

統合ウィザードを完了するには、クライアント ID とこのクライアントの共有シークレット キーが必要です。詳細については、Workspace ONE Access を使用する Horizon Cloud - リモート アプリケーション アクセス クライアントの作成を参照してください。

b Horizon Universal Console 統合ウィザードの手順 1 で [既存のクラウド テナントの追加] を選択した後、構成されたクライアントから必要な情報を求める画面のプロンプトに従います。

次のスクリーンショットは、[既存のクラウド テナントの追加] を選択した後のウィザードの手順 1 を示しています。

設定	説明
Workspace ONE Access テナントの URL	Workspace ONE Access テナントの完全な URL を入力します。次に例を示します。`https://AccessTenant.myCompany.com`
OAuth クライアント ID	Workspace ONE Access を使用する Horizon Cloud - リモート アプリケーション アクセス クライアントの作成の説明に従って、リモート アプリケーション アクセス クライアントのクライアント ID を入力します。
共有シークレット	Workspace ONE Access を使用する Horizon Cloud - リモート アプリケーション アクセス クライアントの作成の説明に従って、構成されたリモート アプリケーション アクセス クライアントの生成された共有シークレットを入力します。
利用規約	提供されたリンクを使用してサービス利用規約を確認し、チェック ボックスを選択して、契約条件に同意することを示します。

次のスクリーンショットは、サンプル データを含むフィールドを示しています。コンソールは動的であり、特定の状況に応じて表示される内容が異なる場合があります。

c 必要な情報をすべて入力したら、[次へ] をクリックします。

指定された Workspace ONE Access テナントで指定されたデータが検証されます。テナントが正常に検証されると、コンソールにテナントの詳細が表示されます。

検証に成功すると、ウィザードの手順 2 を使用して統合手順を続行できます。

4 統合をサポートするには、次の前提条件を満たす必要があります。

a 参加しているすべてのポッドがサポートされている最新のバージョンに更新されていることを確認します。このトピックの最初の要件のリストを参照してください。

b Universal Broker と Workspace ONE Access および Intelligent Hub Services との統合のための互換性のあるバージョンの Workspace ONE Access Connector がインストールされていることを確認します。

一般に、VMware は、Universal Broker およびテナントのポッドの使用と互換性もある最新の使用可能なバージョンをインストールすることをお勧めします。これは、最新バージョンには最新の修正と改善が含まれるためです。Workspace ONE Access Connector のさまざまなバージョンについては、通常どおり、Workspace ONE Access Connector のドキュメント ページとそのリリース ノートを参照してください。Universal Broker との互換性が開始された最も古いバージョンは v19.03.0.1 でした。

そのコネクタのインストールの一環として、コネクタは Workspace ONE Access クラウド テナントとペアリングされます。コネクタのインストール方法については、Workspace ONE Access Connector のドキュメントを参照してください。

注目： Workspace ONE Access、Universal Broker、および Horizon Cloud on Microsoft Azure 環境の組み合わせでは、仮想アプリケーションのコレクション機能はサポートされないことに注意してください。

Universal Broker と Workspace ONE Access の統合は、Horizon Cloud on Microsoft Azure 環境でのレガシーの仮想アプリケーション コレクションの使用よりも優先され、それを置き換えます。

したがって、以前にシングルポッド ブローカの Horizon Cloud on Microsoft Azure 環境が Workspace ONE Access と統合され、その後に Universal Broker に移行したことが理由でこのページに従っている場合は、Universal Broker に移行する前から、Workspace ONE Access テナントとペアリングされた Workspace ONE Access Connector は存在していました。この Workspace ONE Access Connector が v19.03.0.1 以降の場合、そのバージョンは Universal Broker および Workspace ONE Access の統合と互換性があります。v19.03.0.1 コネクタは、このページの手順を実行するまで、および手順 7.d に到達するまで、そのままにしておくことができます。そのコネクタが v19.03.0.1 より前のバージョンの場合は、Universal Broker と Workspace ONE Access の統合が機能するように、v19.03.0.1 以降にアップグレードしてください。

次に、このページの手順 7.d で、コンソールの画面上のクリーンアップ ガイダンスに従って、これらの環境に含まれる既存の仮想アプリケーションのコレクションをクリーンアップする必要があります。クリーンアップ アクティビティを完了すると、統合された Universal Broker と Workspace ONE Access および Intelligent Hub サービスの最新機能を使用して、同じアプリケーションが Workspace ONE Access および Intelligent Hub サービスで引き続き機能するようになります。

クリーンアップ後に、既存の Workspace ONE Access Connector を Universal Broker と互換性のある最新バージョンにアップグレードして、最新の修正と改善を取得することを強くお勧めします。

---

c インストールされている Workspace ONE Access Connector と Active Directory 間のディレクトリ統合を設定します。

Workspace ONE Access でディレクトリを設定する場合は、次の要件を満たしていることを確認してください。

- Workspace ONE Access ディレクトリのディレクトリ検索属性として sAMAccountName を設定します。
- Horizon Cloud テナントに同期されているすべての Active Directory ドメイン、ユーザー、およびグループも Workspace ONE Access テナントに同期されていることを確認します。それ以外の場合、ユーザーには Hub カタログ内のすべての資格が表示されるわけではありません。

注： Active Directory から同期されたユーザーのみが、Hub カタログから Horizon Cloud アプリケーションおよびデスクトップにアクセスできます。ジャストインタイム ユーザーやローカルユーザーなど、その他のタイプのユーザーはサポートされていません。

d Workspace ONE Access を使用する Horizon Cloud：Universal Broker が有効になっている Horizon Cloud テナントと統合するためのユーザー属性の構成 の説明に従って、大文字と小文字を区別するユーザー属性を構成します。

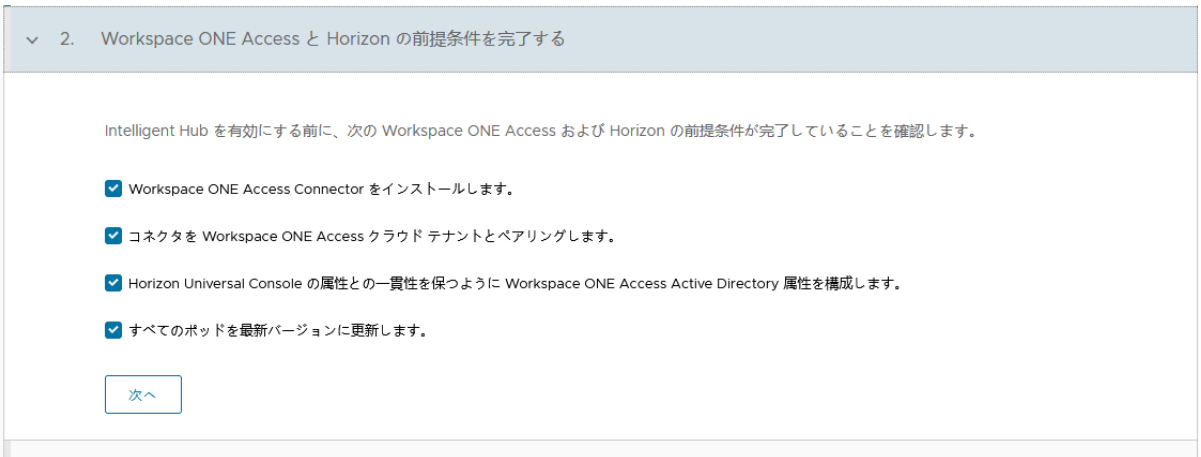
e Workspace ONE Access を使用する Horizon Cloud - Horizon Cloud との統合のための Intelligent Hub の構成の説明に従って、Workspace ONE Intelligent Hub に必要な設定を構成します。

f Workspace ONE Access を使用する Horizon Cloud：Universal Broker が有効になっている Horizon Cloud テナントと統合するためのユーザー属性の構成 の説明に従って、Workspace ONE Access テナントの必須ユーザー属性を構成します。

Workspace ONE Access は、Horizon Cloud ユーザーとの整合性を維持し、割り当て資格を同期するために、これらの属性を構成する必要があります。

5 すべての前提条件を完了したら、Horizon Universal Console の統合ウィザードに戻り、前提条件が完了していることを確認します。

コンソールで、ブローカ ページの [ID とアクセス] タブに移動し、手順 2 を展開し、リストされているすべての前提条件のチェック ボックスを選択して、[次へ] をクリックします。



6 統合ウィザードの手順 3 で、Workspace ONE Intelligent Hub サービスを有効にして、統合ワークフローを完了します。

a アクティベーション プロセスを開始するには、[アクティブ化] をクリックします。アクティベーションの開始時、処理の進行中、正常に完了したときに、コンソールにステータスメッセージが表示されます。アクティベーションを完了するまでに最大 15 分かかる場合があります。

b アクティベーションを完了したら、資格のあるユーザーが Hub カタログで Horizon Cloud の割り当てを表示し、カタログからこれらの割り当てられたリソースに正常に接続できることを確認します。

c 統合ウィザードの Horizon Universal Console ブローカ ページの [ID とアクセス] タブに戻り、エンドユーザーがカタログから割り当てにアクセスできることを示すチェック ボックスをオンにします。

d 次に、表示されるコンソールの画面上のガイダンスに従います。

コンソールの表示は動的であり、特定の状況を反映します。

したがって、表示される画面上のガイダンスを注意深く読み、何をするように指示されているかを特定し、特定の状況に応じてそれに従う必要があります。

以前にシングル ポッド ブローカを使用して Horizon Cloud on Microsoft Azure 環境と統合されていなかった Workspace ONE Access テナントを統合する場合

コンソールの画面上のガイダンスに従って、統合を確認します。

以前にシングル ポッド ブローカ（後で Universal Broker に移行）を使用して Horizon Cloud on Microsoft Azure 環境と統合された Workspace ONE Access テナントを統合する場合

コンソールには、レガシー統合に関連するガイダンスが表示されます。レガシー統合のクリーンアップに関するコンソールの画面上のガイダンスに従います。

画面上のガイダンスと手順に従うと、レガシー統合は Universal Broker 統合環境に変換されます。クリーンアップ タスクをバックグラウンドで自動的に実行することを許可します。

期待値を設定するために、これらのクリーンアップ タスクは次の項目に適用されます。

- Horizon Universal Console の [ID 管理] ページから設定された ID プロバイダの構成エントリ。
- 仮想アプリケーションのコレクションとリソース同期プロファイル。

注意: 仮想アプリケーションのコレクション機能は、Workspace ONE Access、Universal Broker、および Horizon Cloud on Microsoft Azure 環境の組み合わせではサポートされていません。この Workspace ONE Access と Universal Broker の統合プロセスでは、これらの Horizon Cloud on Microsoft Azure 環境から既存のすべての仮想アプリケーションのコレクションをクリーンアップすることが要件です。

コンソールの [クリーンアップ] ボタンを使用したシステムの自動クリーンアップは、Horizon Cloud on Microsoft Azure 環境のすべてのテナント ホスト エントリが現在統合中のこの Horizon Cloud テナントに属している仮想アプリケーションのコレクションにのみ適用されます。仮想アプリケーション コレクションに別の Horizon Cloud テナントまたは Horizon Cloud 以外のホストに属するテナント ホスト エントリが含まれている場合は、必要に応じてテナント ホスト エントリまたは仮想アプリケーション コレクションのいずれかを手動でクリーンアップする必要があります。その後、手動クリーンアップを完了したら、手動クリーンアップ タスクが完了したことを確認するチェック ボックスをオンにする必要があります。

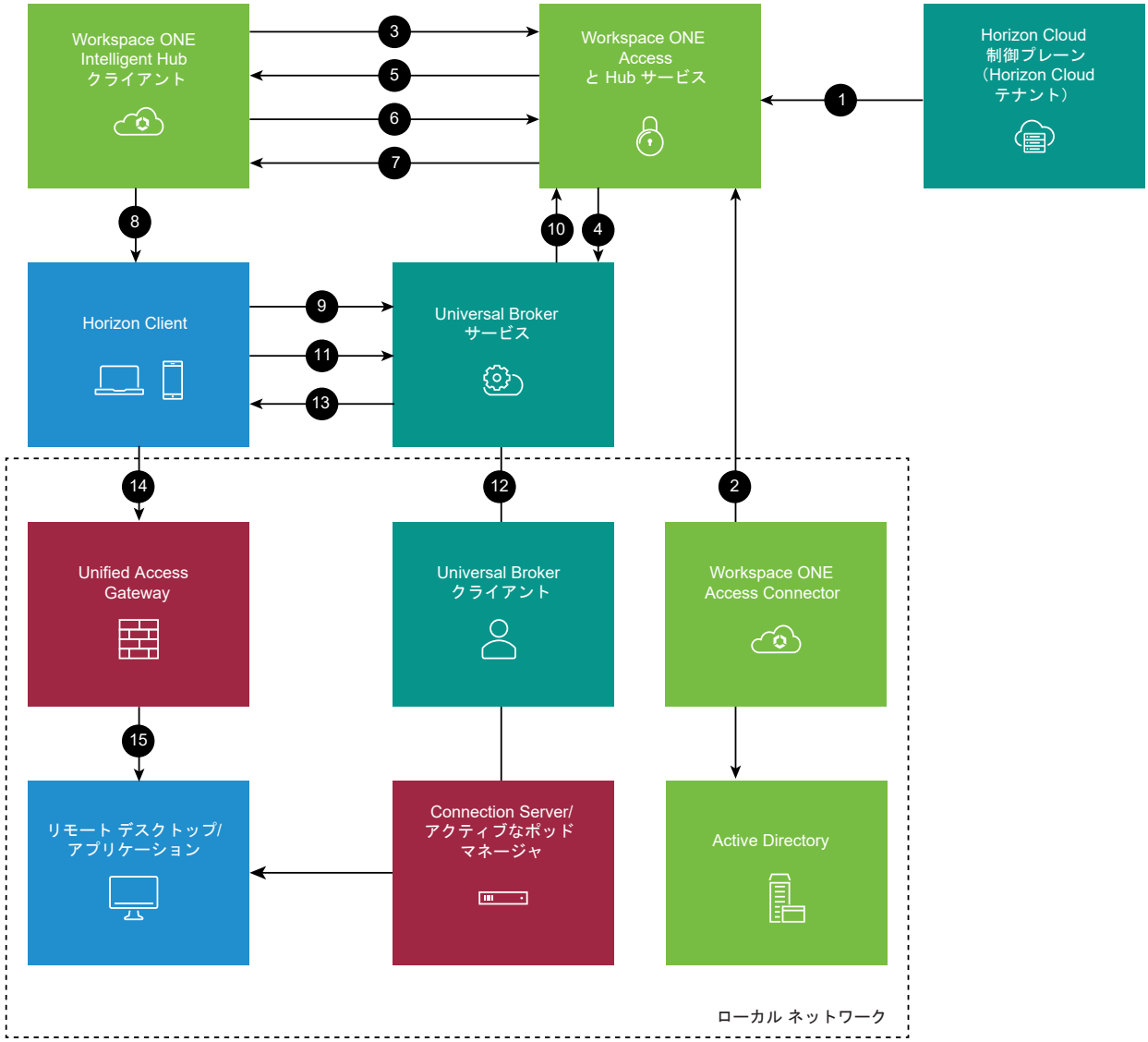
統合が正常に完了したことをシステムが識別すると、統合ワークフローが完了したことを示すバナー メッセージがコンソールに表示されます。

次のステップ

必要に応じて、Universal Broker を使用した第 1 世代の Horizon Cloud - ユーザー接続のための Intelligent Hub リダイレクトの構成の説明に従って、リダイレクト ポリシーを構成します。

Universal Broker による Horizon Cloud 環境 - Workspace ONE Access および Intelligent Hub サービスとの統合によるアーキテクチャ

次の図は、Universal Broker で構成され、Workspace ONE Access および Intelligent Hub サービスと統合された Horizon Cloud 環境のコンポーネントの高レベルのアーキテクチャと通信フローの概要を示しています。



1 アクティベーション ワークフローでは、Workspace ONE Access テナントは Horizon Cloud テナントと統合するために登録されます。

2 Workspace ONE Access Connector は、Workspace ONE Access テナントを Active Directory のユーザーおよびグループと同期します。

3 ユーザーは Workspace ONE Access 経由で認証を行い、Hub カタログのロードを要求します。

4 Workspace ONE Intelligent Hub サービスは、カタログの構成されたすべてのソースからユーザーの資格に関する情報を取得します。ソースには、Workspace ONE Access、Workspace ONE UEM、Okta、Universal Broker サービスを含めることができます。

5 Hub カタログは、資格の統合カタログをユーザーに提供します。カタログには、Universal Broker サービスから取得したユーザーの割り当て権限が含まれています。

6 カタログから、ユーザーは割り当てられたデスクトップまたはアプリケーションをクリックして、そのデスクトップまたはアプリケーションへの接続セッションを開始します。

7 Workspace ONE Intelligent Hub サービスは、Workspace ONE Access と通信して、Universal Broker URL に追加された SAML アーティファクトを生成することによって、割り当てられたリソースの開始 URL を準備します。その後、サービスは、Workspace ONE Intelligent Hub クライアントに開始 URL を送信します。

8 Workspace ONE Intelligent Hub クライアントは Horizon Client デスクトップまたは Web アプリケーションを起動します。

9 Horizon Client は、認証要求を Universal Broker サービスに転送します。

10 Workspace ONE Access との通信により、Universal Broker サービスは SAML アーティファクトを解決し、信頼されたユーザーを検証します。

11 Horizon Client は、割り当てられたデスクトップまたはアプリケーションを Universal Broker サービスから要求します。

12 割り当てられたリソースを最適に提供できるポッドを決定すると、Universal Broker サービスは、そのポッド内で実行される Universal Broker クライアントにメッセージを送信します。Universal Broker クライアントは、Connection Server（Horizon ポッドの場合）またはアクティブなポッド マネージャ（Microsoft Azure のポッドの場合）で実行されている Universal Broker プラグインにメッセージを転送します。Universal Broker プラグインまたはアクティブなポッド マネージャは、エンド ユーザーに割り当てるのに最適なリソースを識別します。

13 Universal Broker サービスは、ポッドの一意の FQDN を含む Horizon Client への接続応答を返します。一意の FQDN は、通常、Horizon ポッドのローカル ロード バランサまたは Microsoft Azure ロード バランサの FQDN です。

14 ロード バランサを通過すると、要求はポッドの Unified Access Gateway に送られます。Unified Access Gateway は、要求が信頼されていることを検証し、Blast Secure Gateway、PCoIP Secure Gateway、およびトンネル サーバを準備します。

15 ユーザーは指定のデスクトップやアプリケーションを受信し、構成されたセカンダリ プロトコル（Blast Extreme、PCoIP、または RDP）に基づいて接続セッションを確立します。

Workspace ONE Access を使用する Horizon Cloud - リモート アプリケーション アクセス クライアントの作成

既存の Workspace ONE Access テナントを、Universal Broker が有効になっている Horizon Cloud 環境に統合するには、最初にそのテナントにリモート アプリケーション アクセス クライアントを作成する必要があります。その後、リモート アプリケーション アクセス クライアントのクライアント ID と共有シークレット キーを使用して、統合ワークフローを完了することができます。

既存のテナントの Workspace ONE Access コンソールで、リモート アプリケーション アクセス クライアントを作成するための画面に移動し、次のように設定を構成します。

- アクセス タイプをサービス クライアント トークンとして設定します。

- クライアントの名前（クライアント ID とも呼ばれる）を入力します。統合ワークフローを完了するために必要なため、このクライアント ID をメモしておきます。
- クライアントの共有シークレット キーを生成します。統合ワークフローを完了するために必要なため、生成された共有シークレット キーをメモしておきます。

リモート アプリケーション アクセス機能については、Workspace ONE Access のドキュメントも参照してください。それらのドキュメント ページは VMware Workspace ONE Access ドキュメントです。ドキュメント ページの再設計中のため、ドキュメント ページへの直接リンクを提供できません。直接リンクはすぐに「404 ページが見つかりません」エラーに変わります。

Workspace ONE Access を使用する Horizon Cloud：Universal Broker が有効になっている Horizon Cloud テナントと統合するためのユーザー属性の構成

Universal Broker が有効になっている Horizon Cloud テナントと Workspace ONE Access テナントを統合するには、Workspace ONE Access コンソールにログインして、必要なユーザー属性を構成する必要があります。これらのユーザー属性の構成は、Workspace ONE Access コンソールの [ID とアクセス管理] 領域内の複数の領域を使用する複数のステップからなるプロセスです。

注： このドキュメント ページでは、ユーザーは Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合するに記載されている手順を実行しているため、このページを読んでいることを前提としています。このページの内容は、その他の状況やコンテキストには適用されません。

概要レベルでは、Workspace ONE Access コンソールで以下を実行します。

1 まず、[ID とアクセス管理] 領域の [セットアップ] 領域を使用して、この統合に必須の Workspace ONE Access 属性を追加します。

2 次に、[ID とアクセス管理] 領域の [管理] 領域を使用して、これらの必要な Workspace ONE Access 属性を Active Directory 属性に適切にマッピングします。

[userPrincipalName]、[objectGuid]、[sid]、および [netBios] の Workspace ONE Access 属性は必須であり、次の手順で説明するように適切な Active Directory 属性にマッピングする必要があります。

また、[sAMAccountName] は Workspace ONE Access ディレクトリのディレクトリ検索属性として設定する必要があります。Workspace ONE Access コンソールでディレクトリを作成するときに、ディレクトリ検索属性を指定します。

前提条件

Universal Broker と Workspace ONE Access の統合手順をサポートするために Workspace ONE Access コンソールでユーザー属性を構成するには、互換性のあるバージョンの Workspace ONE Access Connector をインストールし、それらの統合手順で説明されているように Active Directory とのディレクトリ統合を設定しておく必要があります。

本書の執筆時点では、そのページの手順 5 は、コネクタのインストールとディレクトリ統合が参照される関連ポイントです。

手順

1 管理者として Workspace ONE Access テナントのコンソールにログインします。

2 Workspace ONE Access コンソールの [ID とアクセス管理] 領域にある [セットアップ] 部分を使用して、Workspace ONE Access テナントのユーザー属性が構成されている画面に移動します。

[セットアップ] 領域で [ユーザー属性] というラベルを探します。

3 そのコンソールの Workspace ONE Access ユーザー属性を構成する画面で、デフォルト属性のリストをナビゲートし、ディレクトリに同期する他の属性を追加するためのセクションを見つけ、コンソールのボタンを使用して以下の属性を追加します。

重要： これらの属性では、[大文字と小文字が完全に区別されます]。

そのため、[objectGuid] は[小文字の uid] で入力し、大文字の **`uid`** を使用することは[できません]。

[netBios] は[小文字の ios] で入力し、大文字の **`ios`** を使用することは[できません]。

[大文字と小文字が完全に区別される性質]は、実装に関する技術的な事実です。

Workspace ONE 管理ユーザー インターフェイスでこれらの属性の[大文字と小文字が完全に区別される性質]に従わないと、Universal Broker から Workspace ONE Access 間の同期が解除され、ログインしているエンド ユーザーには表示されるべきデスクトップとアプリケーションが表示されません。

- [objectGuid]
- [sid]
- [netBios]

この統合には [userPrincipalName] も必須ですが、デフォルト属性のリストにすでに表示されているため、ここで追加する必要はないことに注意してください。

4 画面の変更内容を保存します。

5 Workspace ONE Access コンソールの [ID とアクセス管理] 領域の [管理] 領域を使用して、Workspace ONE Access 属性を Active Directory 属性にマッピングします。

a Workspace ONE Access コンソールの [ID とアクセス管理] 領域の [管理] 部分を使用して、ディレクトリが構成されている画面に移動し、Horizon Cloud の資格を持つユーザーとグループを含むディレクトリをクリックします。

b そのディレクトリの画面で、[同期設定] 画面を開き、[マップされた属性] ページに移動します。

c 表示されているとおりに、Workspace ONE Access ユーザー属性を Active Directory 属性にマッピングします。

重要： Workspace ONE Access の属性と Active Directory の属性がどのようにマッピングされるかに注意してください。名前は似ていますが、微妙に異なります。

上記の手順では、Workspace ONE Access の属性で[大文字と小文字が完全に区別される]ことに注意してください。

そのため、Workspace ONE Access の [objectGuid] は[小文字の uid] で入力し、大文字の **uid** を使用することは[できません]。

ただし、Workspace ONE Access で[小文字の uid] が使用されている [objectGuid] は、[大文字の UID] が使用されている Active Directory 属性にマッピングされることに注意してください。

Workspace ONE Access 属性	Active Directory 属性
[userPrincipalName]	[userPrincipalName]
[objectGuid]	[objectGUID]
[sid]	[objectSid]
[netBios]	[msDS-PrincipalName]

6 設定を保存します。

7 Horizon Cloud 環境に同期するすべてのユーザーとグループが選択されていることを確認します。

Workspace ONE Access コンソールで、ユーザーとグループのリストを表示および編集するには、ディレクトリの [同期設定] 画面から、[ユーザー] タブおよび [グループ] タブに移動します。

8 Workspace ONE Access コンソールで、そのディレクトリのページに戻り、[同期] をクリックして、ユーザーとグループを Workspace ONE Access に同期し、すべての正しいユーザー属性を使用します。

次のステップ

Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合するの手順に戻り、ユーザー アクセスの構成手順の後で残りの統合手順を完了します。

Workspace ONE Access を使用する Horizon Cloud - Horizon Cloud との統合のための Intelligent Hub の構成

エンド ユーザーが Hub ブラウザで 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るようにするには、Intelligent Hub の特定の設定を構成する必要があります。Hub ブラウザ エクスペリエンスを有効に

し、Workspace ONE Access テナントが Workspace ONE UEM と統合されている場合は、Hub カタログのソースとして Workspace ONE Access が選択されていることを確認します。

手順

1 管理者として Workspace ONE Access コンソールにログインします。

2 Hub ブラウザ エクスペリエンスを有効にします。

a [カタログ] - [Hub 構成] を選択し、[起動] をクリックして Hub サービス コンソールにアクセスします。

b 左側のペインの [システム設定] をクリックします。

c [Web エクスペリエンス] で、[Hub ブラウザ エクスペリエンスを有効にする] オプションを有効にします。

d [保存] をクリックします。

e 右上にある [Workspace ONE Access に戻る] をクリックして、Workspace ONE Access コンソールに戻ります。

注： Horizon Universal Console から作成された新しい Workspace ONE Access テナントでは、Hub ブラウザ エクスペリエンスがデフォルトで有効になっています。

3 Workspace ONE Access テナントが Workspace ONE UEM と統合されている場合は、Hub カタログのソースとして Workspace ONE Access が選択されていることを確認します。

a Workspace ONE Access コンソールで、[ID とアクセス管理] - [セットアップ] - [VMware Workspace ONE UEM] ページに移動します。

b [Workspace ONE Access カタログ] セクションで [Workspace ONE Access から取得] チェックボックスがオンになっていない場合は、オンにします。

c [保存] をクリックします。

Universal Broker を使用した第 1 世代の Horizon Cloud - ユーザー接続のための Intelligent Hub リダイレクトの構成

Intelligent Hub リダイレクトを有効にすると、Universal Broker FQDN またはポッド レベルの FQDN に直接接続しようとするユーザーは、Workspace ONE Intelligent Hub カタログに自動的に転送され、割り当てられたデスクトップおよびアプリケーションを使用できます。ユーザーが内部ネットワークと外部ネットワークのどちらから接続しているかに基づいて、異なるリダイレクト ポリシーを指定できます。

Horizon Cloud テナントを Workspace ONE Access および Intelligent Hub サービスと統合すると、デスクトップとアプリケーションの割り当てが Hub カタログに表示され、資格のあるユーザーが簡単かつ安全にアクセスできるようになります。ただし、特定のユーザーが Hub カタログ以外のポータルを介してこれらの割り当てにアクセスすることを制限する場合は、Intelligent Hub リダイレクトを構成する必要があります。

Intelligent Hub リダイレクトを有効にしない場合、ユーザーは Universal Broker FQDN に接続するか、Microsoft Azure の Horizon Cloud ポッドの Unified Access Gateway (UAG) の FQDN に直接接続して、割り当てにアクセスできます。Hub カタログを介した割り当てへのアクセスのみを適用する場合は、Intelligent Hub リダイレクトを有効にする必要があります。

Intelligent Hub リダイレクトを有効にすると、接続の試行に対して、内部ネットワークと外部ネットワークのどちらから接続するかに基づいて、異なるリダイレクト ポリシーを指定できます。たとえば、内部ユーザーに対して Hub カタログへのリダイレクトを適用する一方で、外部ユーザーがブローカ レベルまたはポッド レベルの FQDN を介して接続できるようにすることができます。

前提条件

システム環境が次の要件を満たしていることを確認します。

- Horizon 制御プレーン テナントの Universal Broker サービスのセットアップまたはシングル ポッド ブローカから Universal Broker への移行をスケジューリングして完了するの説明に従って、Universal Broker が有効にされ、テナントに対して構成されていること。
- Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合するの説明に従って、Horizon Cloud テナントが VMware Workspace ONE Access および Intelligent Hub サービスと統合されていること。統合が完全に完了していることを確認します。
- Microsoft Azure 内のすべての Horizon Cloud ポッドがオンラインで、準備完了の状態であること。
- VMware SDDC 内のすべての Horizon ポッドに、それぞれの Connection Server インスタンスに関連付けられた SAML 認証子があること。この構成は、Horizon ポッドの Intelligent Hub リダイレクトをサポートするために必要です。Horizon Console での SAML 認証子の構成を参照してください（必要に応じて記事の上部にあるメニューを使用し、Horizon バージョンを選択します）。

内部ユーザーと外部ユーザーに個別のリダイレクト ポリシーを構成するには、Universal Broker の内部ネットワーク範囲の定義で説明されている手順も実行する必要があります。

注目: テナントの Horizon 8 デプロイの場合、一部のエンド ユーザーは、Universal Broker FQDN に加えて、Horizon 8 デプロイの Horizon Connection Server および Unified Access Gateway インスタンスに対して直接 FQDN をすでに持っている場合があります。この状況では、これらのエンド ユーザーは、これらの FQDN のいずれかを使用して接続を試みる場合があります。

Horizon 8 ポッドの場合、Horizon Universal Console [ブローカ] - [認証] 設定は、Universal Broker FQDN の使用時にのみ、リダイレクトを強制します。

したがって、エンド ユーザーがどの FQDN に接続しようとしているかに関係なく、テナントの Horizon 8 ポッドにリダイレクトを強制する場合は、Horizon 8 の「Horizon Console での Workspace ONE Access ポリシーの設定」の手順を使用して、Horizon Console で特定の設定を追加で設定する必要があります。そのページで説明されているように、目標を達成するには、関連する SAML 認証子への認証委任を要求する設定を指定し、Workspace ONE ホスト名で Workspace ONE モードを有効にします。

手順

1 Horizon Universal Console で、[設定] - [ブローカ] の順に選択し、[認証] タブを選択します。

[認証] ページには、Intelligent Hub リダイレクト機能の現在の構成が表示されます。

2 Intelligent Hub リダイレクトの構成を変更するには、オプションの編集アイコンをクリックします。

構成を編集するためのコントロールを含むダイアログ ボックスが表示されます。

3 Intelligent Hub リダイレクトを有効にするには、[Intelligent Hub リダイレクトを適用] トグルを有効にします。

トグルを有効にすると、追加の構成設定が表示されます。

4 内部ネットワークと外部ネットワークのどちらから接続しているかに基づいてユーザーに対して異なるリダイレクト ポリシーを構成するには、[内部ユーザーと外部ユーザーに異なる Intelligent Hub リダイレクトを許可] トグルを有効にします。次に、チェック ボックスを使用して、各カテゴリのユーザーのリダイレクト ポリシーを指定します。

たとえば、内部ユーザーに対してリダイレクトを適用し、外部ユーザーのリダイレクトを無効にするには、[内部ユーザー] チェック ボックスをオンにし、[外部ユーザー] チェック ボックスをオフにします。これらのリダイレクト ポリシーは、ポッド レベル（ポッドの UAG または Connection Server インスタンスのアドレスを介して）とブローカ レベル（Universal Broker FQDN を介して）の両方での接続の試行に適用されます。

注： これらの設定を構成するには、まず内部ネットワークと外部ネットワークに対応する IP アドレス範囲を定義する必要があります。これらのネットワークをまだ構成していない場合は、表示されるリマインダ メッセージの [追加] リンクをクリックし、Universal Broker の内部ネットワーク範囲の定義の指示に従います。

5 [保存] をクリックして、変更を適用します。

結果

構成の変更が Universal Broker サービスと Horizon Cloud ポッド全体で有効になり、新しいリダイレクトの動作が完全に動作状態になるまでに、最大 15 分かかります。

注： Intelligent Hub リダイレクトが有効になっている場合、ユーザーは Hub カタログに転送されます。ここで、Universal Broker によって仲介された要求された Horizon Cloud ポッド リソースへのセッションを開くことができます。Universal Broker サービスが失敗すると、ユーザーは Horizon Cloud ポッド リソースにアクセスできなくなります。回避策として、Universal Broker サービスが復旧するまで Intelligent Hub リダイレクトを無効にすることで、個々のポッドの UAG インスタンスへのユーザー接続を一時的に許可できます。

Universal Broker による Horizon Cloud 環境 - Horizon Cloud Workspace ONE Access の統合の削除

このトピックでは、Workspace ONE Access テナントの現在の統合を削除する方法について説明します。統合を削除すると、そのテナントの Workspace ONE Intelligent Hub カタログに Horizon Cloud 割り当て資格が表示されなくなります。Horizon Cloud 割り当て以外のリソースに対する資格は、カタログ内で使用できます。

手順

1 Horizon Universal Console で、[設定] - [ブローカ] の順に選択し、[ID とアクセス] タブを選択します。

このアクションによって、ページには統合された Workspace ONE Access テナントの構成の詳細が表示されます。

2 テナント統合を削除するには、[削除] をクリックします。表示される確認メッセージで、[削除] をクリックします。

テナント統合が完全に削除されるまで、最大 30 分かかります。

統合は削除されますが、Workspace ONE Access テナントはそのまま残ります。ユーザーは引き続き Workspace ONE Access コンソールにアクセスでき、そのテナントの Hub カタログにアクセスすることができますが、カタログ内の Horizon Cloud 資格は表示されなくなります。

シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure の環境の Horizon Cloud ポッドと Workspace ONE Access の統合

この手順は、Horizon Cloud テナント環境がシングルポッド仲介を使用するように構成されていて、その環境で Workspace ONE Access を使用する場合に使用します。Horizon Cloud on Microsoft Azure デプロイをクラウドでホストされる Workspace ONE Access 環境と統合することにより、エンド ユーザーは、ポッドでプロビジョニングされた資格のあるデスクトップおよびアプリケーションを Workspace ONE Access の統合された単一のカタログから認証することができます。

Horizon Cloud は、クラウド ホスト型の Workspace ONE Access との統合をサポートします。

この統合を実現するには、Workspace ONE Access 環境とポッドをブリッジする Workspace ONE Access Connector をデプロイする必要があります。このコネクタを使用すると、エンド ユーザーの資格をポッドから Workspace ONE Access に同期することができます。

注： Workspace ONE Access ドキュメントのスクリーンショットは、特定の Workspace ONE Access 環境で見られるユーザー インターフェイス要素と異なるように見える可能性があります。

背景情報と用語

- ユーザーおよびグループに対してデスクトップおよびリモート アプリケーションの割り当てを通常どおり Horizon Universal Console で構成します。
- ポッドを Workspace ONE Access 環境と統合する手順を完了したら、ポッドの割り当て情報を Workspace ONE Access に同期します。
- これにより、デスクトップおよびアプリケーションが Workspace ONE Access 管理コンソールに表示され、エンド ユーザーが Workspace ONE Access から自分に割り当てられたリソースに認証できるようになります。
- 割り当て情報を Horizon Cloud から Workspace ONE Access 環境に同期する定期的な同期スケジュールを設定できます。
- Workspace ONE Access の以前の名前は VMware Identity Manager™ です。コネクタの以前の名前は VMware Identity Manager™ Connector です。特に古いコネクタ バージョンを使用している場合は、製品、ドキュメント、およびナレッジベースの記事に以前の名前が引き続き使用されていることがあります。
- Workspace ONE Access ドキュメントでは、ポッドから Workspace ONE Access へのコネクタの同期について説明するときは、資格という用語を使用します。

  Horizon Cloud では、割り当てはリソースと資格の組み合わせを表します。

Horizon Universal Console で、ユーザーを割り当てに追加すると、そのユーザーには、ポッドでプロビジョニングされた割り当てのリソースを使用する資格が付与されます。たとえば、専用の VDI デスクトップ割り当てを作成するときなどです。

- Workspace ONE Access コンソールが、Horizon Cloud コレクションという用語を使用するウィザードで更新されました。Workspace ONE Access ドキュメントと Horizon Cloud ドキュメント内で、仮想アプリケーションのコレクションと Horizon Cloud コレクションの両方のフレーズが表示されることがあります。

主要コンポーネントの概要

Horizon Cloud テナント環境がシングル ポッド仲介を使用するように構成されている場合は、Microsoft Azure の個々のポッドを Workspace ONE Access と統合して、各ポッドからプロビジョニングされたエンド ユーザー リソースを使用して Workspace ONE Access の機能を使用できるようにします。

Microsoft Azure のポッドと Workspace ONE Access との統合には、次の主要な概念が含まれます。

- Microsoft Azure にデプロイされたポッド
- Workspace ONE Access テナント環境
- ポッドのマネージャ仮想マシンにアップロードされた有効な SSL 証明書。この SSL 証明書により、Workspace ONE Access Connector は、Workspace ONE Access Connector が Workspace ONE Access で定義された Horizon Cloud 仮想アプリケーション コレクションの使用資格とポッド プロビジョニングされたリソースを同期するときに、ポッドへの接続を信頼できるようになります。
- Workspace ONE Access Connector がインストールされ、以下のリソースに関する情報を Workspace ONE Access に同期するように設定が行われています。
  - Active Directory のユーザーおよびグループ
  - ポッドの割り当て（ポッドでプロビジョニングされたリソースとこれらのリソースに対する資格）
- Workspace ONE Access がポッドとの SAML 通信を実行するのに必要な SAML アーティファクトを設定するための Horizon Universal Console の構成。

統合プロセスの概要

次の一覧は、エンド ユーザーが Workspace ONE Access を使用してポッドでプロビジョニングされたデスクトップおよびアプリケーションに認証できるようにするためのエンドツーエンド手順の大まかな概要です。

これらの手順を実行する前に、ポッドがすでに Microsoft Azure にデプロイされていること、Horizon Cloud 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こと、および Workspace ONE Access クラウド テナントがあることが必要です。

1 DNS サーバで、ポッド マネージャの Azure ロード バランサの IP アドレスを `mypod1.example.com` などの完全修飾ドメイン名 (FQDN) にマッピングします。ポッドの詳細ページで、IP アドレスを確認できます。ポッドの詳細ページ内でその IP アドレスを特定する場所については、Horizon Cloud ポッドのマネージャ仮想マシンでの SSL 証明書の構成の概要（主にシングルポッド ブローカ環境でポッドを使用する Workspace ONE Access Connector で使用）を参照してください。

注： 2020 年 7 月四半期より前のサービス リリースでは、この IP アドレスは、[テナント アプライアンスの IP アドレス] というラベルが付けられてポッドの詳細ページに表示されていました。現在のラベルは [ポッド マネージャ ロード バランサの IP アドレス] です。最新のマニフェストのポッドには、デフォルトでポッド マネージャ インスタンス用にデプロイされた Microsoft Azure ロード バランサが含まれているため、現在のラベルにはそのポッド アーキテクチャが反映されています。マニフェストのポッド（1,600 個未満）にポッド マネージャ仮想マシン用の Microsoft Azure ロード バランサがデプロイされていない場合でも、このペアリング タスクでは、ポッドの詳細ページの該当ラベルの横に表示される IP アドレスを使用する必要があります。

2 その FQDN に基づく信頼された SSL 証明書を取得します。必要な項目に関する詳細については、次のトピックを参照してください。

- Horizon Cloud ポッドのマネージャ仮想マシンでの SSL 証明書の構成の概要（主にシングルポッド ブローカ環境でポッドを使用する Workspace ONE Access Connector で使用）
- Horizon Universal Console コンソールの [ポッド証明書のアップロード] ワークフローを実行して、Horizon Cloud ポッドのマネージャ仮想マシンで SSL 証明書を構成するための前提条件

注： SSL 証明書をポッドにアップロードするために必要な証明書ファイルの形式は、ポッド ゲートウェイの構成で使用される PEM ファイル形式とは異なります。

3 コネクタがポッド マネージャ仮想マシンへの接続を信頼できるように、Workspace ONE Access コネクタ アプライアンスを Microsoft Azure の Horizon Cloud ポッドと統合する場合には、ポッド マネージャ仮想マシンで SSL 証明書を直接構成します。の説明に従って、その 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。

重要： 接続を試みる Workspace ONE Access Connector に提供するように説明どおりに構成された SSL 証明書がポッドにない場合、コネクタは信頼されていないネットワーク接続を確立しないため、使用資格とリソースを同期するためにポッドに接続しようとすると失敗します。ポッドに正常に接続するには、ポッドの SSL 証明書が Workspace ONE Access Connector によって信頼されている必要があります。基準を満たす SSL 証明書をポッドにアップロードするまでは、Workspace ONE Access とポッドを正常に統合することはできません。

4 Workspace ONE Access ポッドと Active Directory 環境の両方と通信できるネットワークに、Horizon Cloud Connector アプライアンスをデプロイします。コネクタの目的は、ポッドのリソースと資格を同期すること、および Active Directory 環境のユーザーとグループを同期することです。

コネクタに関連するすべての前提条件については、以下の「統合手順を開始する前に必要な事項」以降のセクションを参照してください。

重要： そのコネクタで構成した信頼性のあるタイム ソースがポッドで構成されている NTP サーバと一致することも確認する必要があります。タイム ソースが一致しない場合、同期の問題が発生する可能性があります。ポッドの詳細ページには、ポッドの構成済み NTP サーバが表示されます。ポッドの詳細ページは、Horizon Universal Console キャパシティ ページから開くことができます。

5 状況に適した Workspace ONE Access 製品ドキュメントの説明に従って、統合のための Workspace ONE Access 前提条件を満たしていることを確認します。以下の「統合手順を開始する前に必要な事項」というセクションを参照してください。

Workspace ONE Access ドキュメントの統合の前提条件ページを参照してください。

6 Workspace ONE Access 製品情報の説明に従って、Horizon Cloud 環境から Workspace ONE Access 環境へのデスクトップを有効にします。

Workspace ONE Access ドキュメントの VMware Workspace ONE Access での Horizon Cloud テナントの構成ページを参照してください。

Workspace ONE Access ドキュメントの手順に従う場合は、次の重要な点に注意してください。

- Workspace ONE Access アクセスのためのポッドを構成する下の手順 8 を完了するまでは、コレクションを同期しないでください。
- Horizon Cloud テナント情報を入力するための Workspace ONE Access 画面の [ホスト] フィールドに、DNS サーバでポッド マネージャの Azure ロード バランサ IP アドレスにマッピングした FQDN を指定して、ポッド マネージャ仮想マシンにアクセスします。

  この FQDN は、コネクタがポッド マネージャ仮想マシンへの接続を信頼できるように、Workspace ONE Access コネクタ アプライアンスを Microsoft Azure の Horizon Cloud ポッドと統合する場合には、ポッド マネージャ仮想マシンで SSL 証明書を直接構成します。の説明に従って、ポッドに直接アップロードした SSL 証明書と一致する必要があります。

7 構成済みの Workspace ONE Access 環境をポッドの ID 管理プロバイダとして使用できるようにする設定を入力します。シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure で関連する Workspace ONE Access テナント情報を使用して Horizon Cloud ポッドを構成する手順を参照してください。

8 Workspace ONE Access クラウド テナントで、コレクションを手動で同期して、次の手順で確認できるようにします。Workspace ONE Access 管理コンソールでコレクションを見つけて、[同期] をクリックします。

9 デスクトップおよびアプリケーションへの エンド ユーザー アクセスを確認するには、Workspace ONE Access にエンド ユーザーとしてログインし、カタログからデスクトップおよびアプリケーションを起動します。シングルポッド仲介を使用した Horizon Cloud 環境：エンド ユーザーによる Workspace ONE Access のデスクトップ割り当てへのアクセスの確認を参照してください。

統合が動作していることを確認したら、オプションでエンド ユーザーが Workspace ONE Access を経由してデスクトップおよびアプリケーションを認証し、アクセスするように強制できます。シングルポッド仲介を使用した Horizon Cloud 環境では、エンド ユーザーが Workspace ONE Access を使用して、使用資格が付与されたデスクトップやアプリケーションにアクセスすることを強制します。 を参照してください。

統合手順を開始する前に必要な事項

Workspace ONE Access を使用してポッドが提供するデスクトップまたは RDS ベースのリモート アプリケーションへのエンド ユーザー アクセスを検証する手順まで、統合プロセスをエンドツーエンドですべて完了するには、次の要件が整っていることを確認します。

- Horizon Cloud ポッドのマネージャ仮想マシンでの SSL 証明書の構成の概要（主にシングルポッド ブローカ環境でポッドを使用する Workspace ONE Access Connector で使用）および Horizon Universal Console コンソールの [ポッド証明書のアップロード] ワークフローを実行して、Horizon Cloud ポッドのマネージャ仮想マシンで SSL 証明書を構成するための前提条件に記載されているように、ポッド マネージャの Azure ロード バランサーの IP アドレスを完全修飾ドメイン名 (FQDN) にマッピングする DNS サーバのエントリが必要です。

  SSL 証明書で使用する FQDN を、[Pod Manager ロード バランサ IP] ラベルの横にある Horizon Universal Console のポッドの詳細ページに表示される IP アドレスに解決する必要があります。

  たとえば、下のスクリーンショットに示すポッドがあり、ポッドへの Workspace ONE Access 接続の目的で、そのポッドの FQDN として `mypod-a.example.com` という FQDN を使用するとします。

  この例では、DNS で、`mypod-a.example.com` を図に示された IP アドレス 192.168.21.4 にマッピングします。

  ```
  mypod-a.example.com    192.168.21.4
  ```

  Workspace ONE Access 画面で Horizon Cloud テナント情報を入力するための手順を実行するときに、その Workspace ONE Access 画面の [ホスト] フィールドにこの FQDN を指定します。

- ポッドの詳細ページを使用してポッド マネージャ自体にアップロードした、信頼できる有効な SSL 証明書を持つ完全に構成されたポッド。証明書のアップロードの詳細については、Horizon Cloud ポッドのマネージャ仮想マシンでの SSL 証明書の構成の概要（主にシングルポッド ブローカ環境でポッドを使用する Workspace ONE Access Connector で使用）を参照してください。
- ポッドに対して構成された VDI デスクトップ割り当て、セッション デスクトップ割り当て、またはリモート アプリケーション割り当て。
- 組織の構成済み Workspace ONE Access クラウド テナントへのアクセス。

  クラウドホスト型の Workspace ONE Access を使用する場合、ポッドをテナントと統合するには、Workspace ONE Access コネクタ アプライアンスが必要です。このコネクタは、ユーザーおよびグループ資格に関する情報を仮想デスクトップに送信し、アプリケーションを Workspace ONE Access テナントに送信します。Active Directory ネットワークに Workspace ONE Access コネクタ アプライアンスをインストールする必要があります。このドキュメント ページから入手可能 Workspace ONE Access Cloud のドキュメント、および Horizon Cloud を Workspace ONE Access と統合するためのデプロイ シナリオで説明されている手順に従います。今回のリリースで必要なコネクタのバージョンについては、https://www.vmware.com/resources/compatibility/sim/interop_matrix.php にある VMware 製品の相互運用性マトリックスを参照してください。

  コネクタで構成した信頼性のあるタイム ソースが、ポッドに対して構成されている NTP サーバと一致していることを確認します。

  注： 既存の統合および VMware Workspace ONE® Access™ コネクタ アプライアンスがある場合のベスト プラクティスは、ポッドをソフトウェア レベルの最新ポッドに更新する前に、コネクタを更新することです。

- Workspace ONE Access のドキュメント ページ統合の前提条件の説明に従って、構成されている Workspace ONE Access 環境が Horizon Cloud リソースとの統合の前提条件をすべて満たしていることを確認します。

シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure で関連する Workspace ONE Access テナント情報を使用して Horizon Cloud ポッドを構成する手順

Microsoft Azure のポッドを Workspace ONE Access に統合するには、適切な Workspace ONE Access 情報に基づいてポッドを設定する必要があります。この情報を構成するには、Horizon Universal Console を使用します。

前提条件

コネクタがポッド マネージャ仮想マシンへの接続を信頼できるように、Workspace ONE Access コネクタ アプライアンスを Microsoft Azure の Horizon Cloud ポッドと統合する場合には、ポッド マネージャ仮想マシンで SSL 証明書を直接構成します。の説明に従って、その FQDN に基づく SSL 証明書がポッド マネージャ仮想マシンにアップロードされていることを確認します。シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure の環境の Horizon Cloud ポッドと Workspace ONE Access の統合の手順 3 で説明するように、その SSL 証明書は、DNS サーバでポッド マネージャの Azure ロード バランサの IP アドレスにマッピングした FQDN に基づいている必要があります。

ポッドでプロビジョニングされたエンドユーザーのリソースと資格を Workspace ONE Access と同期するには、Workspace ONE Access 環境がその FQDN を使用するように設定されていることを確認します。

以下の情報があることを確認します。

- Workspace ONE Access テナントからの SAML ID プロバイダ (IdP) メタデータ URL。

  環境の SAML IdP メタデータ URL は、Workspace ONE Access 管理コンソールの [SAML メタデータ] を使用して取得します。

  Workspace ONE Access Cloud のドキュメント ページ Horizon Cloud テナントでの SAML 認証の構成 を参照してください。

  そのページの [ID プロバイダ (IdP) メタデータ] リンクをクリックすると、ブラウザのアドレス バーに URL が通常 `https://WS1AccessFQDN/SAAS/API/1.0/GET/metadata/idp.xml` の形式で表示されます。ここで *WS1AccessFQDN* は Workspace ONE Access 環境の完全修飾ドメイン名 (FQDN) です。

- Horizon Cloud に接続するためにエンドユーザーが接続先に指定する FQDN。

手順

1 Horizon Universal Console で、[設定] - [ID 管理] の順に移動し、[新規] をクリックします。

2 以下のオプションを構成します。

設定	説明
[VMware Workspace ONE Access メタデータの URL]	Workspace ONE Access テナントの SAML ID プロバイダ (IdP) メタデータ URL を入力します。このメタデータ URL は通常 `https://WS1AccessFQDN/SAAS/API/1.0/GET/metadata/idp.xml` の形式です。ここで *WS1AccessFQDN* は Workspace ONE Access 環境の FQDN です。
[SSO トークンのタイムアウト]	SSO トークンがタイムアウトになるまでの時間を分単位で入力します。あらかじめ入力されているシステムのデフォルト値はゼロ (0) です。
[場所]	場所の 1 つを選択し、[ポッド] ドロップダウンをフィルタして、その場所に関連付けられたポッドのセットを取得します。
[ポッド]	この構成を適用するポッドを選択します。
[データセンター]	ドロップダウン リストには、Horizon Cloud ポッドのマニフェスト バージョンに関連する数値が表示されます。デフォルトのままにします。

設定	説明
[クライアント アクセスの FQDN]	Horizon Cloud に接続するためにエンドユーザーが接続先に指定する FQDN を入力します。
[Workspace ONE のリダイレクト]	また、エンドユーザーが Workspace ONE Access を経由してアクセスするように設定している場合、これを [はい] に設定してエンドユーザーのクライアントを自動的にその Workspace ONE Access 環境にリダイレクトすることができます。エンドユーザーのアクセスが Workspace ONE Access を経由するように強制するオプションの設定については、シングルポッド仲介を使用した Horizon Cloud 環境では、エンド ユーザーが Workspace ONE Access を使用して、使用資格が付与されたデスクトップやアプリケーションにアクセスすることを強制します。 を参照してください。 自動リダイレクトを [はい] に設定した場合、エンドユーザー クライアントでクライアントが Horizon Cloud に接続しようとしたときに Workspace ONE Access を介して認証するように構成されていると、クライアントはポッドに統合されている Workspace ONE Access 環境に自動的にリダイレクトされます。 トグルを [いいえ] に設定すると、自動リダイレクトは有効になりません。 自動リダイレクトが有効になっておらず、強制アクセスが構成されている場合、クライアントは代わりに情報メッセージをユーザーに表示します。詳細については、シングルポッド仲介を使用した Horizon Cloud 環境では、エンド ユーザーが Workspace ONE Access を使用して、使用資格が付与されたデスクトップやアプリケーションにアクセスすることを強制します。 を参照してください。 **注：** Workspace ONE Access リダイレクトは、ここで設定されている ID 管理プロバイダの 1 つに対してのみ有効にできます。別の構成に対してすでに [はい] に設定されている場合、ここで [はい] に設定しようとするとエラー メッセージが表示されます。

3 [保存] をクリックします。

結果

緑色のステータスは、構成が成功したことを示します。

次のステップ

Workspace ONE Access クラウド テナントで、資格のあるデスクトップとアプリケーションを手動で同期します。Workspace ONE Access 管理コンソールで、この Horizon Cloud ポッドに定義されているコレクションを見つけて、[同期] をクリックします。

重要：

- Horizon Cloud でリソースまたは資格が変更されるたびに、同期を実行して変更を Workspace ONE Access に伝達する必要があります。
- そのコネクタで構成した信頼性のあるタイム ソースがポッドで構成されている NTP サーバと一致することも確認する必要があります。タイム ソースが一致しない場合、同期の問題が発生する可能性があります。ポッドの詳細ページには、ポッドの構成済み NTP サーバが表示されます。ポッドの詳細ページは、Horizon Universal Console キャパシティ ページから開くことができます。

シングルポッド仲介を使用した Horizon Cloud 環境：エンド ユーザーによる Workspace ONE Access のデスクトップ割り当てへのアクセスの確認

Workspace ONE Access 環境に Horizon Cloud 環境を統合した後、これらの手順に従って、エンド ユーザーがそれらの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リモート アクセスできることを確認することができます。

前提条件

次の項目が完了していることを確認します。

- シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure の環境の Horizon Cloud ポッドと Workspace ONE Access の統合 に記載されている統合プロセスに従って、ウィザードを完了します。
- シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure で関連する Workspace ONE Access テナント情報を使用して Horizon Cloud ポッドを構成する手順の手順を完了させます。
- エンド ユーザーが Workspace ONE Access 経由でデスクトップにアクセスするための方法を設定します。
- 資格のあるデスクトップが統合された Horizon Cloud ポッドから Workspace ONE Access 環境に同期されることを確認します。Workspace ONE Access 管理コンソールで、[仮想アプリケーションの構成] ページに移動し、Horizon Cloud コレクションを同期します。

手順

1 組織の Workspace ONE Access URL を使用して Workspace ONE Access にログインします。

2 資格のある Horizon Cloud デスクトップとリモート アプリケーションをポータルから起動します。

True SSO を Horizon Cloud 環境で使用するために構成する

Horizon Cloud 環境で Active Directory ドメインを登録し、環境を VMware Workspace ONE と統合した後、True SSO を構成することができます。True SSO は Workspace ONE Access との統合を行い、ユーザーが Windows オペレーティング システムに Active Directory 認証情報を入力することなく Horizon Cloud によって提供される仮想 Windows デスクトップおよびアプリケーションにシングル サインオン (SSO) できるようにする機能です。環境に True SSO が構成されている場合、エンドユーザーは、使用資格が付与されたデスクトップおよびアプリケーションにアクセスするために入力した Workspace ONE URL で認証されます。認証されたら、ユーザーは資格が付与されたデスクトップまたはアプリケーションを、Active Directory 認証情報を求められることなく、起動することができます。

重要： True SSO 構成は、テナント全体の構成です。True SSO 構成は、ポッド フリートのすべての Microsoft Azure の Horizon Cloud ポッドに適用されます。その結果、Horizon Cloud テナントで初めて True SSO を正常に構成した後で、自動ポッド デプロイ ウィザードを使用して追加の Horizon Cloud ポッドを Microsoft Azure サブスクリプションにデプロイすると、システムはそれらすべてのポッドに同じ True SSO 構成を送信し、それらのポッドに対して同じ True SSO 構成を検証しようとします。

環境で使用するように True SSO を構成することは、複数の手順によるプロセスです。概要レベルでは、手順は次のとおりです。

1 以下を実行して、True SSO を操作するために必要なインフラストラクチャを設定します。

   a Microsoft Windows Server 認証局 (CA) をエンタープライズ CA にするためにインストールおよび構成。このセクションの手順は、Microsoft Windows Server 2012 R2 の場合の手順です。この機能での使用がサポートされているその他の Microsoft Windows Server バージョンでは、同様の手順に従うことができます。

b 認証局 (CA) での証明書テンプレートの設定。

重要： True SSO テンプレートの名前には ASCII 文字のみを使用します。この既知の問題により、True SSO テンプレート名に 非 ASCII 文字または拡張 ASCII 文字が含まれていると Horizon Cloud 環境で True SSO を正しく設定できません。

c Horizon Universal Console の Active Directory ページからの Horizon Cloud ペアリング バンドルのダウンロード。ペアリング バンドルは、登録サーバを設定するときに使用されます。

d 登録サーバの設定。

重要： 登録サーバの設定後、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 名に記載されているとおりに登録サーバのポート要件が満たされていることを確認してください。

2 Horizon Universal Console の Active Directory ページに登録サーバの情報を追加します。

構成が完了すると、ユーザーが資格を持っているデスクトップおよびアプリケーションにユーザーをログインさせるために使用する一時的な証明書を、エンタープライズ CA と登録サーバが連携して発行します。Horizon Cloud ポッドは、登録サーバに対して資格が付与された特定のユーザーの証明書を求めます。登録サーバは要求された証明書を生成する CA に問い合わせて、Horizon Cloud ポッドに証明書を返します。

前提条件

True SSO を設定する前に、少なくとも 1 つの Workspace ONE Access 環境を Horizon Cloud 環境で構成する必要があります。ドキュメントのトピック 8 章 VMware Workspace ONE およびオプションの True SSO 機能を使用した Horizon Cloud 環境の使用についてを参照して、Horizon Cloud 環境の構成に適した統合手順を実行します。

結果

手順の完了後、環境が True SSO で構成されます。

Horizon Cloud - True SSO - Microsoft Windows Server システムを使用したエンタープライズ認証局の設定

True SSO 機能を使用するために必要な要素は、Microsoft 認証局 (CA) です。認証局 (CA) をまだ設定していない場合、Active Directory Certificate Services (AD CS) ロールを Microsoft Windows Server に追加し、Windows Server がエンタープライズ CA になるように構成する必要があります。この手順を実行するには、Service Manager ウィザードを使用します。

Microsoft 認証局 (CA) の標準的な設定手順を以下に示します。このトピックでは、ラボ環境で使用するのに適した簡単なフォームで手順を説明しますが、実際の本稼動システムでは業界のベスト プラクティスに従って認証局 (CA) を設定することをお勧めします。

認証局 (CA) の設定に関する詳細なガイダンスが必要な場合は、標準の Microsoft テクニカル リファレンスである『ステップ バイ ステップ ガイド - Active Directory 証明書サービス』および『ルート認証局のインストール』を参照してください。

注： このプロセスを説明するために、このトピックの具体的な手順は Windows Server 2012 R2 の使用に基づいています。その他の Windows Server システムでも同様の手順に従うことができます。登録サーバをこの CA をホストするシステムと同じシステムにインストールする場合は、登録サーバでサポートされている Windows Server のバージョンのいずれかを使用していることを確認してください。第 1 世代の Horizon Cloud - True SSO - 登録サーバの設定を参照してください。

手順

1 Server Manager ダッシュボードで、[ロールと機能の追加] をクリックしてウィザードを開き、[次へ] をクリックします。

2 [インストール タイプの選択] ページで、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、[次へ] をクリックします。

3 [サーバの選択] ページで、デフォルトの設定をそのまま使用して [次へ] をクリックします。

4 [サーバ ロール] ページで以下を実行します。

   a [Active Directory 証明書サービス] を選択します。

   b ダイアログで、[管理ツールを含める] を選択し（該当する場合）、[機能の追加] をクリックします。

   c [次へ] をクリックします。

5 [機能] ページで、[次へ] をクリックします。

6 [認証局 CS] ページで、[次へ] をクリックします。

7 [ロール サービス] ページで、認証局を選択し、[次へ] をクリックします。

8 [確認] ページで、[必要に応じて自動的にターゲット サーバを再起動する] を選択し、[インストール] をクリックします。

   インストールの進捗状況が表示されます。インストールが完了すると URL リンクが表示され、新しくインストールした認証局 (CA) をターゲット サーバ上で「Active Directory 証明書サービスの構成」として構成できます。

9 構成リンクをクリックして構成ウィザードを起動します。

10 [認証情報] ページで、エンタープライズ管理者グループからユーザー認証情報を入力し、[次へ] をクリックします。

11 [ロール サービス] ページで、認証局 (CA) を選択し、[次へ] をクリックします。

12 [セットアップ タイプ] ページで、[エンタープライズ CA] を選択し、[次へ] をクリックします。

13 [CA のタイプ] ページで、必要に応じて [ルート CA] または [下位 CA]（この例では [ルート CA]）を選択し、[次へ] をクリックします。

14 [プライベート キー] ページで [新しいプライベート キーを作成する] を選択し、[次へ] をクリックします。

15 [暗号化] ページに以下の情報を入力します。

フィールド	説明
暗号化サービス プロバイダ	RSA#Microsoft Software Key Storage Provider
キーの長さ	4096（または別の任意の長さ）
ハッシュ アルゴリズム	SHA256（または別の任意の SHA アルゴリズム）

16 [CA 名] ページで、任意の値に変更するか、デフォルトの設定をそのまま使用して [次へ] をクリックします。

17 [有効期間] ページで、必要な設定を行い [次へ] をクリックします。

18 [証明書データベース] ページで、[次へ] をクリックします。

19 [確認] ページで情報を確認し、[設定] をクリックします。

20 次のタスクを実行して、構成プロセスを完了します（コマンド プロンプトからすべてのコマンドを実行）。

a 非パーシステントの証明書の処理用に認証局 (CA) を構成します。

```
certutil -setreg DBFlags
+DBFLAGS_ENABLEVOLATILEREQUESTS
```

b オフラインの CRL エラーを無視するように認証局 (CA) を構成します。

```
certutil -setreg ca\CRLFlags
+CRLF_REVCHECK_IGNORE_OFFLINE
```

c 認証局 (CA) サービスを再起動します。

```
net stop certsvc
net start certsvc
```

21 Horizon Cloud - True SSO - CA での証明書テンプレートの設定の手順に従って、CA の証明書テンプレートを設定します。

Horizon Cloud - True SSO - CA での証明書テンプレートの設定

認証局 (CA) 上で証明書テンプレートを構成する必要があります。証明書テンプレートは、認証局 (CA) によって生成される証明書の基本です。

前提条件

Horizon Cloud - True SSO - Microsoft Windows Server システムを使用したエンタープライズ認証局の設定で説明する手順を実行します。

手順

1 新しいユニバーサル セキュリティ グループを作成します。

このグループを作成すると、ユーザーに代わって証明書を発行するために必要な権限を単一のセキュリティ グループに割り当てることができるようになります。VMware 登録サーバがインストールされているすべてのコンピュータは、このグループのメンバーになることによってそれらの権限を継承できます。

a [開始] をクリックし、**dsa.msc** と入力します。

[Active Directory ユーザーとコンピュータ] ウィンドウが表示されます。

b ツリーで、ドメイン コントローラの [ユーザー] フォルダを右クリックし、[新規 > グループ] を選択します。

[新規オブジェクト - グループ] ウィンドウが表示されます。

c [グループ名] フィールドで、新しいグループの名前を入力します。たとえば、「True SSO Enrollment Servers」などです。

d 次の値を設定します。

設定	値
グループのスコープ	ユニバーサル
グループ タイプ	セキュリティ

e [OK] をクリックします。

[Active Directory ユーザーとコンピュータ] ウィンドウのツリーに新しいグループが表示されます。

f グループを右クリックして、[プロパティ] を選択します。

g タブのメンバーで、登録サーバをインストールするすべてのコンピュータを追加し、[OK]をクリックします。

h 登録サーバをインストールするすべてのコンピュータを再起動します。

2 証明書テンプレートを構成します。

a [コントロール パネル > 管理ツール > 認証局] の順に選択します。

b ツリーで、ローカルの認証局 (CA) 名を展開します。

c [証明書テンプレート] フォルダを右クリックし、[管理] を選択します。

証明書テンプレート コンソールが表示されます。

d [スマートカード ログイン] テンプレートを右クリックし、[テンプレートの複製] を選択します。

[新規テンプレートのプロパティ] ウィンドウが表示されます。

e ウィンドウのタブに以下のように情報を入力します。

タブ	設定
[互換性]	■ [変更の結果を表示] チェック ボックスをオンにします。 ■ 認証局：Windows オペレーティング システムを選択します ■ 証明書受信者：Windows オペレーティング システムを選択します。
[全般]	**重要：** True SSO テンプレートの名前には ASCII 文字のみを使用します。この既知の問題により、True SSO テンプレート名に 非 ASCII 文字または拡張 ASCII 文字が含まれていると Horizon Cloud 環境で True SSO を正しく設定できません。 ■ [テンプレートの表示名] - 任意の名前。たとえば、「True SSO Template」などです。 ■ [テンプレート名] - 任意の名前。たとえば、「True SSO Template」などです。 ■ [有効期間] - 1 時間 ■ [更新期間] - 0 週間
[要求の処理]	■ [目的] - [署名とスマートカード ログイン] ■ [スマートカード証明書の自動更新の場合 . . .] チェック ボックスをオンにします。 ■ [登録時にユーザーにプロンプトを表示] ラジオ ボタンをオンにします。
[暗号化]	■ [プロバイダのカテゴリ] - [キー ストレージ プロバイダ] ■ [アルゴリズム名] - [RSA] ■ [キーの最小サイズ] - [2048] ■ [要求に使用可能な任意のプロバイダを使用できる...] ラジオ ボタンをオンにします。 ■ [要求ハッシュ] - [SHA256]
[サブジェクト名]	■ [この Active Directory 情報からビルド] ラジオ ボタンをオンにします。 ■ [サブジェクト名の形式] - [完全識別名 (DN)] ■ [ユーザー プリンシパル名 (UPN)] チェック ボックスをオンにします。
[サーバ]	[CA データベース内に証明書および要求を保存しない] チェック ボックスをオンにします。
[発行の要件]	■ [登録には以下が必要] - [認証された署名の数] を選択して **1** を入力。 ■ [署名に必要なポリシー タイプ] - [アプリケーション ポリシー] ■ [アプリケーション ポリシー] - [証明書要求エージェント] ■ [登録には以下が必要] - [有効な既存の証明書]
セキュリティ	上部のタブで、作成した新しいグループを選択します。次に、下部のタブでは、読み取りと登録権限に対して [許可] を選択します。

f [OK] をクリックします。

3 True SSO のテンプレートを発行します。

a [証明書テンプレート] フォルダをもう一度右クリックし、[新規 > 発行する証明書テンプレート] を選択します。

[証明書テンプレートを有効にする] ウィンドウが表示されます。

b [TrueSsoTemplate] を選択し、[OK] をクリックします。

4 登録エージェント テンプレートを発行します。

a [証明書テンプレート] フォルダをもう一度右クリックし、[新規 > 発行する証明書テンプレート] を選択します。

[証明書テンプレートを有効にする] ウィンドウが表示されます。

b 登録エージェント コンピュータを選択し、[OK] をクリックします。

注： このテンプレートには、前の手順で発行されたテンプレートと同じセキュリティ設定が必要です。

これで、認証局 (CA) は True SSO で使用するための適切な証明書テンプレートを使用して設定および構成されました。

5 Horizon Cloud - True SSO - Horizon Cloud ペアリング バンドルのダウンロードの手順に従って、Horizon Cloud ペアリング バンドルをダウンロードします。

Horizon Cloud - True SSO - Horizon Cloud ペアリング バンドルのダウンロード

True SSO の Horizon Cloud 環境を構成しているときに、登録サーバの設定手順を完了するためにこのペアリング バンドルが必要です。Horizon Universal Console の Active Directory ページから、ペアリング バンドルをダウンロードします。

重要： True SSO 構成は、テナント全体の構成です。True SSO 構成は、ポッド フリートのすべての Microsoft Azure の Horizon Cloud ポッドに適用されます。その結果、Horizon Cloud テナントで初めて True SSO を正常に構成した後で、自動ポッド デプロイ ウィザードを使用して追加の Horizon Cloud ポッドを Microsoft Azure サブスクリプションにデプロイすると、システムはそれらすべてのポッドに同じ True SSO 構成を送信し、それらのポッドに対して同じ True SSO 構成を検証しようとします。

ペアリング バンドルには、Horizon Cloud 環境で Microsoft Azure にデプロイされた Horizon Cloud ポッドのそれぞれに対する証明書ファイルが含まれています。True SSO を構成する対象となるポッドについては、それらのポッドの証明書ファイルを登録サーバにアップロードします。ポッドが 1 つの場合は、バンドルには CRT 形式の 1 つの証明書ファイルが含まれます。複数のポッドがある場合は、バンドルにはポッドごとに 1 つ、全部で複数の CRT ファイルが含まれています。各 CRT ファイルの名前は次の形式になります。

```
podID_truesso.crt
```

この *podID* には、ポッドの [サマリ] ページに表示されているポッドの ID が入ります。

手順

1 コンソールで、[設定] - [Active Directory] に移動します。

2 [True SSO の設定] 領域で、[ペアリング トークンのダウンロード] をクリックして `pairing_bundle.7z` ファイルを取得します。

3 その内容を抽出できる場所にファイルを保存します。

4 True SSO を構成する対象となるポッドについては、ポッドの CRT ファイルをペアリング バンドルから、登録サーバを設定するときに取得できる場所に抽出します。

   ペアリング バンドルには、環境内の各ポッドの証明書ファイルが含まれています。各 CRT ファイルの名前は、*podID*_truesso.crt の形式を取ります。この場合の *podID* はポッドの ID 値です。

5 第 1 世代の Horizon Cloud - True SSO - 登録サーバの設定の手順に従って、登録サーバをセットアップします。

第 1 世代の Horizon Cloud - True SSO - 登録サーバの設定

このドキュメント ページでは、第 1 世代の Horizon Cloud on Microsoft Azure デプロイで使用するために登録サーバを設定する方法について説明します。

登録サーバ (ES) は、True SSO のインフラストラクチャ設定の最後の手順として Windows Server マシンにインストールする Horizon Cloud on Microsoft Azure コンポーネントです。登録エージェント（コンピュータ）証明書をサーバにデプロイすることにより、この ES が登録エージェントとして機能し、ユーザーに代わって証明書を生成することを承認します。

注目: 第 1 世代テナントでフリート内に複数の Horizon Cloud on Microsoft Azure デプロイがある場合は、登録サーバを設定するときに、これらのデプロイのすべてのポッド マネージャ インスタンスから登録サーバにアクセスできることを確認する必要があります。そうしないと、最後のペアリング手順が失敗します（完了手順が失敗します）。

「True SSO を Horizon Cloud 環境で使用するために構成する」ページの重要な注意事項で説明されているように、True SSO 構成は、テナント全体の構成です。システムは、テナントのフリート内のすべてのポッドに同じ True SSO 構成を送信し、それらのすべてで同じ True SSO 構成を検証しようとします。ポッド A と連携するように登録サーバを立ち上げ、別の登録サーバを立ち上げて Pod-B と連携する場合は、それらの登録サーバの両方が Pod-A と Pod-B の両方からアクセスできる必要があります。

前提条件

Horizon Cloud - True SSO - Microsoft Windows Server システムを使用したエンタープライズ認証局の設定、Horizon Cloud - True SSO - CA での証明書テンプレートの設定、および Horizon Cloud - True SSO - Horizon Cloud ペアリング バンドルのダウンロード の手順を完了していることを確認します。

注： このページに記載されている手順の [証明書登録] ウィザードに適切な項目を表示するには、エンタープライズ CA を設定する必要があります。

登録サーバ ソフトウェアをインストールするシステムが、このインストールでサポートされているオペレーティング システム（Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 のいずれか）を実行していることを確認します。システムには、少なくとも 4 GB のメモリが必要です。

注： Windows Server 2022 の使用は、第 1 世代の Horizon Cloud on Microsoft Azure デプロイでの登録サーバの使用のサポートには適していません。

次の手順のラベルは、Windows Server 2016 システムでの手順の実行を反映しています。

手順

1 登録サーバをシステムにインストールします。

a My VMware サイトから登録サーバの `.exe` ファイルをダウンロードします。ファイル名は `VMware-HorizonCloud-TruessoEnrollmentServer-x86_64-7.3.0-xxxxx.exe` のようになります。

b システムが前述の前提条件を満たしていることを確認します。

c インストーラを実行し、ウィザードに従います。

2 登録サーバで、証明書スナップインを MMC (Microsoft 管理コンソール) に追加します。

a MMC を開き、[ファイル] - [スナップインの追加と削除] の順に選択します。

b [利用できるスナップイン] で [証明書] を選択し、[追加] をクリックします。

c [証明書スナップイン] ウィンドウで、[コンピュータ アカウント] を選択し、[次へ] をクリックします。

d [コンピュータの選択] ウィンドウで、デフォルトの [ローカル コンピュータ] を選択したままにして、[終了] をクリックします。

e [スナップインの追加と削除] ウィンドウに戻り、[OK] をクリックして証明書スナップインの追加を完了します。

3 この登録サーバに登録エージェント証明書をデプロイします。

a MMC で、前の手順で追加した [証明書 (ローカル コンピュータ)] を展開し、[個人] フォルダを右クリックして、[すべてのタスク > 新しい証明書の要求] を選択します。

[証明書登録] ウィザードが起動します。

b [証明書登録] ウィザードを続行し、[証明書の要求] 手順に達するまでデフォルト値を受け入れます。

c ウィザードの [証明書の要求] 手順で、[登録エージェント (コンピュータ)] チェック ボックスをオンにして、[登録] をクリックします。

d ウィザードを続行し、残りの手順のデフォルト値を受け入れて、最後の手順で [終了] をクリックします。

4 `pairing_bundle.7z` ファイルから抽出された、True SSO を構成する対象となるポッドの証明書 CRT ファイルをインポートします。

ペアリング バンドルには、環境内の各ポッドの証明書ファイルが含まれています。各 CRT ファイルの名前は、*`podID`*`_truesso.crt` の形式を取ります。この場合の *podID* はポッドの ID 値です。

a MMC で、[VMware Horizon View 登録サーバの信頼されたルート] フォルダの [証明書] サブフォルダを右クリックし、[すべてのタスク > インポート] を選択します。

b [証明書のインポート] ウィザードで、プロンプトに従って、`pairing_bundle.7z` バンドルから証明書ファイルを抽出した場所を参照します。

1 つのみのポッドがある場合は、バンドルに含まれている CRT ファイルは 1 つのみです。複数のポッドがある場合は、バンドルにはそれぞれのポッドの CRT ファイルが含まれています。

c 構成しているポッドの数に応じて、1 つまたは複数の証明書ファイルをインポートします。

d [次へ] をクリックし、[終了] をクリックします。

5 Horizon Cloud - True SSO - Horizon Cloud 環境の True SSO の構成を完了するで説明されている残りの構成の手順を完了します。

Horizon Cloud - True SSO - Horizon Cloud 環境の True SSO の構成を完了する

登録サーバが設定されたら、Horizon Universal Console の [Active Directory] ページに情報を入力します。

前提条件

前の手順第 1 世代の Horizon Cloud - True SSO - 登録サーバの設定を完了します。

ポッドのマネージャの仮想マシンと登録サーバのネットワーク トラフィックが、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 名に記載されているとおりにポートとプロトコルの要件を満たしていることを確認します。適切なポートでトラフィックが許可されない場合、登録サーバのペアリングは失敗します。

手順

1 コンソールで、[設定] - [Active Directory] に移動します。

2 True SSO の設定の横にある [追加] をクリックします。

[True SSO の設定] ダイアログが表示されます。

注： 登録サーバはすでに構成されているため、このダイアログの [ペアリング トークンのダウンロード] リンクは無視してかまいません。

3 登録サーバの完全修飾ドメイン名 (FQDN) を [プライマリ登録サーバ] フィールドに入力し、フィールドの横にある [ペアリングのテスト] ボタンをクリックします。

その他の必須フィールドには自動的に入力されます。

4 [保存] をクリックします

5 高可用性のためにセカンダリ登録サーバを構成するには、次の手順を実行します。

a 第 1 世代の Horizon Cloud - True SSO - 登録サーバの設定 に記載されたプロセスを 2 台目のマシンに対して繰り返します。

b True SSO の設定を編集し、[セカンダリ登録サーバ] フィールドに 2 番目の ES アドレスを追加して、ペアリングをテストします。

c もう一度設定を保存します。

結果

構成情報が [Active Directory] ページの [True SSO の設定] に表示されます。

重要： True SSO 構成は、テナント全体の構成です。True SSO 構成は、ポッド フリートのすべての Microsoft Azure の Horizon Cloud ポッドに適用されます。その結果、Horizon Cloud テナントで初めて True SSO を正常に構成した後で、自動ポッド デプロイ ウィザードを使用して追加の Horizon Cloud ポッドを Microsoft Azure サブスクリプションにデプロイすると、システムはそれらすべてのポッドに同じ True SSO 構成を送信し、それらのポッドに対して同じ True SSO 構成を検証しようとします。

Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた資格のあるデスクトップおよびリモート アプリケーションへのエンド ユーザーの接続

9

これらのトピックでは、Horizon Cloud ポッドによってプロビジョニングされた資格のあるデスクトップおよびリモート アプリケーションへのエンド ユーザーの接続に関連する領域についての情報を提供します。このようなポッドは、コンソールのポッド デプロイ ウィザードを使用して Horizon Cloud によって Microsoft Azure にデプロイされるポッド マネージャ ベースのポッドです。

PCOIP URL と、内部ゲートウェイ構成があるポッドを使用する場合

6 章 ユーザーの Horizon Cloud on Microsoft Azure 環境に説明されているように、Microsoft Azure の Horizon Cloud ポッドは、Unified Access Gateway インスタンスを使用して、内部ゲートウェイ構成とともに構成できます。内部ゲートウェイ タイプの場合、HTML Access（Blast プロトコル）が外部 URL をユーザーが指定した FQDN に構成していても、PCOIP URL は IP アドレスを代わりに使用します。この動作により、外部ゲートウェイ タイプと内部ゲートウェイ タイプの間に、PCOIP に関する相違が生じます。

- 外部ゲートウェイ タイプ：PCOIP URL は、外部ゲートウェイ構成のロード バランサ リソースのパブリック IP アドレスに設定されます。
- 内部ゲートウェイ タイプ：PCOIP URL は、最初に、DNS を使用して指定された FQDN を IP アドレスに解決することを試みて、次にその IP アドレスを PCOIP URL として使用します。PCOIP URL が指定された FQDN を解決できない場合、PCOIP URL は、内部ゲートウェイ構成の内部ロード バランサ リソースのプライベート IP アドレスを代わりに使用します。

現在、ご利用のネットワーク環境で、内部ゲートウェイ構成のロード バランサが、エンド ユーザーの接続試行の最初のエンドポイントではない可能性があります。例として、内部ゲートウェイ構成のロード バランサにリダイレクトするように設定した追加のエンドポイントまたはロード バランサがある場合があります。ポッドをデプロイまたは編集したときに、内部 Unified Access Gateway ゲートウェイ構成にアップロードした証明書によっては、その証明書がネットワーク セットアップの最初のエンドポイントの FQDN または IP アドレスと一致している可能性があります。おそらく、エンドユーザー クライアントがその最初のエンドポイントから開始してネットワーク環境にアクセスすることが想定されていました。ご利用のネットワーク環境がこの説明と一致する場合は、エンドユーザー クライアントは最初のエンドポイントとして内部ゲートウェイ構成のロード バランサではないエンドポイントに最初にアクセスすることになり、DNS マッピングによって、確実にエンドユーザー クライアントが提供された証明書に対して適切な認証を行うために一致する PCOIP URL が提供される必要があります。

次のトピックを参照してください。

- RDS デスクトップ セッションと RDS ベースのアプリケーション セッションのタイム ゾーン リダイレクトの有効化
- Microsoft Azure の Horizon Cloud ポッドによって提供されるデスクトップおよびリモート アプリケーションの複数モニタのサポート
- Horizon Cloud on Microsoft Azure - Microsoft Teams のメディア最適化のサポート
- デスクトップおよびアプリケーションへのアクセス

RDS デスクトップ セッションと RDS ベースのアプリケーション セッションのタイム ゾーン リダイレクトの有効化

ファームの RDSH 仮想マシンのタイム ゾーンとエンド ユーザーのタイム ゾーンが異なる場合、デフォルトでは、そのユーザーが RDS セッションベースのデスクトップに接続すると、デスクトップにはファームの RDSH 仮想マシンのタイム ゾーンの時間が表示されます。タイム ゾーン リダイレクト グループ ポリシー設定を有効にすることにより、セッションベースのデスクトップにローカル タイム ゾーンの時間を表示することができます。このポリシー設定はリモート アプリケーション セッションにも適用されます。

前提条件

- Active Directory サーバでグループ ポリシー管理機能が使用できることを確認します。

  グループ ポリシー管理コンソールを開く手順は、Windows 2012、Windows 2008、および Windows 2003 Active Directory の各バージョンによって異なります。お使いのオペレーティング システムのバージョン用の Windows オンライン ヘルプを参照してください。
- Horizon RDS ADMX ファイルが Active Directory に追加されていることを確認します。これらの手順の例については、VMware Horizon ドキュメントの『Horizon リモート デスクトップ機能と GPO』ガイドにある Active Directory への ADMX テンプレート ファイルの追加に関するコンテンツを参照してください。
- VMware Horizon ドキュメントの『Horizon リモート デスクトップ機能と GPO』ガイドで説明されている RDS デバイスおよびリソース リダイレクトのグループ ポリシー設定について理解しておきます。

手順

1. Active Directory サーバで、グループ ポリシー管理コンソールを開きます。
2. ドメインと [グループ ポリシー オブジェクト] を展開します。
3. グループ ポリシー設定用に作成した GPO を右クリックし、[編集] を選択します。
4. グループ ポリシー管理エディタで、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [Windows コンポーネント] - [リモート デスクトップ サービス] - [リモート デスクトップ セッション ホスト] - [デバイスとリソースのリダイレクト] の順に移動します。
5. [タイム ゾーン リダイレクトの許可] の設定を有効にします。

Microsoft Azure の Horizon Cloud ポッドによって提供されるデスクトップおよびリモート アプリケーションの複数モニタのサポート

このトピックでは、Microsoft Azure の Horizon Cloud ポッドによってプロビジョニングされた、エンド ユーザーに資格付与されたリソースで複数のモニターを使用するための特定のサポートについて説明します。

エンド ユーザーが使用する Horizon Client のモニタと画面解像度の使用に関する全般的かつ広範な詳細については、モニタと画面解像度を参照してください。

注： エンド ユーザーの環境内の変数の数が、ネットワークの状態、バンド幅の消費、ワークロードの強度などのグラフィカル ユーザー エクスペリエンスに影響を与える可能性があるため、テストを実施して、特定のビジネス要件を満たす最適な操作性、コスト、パフォーマンスの組み合わせを特定することが推奨されています。

次の表に示す構成は、オフィスの生産性アプリケーション、ブラウザのストリーミング メディア、インターネットの使用など、一般的なナレッジ ワーカーのワークロードに対するものです。エクスペリエンスは仮想マシンのサイズ、使用している表示プロトコル、画面解像度、ワークロード、およびその他の要因によって異なる場合があります。

表 9-1. RDSH 仮想マシンでサポートされる構成

仮想マシンのタイプ	グラフィックス	ワークロード	監視オプション
GPU を搭載していない RDSH 仮想マシン	Microsoft Hyper-V ディスプレイ アダプタ	基本、すなわち高度なグラフィックス機能や HD ビデオ再生を必要としない	単一の 4K ディスプレイ
GPU を搭載した NV シリーズ RDSH 仮想マシン	NVIDIA GRID GPU ドライバの詳細については、以下を参照してください。 ■ https://docs.microsoft.com/en-us/azure/virtual-machines/nv-series ■ https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/n-series-driver-setup	グラフィックスに負荷がかかる、または高度なグラフィックス機能を必要とする	単一の 4K ディスプレイ
GPU を搭載した NVv4 シリーズ RDSH 仮想マシン	AMD GPU ドライバの詳細については、以下を参照してください。 ■ https://docs.microsoft.com/en-us/azure/virtual-machines/nvv4-series ■ https://docs.microsoft.com/en-us/azure/virtual-machines/windows/n-series-amd-driver-setup	主に、3D アプリケーションなどのアプリケーション レンダリングに使用されます。	単一の 4K ディスプレイ

表 9-2. VDI デスクトップ仮想マシンでサポートされる構成

仮想マシンのタイプ	グラフィックス	ワークロード	監視オプション
GPU を搭載していない VDI デスクトップ仮想マシン	VMware ディスプレイ アダプタ **注：** このドライバは VMware ESX ディスプレイ ドライバではありません。 高度なグラフィックス機能には Microsoft ソフトウェア レンダリングが使用されます。	基本、すなわち高度なグラフィックス機能や HD ビデオ再生を必要としない	1 台の 2560x1440 ディスプレイ 2 台の 1920x1080 ディスプレイ
GPU を搭載した NV シリーズ VDI デスクトップ仮想マシン	NVIDIA GRID GPU ドライバの詳細については、以下を参照してください。 ■ https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/sizes-gpu#nv-series ■ https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/n-series-driver-setup	グラフィックスに負荷がかかる、または高度なグラフィックス機能を必要とする	最大 4 台の 4K ディスプレイ **注：** Microsoft NV シリーズの仮想マシンでは、VDI デスクトップに最大 4 つの 4K ディスプレイを使用できます。サポートされている解像度およびワークロードの推奨事項を確認するには、使用している GPU の NVIDIA GRID のドキュメントを参照してください。
GPU を搭載した NVv4 シリーズ VDI デスクトップ仮想マシン	AMD GPU ドライバの詳細については、以下を参照してください。 ■ https://docs.microsoft.com/en-us/azure/virtual-machines/nvv4-series ■ https://docs.microsoft.com/en-us/azure/virtual-machines/windows/n-series-amd-driver-setup	主に、3D アプリケーションなどのアプリケーション レンダリングに使用されます。	単一の 4K ディスプレイ **注：** 検証テストと AMD Radeon MI25 仕様に基づき、ここでは単一の 4K ディスプレイが推奨されます。サポートされている解像度およびワークロードの推奨事項を確認するには、使用している GPU の AMD Radeon Instinct MI25 のドキュメントを参照してください。

Horizon Cloud on Microsoft Azure - Microsoft Teams のメディア最適化のサポート

Horizon Cloud on Microsoft Azure 環境からプロビジョニングされた仮想デスクトップとリモート アプリケーションで、Microsoft Teams のメディア最適化のための Horizon リモート エクスペリエンス機能を使用できます。『Horizon リモート デスクトップ機能と GPO』ガイドで説明しているように、この機能により、Teams のメディア処理が仮想デスクトップではなくクライアント マシンで行われるようになります。

Horizon Cloud on Microsoft Azure 環境の場合、この機能を使用するには、ポッド マニフェスト 2298.0 以降と Horizon Agents Installer (HAI) バージョン 20.2 以降が必要です。2020 年 8 月 11 日の時点では、Horizon Client バージョン 2006 以降を使用して、これらのポッドからプロビジョニングされた仮想デスクトップでこの機能を使用できます。VMware Horizon のドキュメントにある『Horizon リモート デスクトップ機能と GPO』ガイドの情報を参照してください。

デスクトップおよびアプリケーションへのアクセス

デスクトップとアプリケーションの割り当てを作成すると、エンド ユーザーは、Horizon Client を使用するか、または Horizon HTML Access 機能を備えたブラウザを使用して、デスクトップとアプリケーションにアクセスすることができます。お使いの環境を VMware Workspace ONE® Access™ 環境と統合している場合、オプションでエンドユーザー アクセスをその環境を経由するように強制できます。

Horizon Client を使用したデスクトップまたは RDS ベースのリモート アプリケーションへのログイン

エンド ユーザーが Horizon Client を使用して Horizon Cloud に接続すると、割り当てられたデスクトップまたはリモート アプリケーションを使用できます。

次の手順では、Horizon Client を初めて使用して、Horizon Cloud ポッドで提供されるデスクトップに接続します。

重要： エンド ユーザーに URL リダイレクトを割り当てる場合は、URL コンテンツ リダイレクト機能を有効にして Horizon Client をインストールし、ユーザーがその機能を使用できるようにする必要があります。クライアントで URL コンテンツ リダイレクトを有効にするには、コマンドラインを使用してクライアントをインストールする必要があります。この領域について詳しく知るには、はじめに Horizon Client のドキュメントの次のトピックを参照してください。

- コマンド ラインからの Horizon Client for Windows のインストール
- Horizon Client の外部で開く URL リンクのクリック

前提条件

- VMware Horizon Clients に関する最新の情報を確認します。たとえば、Horizon Client の最新のサポート情報を VMware 製品の相互運用性マトリクス (https://www.vmware.com/resources/compatibility/sim/interop_matrix.php) で確認し、また、対応するドキュメントを Horizon Client のドキュメント ページ (https://docs.vmware.com/jp/VMware-Horizon-Client/index.html) で確認します。
- 組織の DNS 情報から、たとえば `desktops.mycorp.example.com` など、このポッドへのエンド ユーザー接続のためのドメイン名システム (DNS) で組織が関連付けている完全修飾ドメイン名 (FQDN) を取得します。

  たとえば、Microsoft Azure の Horizon Cloud ポッドがエンド ユーザー接続に Unified Access Gateway を使用するように構成されている場合、組織には、デプロイ ウィザードで指定した FQDN を、ポッドのデプロイ済みロード バランサの自動生成されたパブリック FQDN にマップする DNS CNAME または A レコードがあります。この自動生成されたパブリック FQDN の詳細については、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を参照してください。

- クライアント再試行の機能を実装している Horizon Client が、システムが基盤となるデスクトップ仮想マシンまたはファーム RDSH 仮想マシンをパワーオンする必要があるときに、接続を自動的に再試行するようにする場合は、Horizon Universal Console のブローカ ページで [クライアントが電源オフの仮想マシンを待機することを許可する] オプションを [はい] に設定します。Horizon Client for Windows および Horizon Client for Mac のバージョン 4.8 以降で、この機能が実装されています。

手順

1 Horizon Client を起動します。

2 クライアントで、新しいサーバを追加するオプションを選択します。

3 新しいサーバ構成で、エンド ユーザー接続の DNS に追加された名前（`desktops.mycorp.com` など）を入力します。

4 認証ダイアログ ボックスに Active Directory ユーザーの認証情報を入力します。

5 2 要素認証が構成されている場合は、プロンプトに従って 2 要素認証の認証情報を入力します。

6 資格のあるデスクトップおよびリモート アプリケーションの表示リストから、使用したいものに接続します。

基盤となるデスクトップ仮想マシンまたはファーム RDSH 仮想マシンがパワーオフされると、VDI デスクトップ割り当てまたはファームで構成された電源管理スケジュールによって、システムは接続要求に応答して仮想マシンのパワーオンを開始します。Horizon Client for Windows または Horizon Client for Mac のバージョン 4.8 以降を実行していて、テナント環境で [クライアントが電源オフの仮想マシンを待機することを許可する] オプションを [はい] に設定している場合、クライアントは、デスクトップの準備ができる時期と、それにかかる推定時間を説明するメッセージを表示します。

7 （オプション） 選択した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適用されるその他のオプションを構成するには、アイコンを右クリックして選択を行います。

ブラウザを使用したデスクトップおよび RDS ベースのリモート アプリケーションへのログイン

組織がそれらのリソースへのエンドユーザー接続用に構成した完全修飾ドメイン名（FQDN）にブラウザをポイントすることにより、ユーザーが資格を付与した Horizon Cloud 環境のリソースにアクセスできます。

次の手順では、ブラウザを使用して、ポッドで提供されるデスクトップを起動します。

注： VMware Workspace ONE® Access™ 環境との統合が構成されている場合、エンド ユーザーはその環境を使用して自分の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必要があることがあります。シングルポッド仲介を使用した Horizon Cloud 環境では、エンド ユーザーが Workspace ONE Access を使用して、使用資格が付与されたデスクトップやアプリケーションにアクセスすることを強制します。 を参照してください。

前提条件

- Horizon HTML Access に関する最新の情報を確認します。たとえば、Horizon HTML Access の最新のサポート情報を VMware 製品の相互運用性マトリクス (https://www.vmware.com/resources/compatibility/sim/interop_matrix.php) で確認し、また、対応するドキュメントを Horizon HTML Access のドキュメント ページ (https://docs.vmware.com/jp/VMware-Horizon-HTML-Access/index.html) で確認します。
- 組織の DNS 情報から、たとえば `desktops.mycorp.example.com` など、Microsoft Azure でこの Horizon Cloud ポッドへのエンド ユーザー接続のために、ドメイン名システム (DNS) で組織が関連付けている完全修飾ドメイン名 (FQDN) を取得します。

  たとえば、ポッドがエンドユーザー接続に Unified Access Gateway を使用するように構成されている場合、組織の DNS には、ゲートウェイで構成された FQDN を、Azure ロード バランサの自動生成されたパブリック FQDN にマッピングする CNAME レコードがあります。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を参照してください。
- システムが基盤となるデスクトップ仮想マシンまたは RDSH 仮想マシンの電源をオンにする必要がある場合に、エンドユーザーの Horizon HTML Access クライアントが自動的に接続を再試行するようにするには、[クライアントが電源オフの仮想マシンを待機することを許可する] オプションを [はい] に設定します。このオプションは Horizon Universal Console のブローカ ページにあります。バージョン 4.10 以降の Horizon HTML Access クライアントには、この機能が実装されています。
- VDI デスクトップ、セッション デスクトップまたはリモート アプリケーションが割り当てられているユーザーの認証情報があることを確認します。

手順

1. ブラウザを `https://<desktops-FQDN>` という形式の URL にポイントします。*desktops-FQDN* は、エンド ユーザー接続のために DNS に追加された完全修飾ドメイン名です。

   たとえば、会社の DNS に `myDesktops.example.com` の FQDN が関連付けられている場合は、ブラウザを `https://myDesktops.example.com` にポイントします。
2. デスクトップ割り当てを持つユーザーの認証情報を使用してログインします。

結果

ユーザーの割り当てを示すアイコンがブラウザに表示されます。ユーザーはそのアイコンをクリックして、デスクトップまたはアプリケーションを起動できます。

ファイルのリダイレクトを使用したリモート アプリケーションによるローカル ファイルへのアクセス

ファイルのリダイレクト機能を使用すると、指定のファイル タイプをサポートする資格のあるリモート アプリケーションでローカル ファイルを開くことができます。

この機能は、Horizon Client で [[ホスト対象アプリケーションでローカル ファイルを開く]] オプションが選択されている場合に有効になります。

この機能によって、ユーザーは次の操作を実行できます。

- クライアント マシンでファイルをダブルクリックするか、右クリックして [[このアプリケーションで開く]] を選択し、メニューからリモート アプリケーションを選択して、リモート アプリケーションでローカル ファイルを開く。
- リモート アプリケーションで、ファイルが存在する完全なフォルダを参照する。
- リモート アプリケーションで行った変更をローカル クライアント ディスクに保存する。
- 資格のあるアプリケーションをアプリケーションが開くことができるファイル タイプのファイル ハンドラとして登録するか、一度だけリモート アプリケーションを使用して開くことを選択する。

  アプリケーションをデフォルトのハンドラとして設定した場合：

  - ファイルのプレビュー アイコンが、アプリケーション ランチャ ページでの資格のあるアプリケーションのアイコンと一致します。
  - ファイル タイプの説明は、リモート アプリケーションによってオーバーライドされます（存在する場合）。
  - そのタイプのファイルをダブルクリックすると、Horizon Client が起動します。

Universal Broker を使用した Horizon Cloud 環境では、エンド ユーザーが Workspace ONE Intelligent Hub を使用して、使用資格が付与されたデスクトップやアプリケーションにアクセスすることを強制します。

これらの手順は、Horizon Cloud 環境が Universal Broker 用に構成されていて、Horizon Cloud を Workspace ONE Access テナントに統合している場合に適用されます。Horizon Cloud には、エンド ユーザーがポッドでプロビジョニングされた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 Workspace ONE Intelligent Hub カタログを経由する必要があることを指定するための機能が用意されています。エンド ユーザーに Hub カタログを使用してデスクトップにアクセスするように要求することにより、Horizon Client または HTML Access を使用してデスクトップに直接アクセスすることができなくなります。この強制は、Workspace ONE テナント環境で設定されている 2 要素認証方法を使用する場合に有用です。

環境が Universal Broker で構成されている場合、エンド ユーザーは通常、次の方法を使用して資格のあるデスクトップを起動します。

- ブラウザから、エンド ユーザー アクセス用の Universal Broker URL をロードします。この URL は Horizon Universal Console の [ブローカ] ページに表示されます。
- Horizon Client アプリケーションから、その Universal Broker URL をクライアント アプリケーションの新しいサーバの場所として含める。
- Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合する の説明に従って、環境を統合している場合は Workspace ONE Hub カタログから。

Horizon Universal Console では、オプションで、エンド ユーザーが Workspace ONE Hub カタログのみを使用するように Horizon Cloud 環境を設定することができます。

前提条件

Universal Broker および Workspace ONE Access テナントで構成された Horizon Cloud が正常に統合されていることを確認します。Universal Broker を使用した Horizon Cloud 環境 - テナントを Workspace ONE Access および Intelligent Hub サービスと統合するを参照してください。

手順

1 コンソールで、[設定] - [ブローカ] - [認証] の順に移動します。

2 [Intelligent Hub を適用] トグルを有効にして、選択内容を確認します。

次のステップ

デスクトップ アクセスが設定に応じて動作することを確認するには、Workspace ONE Hub カタログからではなく、Horizon Client または直接ブラウザを使用してデスクトップにアクセスしてください。

シングルポッド仲介を使用した Horizon Cloud 環境では、エンド ユーザーが Workspace ONE Access を使用して、使用資格が付与されたデスクトップやアプリケーションにアクセスすることを強制します。

これらの手順は、Horizon Cloud 環境がシングルポッド仲介用に構成されており、Workspace ONE Access 環境を Microsoft Azure のポッドと統合している場合に適用されます。Horizon Cloud には、エンド ユーザーがポッドでプロビジョニングされた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 Workspace ONE Access を経由する必要があることを指定するための機能が用意されています。エンド ユーザーに Workspace ONE Access を使用してデスクトップにアクセスするように要求することにより、Horizon Client または HTML Access を使用してデスクトップに直接アクセスすることができなくなります。この強制は、Workspace ONE Access 環境で設定されている 2 要素認証方法を使用する場合に有用です。

エンド ユーザーは通常、次の方法を使用して資格のあるデスクトップを起動します。

- ブラウザから、組織の DNS レコードがアクセスが必要なポッドに関連付けたエンド ユーザー アクセス用の FQDN をロードする。
- Horizon Client アプリケーションから、その FQDN をクライアント アプリケーションの新しいサーバの場所として含める。
- Workspace ONE Access から（シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure の環境の Horizon Cloud ポッドと Workspace ONE Access の統合の説明に従って、環境を統合している場合）。

Horizon Universal Console では、オプションで、エンド ユーザーが Workspace ONE Access のみを使用するように Horizon Cloud 環境を設定することができます。企業のネットワーク外の場所からデスクトップおよびアプリケーションにアクセスしているユーザー、または企業のネットワーク内からアクセスしているユーザー、あるいはその両方に対し、強制を設定できます。強制が有効なときに自動的に Workspace ONE Access にリダイレクトするようにクライアントを設定することもできます。

Workspace ONE Access へのエンドユーザー アクセスを強制する機能は、次のように Workspace ONE Access リダイレクト機能と連携して動作します。

Workspace ONE Access 設定を介したエンドユーザー アクセスの強制	Workspace ONE Access リダイレクトの設定	エンドユーザーのクライアントが Horizon Cloud に接続して自分のデスクトップとアプリケーションにアクセスした場合の動作
有効（はい）	有効（はい）	クライアントは Workspace ONE Access に自動的にリダイレクトされる。
有効（はい）	無効（いいえ）	クライアントは Workspace ONE Access を介して Horizon Cloud にアクセスしなければならないことをユーザーに通知するメッセージを表示する。自動リダイレクトは発生しない。
無効（いいえ）	有効（はい）	クライアントはエンドユーザーがログインするための Horizon Cloud ログイン画面を表示する。Workspace ONE Access への強制アクセスが有効になっていないため、自動リダイレクトは発生しない。
無効（いいえ）	無効（いいえ）	クライアントはエンドユーザーがログインするための Horizon Cloud ログイン画面を表示する。このシナリオでは、強制アクセスと自動リダイレクト機能の両方が無効になっている。

前提条件

Horizon Cloud 環境および Workspace ONE Access 環境が正しく統合されていることを確認します。シングルポッド仲介を使用した Horizon Cloud 環境：Microsoft Azure の環境の Horizon Cloud ポッドと Workspace ONE Access の統合を参照してください。

手順

1 コンソールで、[設定] - [ID 管理] に移動し、[構成] をクリックします。

2 ダイアログ ボックスで、組織のニーズに合わせて選択を行います。

オプション	説明
[リモート ユーザー を]Workspace ONE Access に強制的に登録	[はい] に設定すると、企業のネットワーク外の場所からデスクトップにアクセスしようとしているユーザーは Workspace ONE Access にログインし、そこからデスクトップにアクセスする必要があります。
[内部ユーザーを]Workspace ONE Access に強制的に登録	[はい] に設定すると、企業のネットワーク内の場所からデスクトップにアクセスしようとしているユーザーは Workspace ONE Access にログインし、そこからデスクトップにアクセスする必要があります。

3 [保存] をクリックして、その設定をシステムに確認します。

4 （オプション） ID 管理の構成で Workspace ONE Access のリダイレクトを設定します。

注： Workspace ONE Access リダイレクトは [ID 管理] ページで設定されているいずれか 1 つの ID 管理 URL に対してのみ有効にできます。[ID 管理] ページに ID 管理 URL が異なる複数の設定がリストされていて、その 1 つが [はい] に設定されている場合、別の ID 管理 URL の設定を [はい] にするとエラー メッセージが表示されます。

a [ID 管理] ページで、リダイレクトを設定する Workspace ONE Access 設定のチェックボックスをオンにし、[編集] をクリックして設定を開きます。

b [Workspace One のリダイレクト] を [はい] に設定します。

c [保存] をクリックします。

次のステップ

デスクトップ アクセスが設定に応じて動作することを確認するには、Workspace ONE Access からではなく、Horizon Client または直接ブラウザを使用してデスクトップにアクセスしてください。

Horizon Cloud 環境の管理者向けトラブルシューティング

10

Horizon Cloud 環境での継続的な操作で発生する可能性のある問題をトラブルシューティングすることができます。

次のトピックを参照してください。

- Horizon Cloud - Horizon Universal Console を使用したエージェント ログの収集
- ファームまたは VDI デスクトップ割り当てのディスク サイズが増加した場合に必要な管理者のアクション
- Horizon Universal Console の最初のログイン画面で正常にログインできない
- ログに記録された Microsoft Windows Sysprep エラーを解決した後でも、イメージへの変換タスクがタイムアウト エラーで失敗する
- Windows Server 2012 イメージの場合に、イメージ タスクへの変換がタイムアウト エラーで失敗する
- プライマリ ドメイン バインド アカウントがロックアウトされているときの通知
- 新しいファームが進行中のままになる
- フローティング VDI デスクトップ割り当てからデスクトップへの接続を試みると Windows のエラー メッセージが表示される
- True SSO が構成され、ユーザーに証明書の失効ステータスに関するメッセージが表示される場合
- ポッドがマニフェスト 1230 以降に更新されていないときに、インポートしたイメージにリモート接続するためのドメイン アカウントの機能を設定する方法

Horizon Cloud - Horizon Universal Console を使用したエージェント ログの収集

この機能が Horizon Cloud テナントで有効になっていて、Microsoft Azure の Horizon Cloud ポッドが特定の前提条件を満たしている場合、[ログの生成] アクションは、Horizon Universal Console でそのポッドからのインポートされた仮想マシン、ファーム ホスト仮想マシン、および VDI デスクトップ仮想マシンに対して使用できます。

この機能は通常、テクニカル サポート リクエスト (SR) を発行した後にのみ使用され、その SR に応答する過程で、割り当てられたサポート チームは、問題を診断するために特定の仮想マシンからの診断ログ バンドルが必要であると判断しました。DCT バンドル（データ収集ツール バンドル）という用語は、このタイプのログ バンドルに関連して、VMware サポート チームによって頻繁に使用されます。

注意: クラウドベースの Horizon Universal Console のツアーで説明されているように、第 1 世代のコンソールは動的であり、第 1 世代のテナント環境の最新の構成に適した機能を反映しています。このドキュメントで説明されている機能へのアクセスは、以下の要因（ただしこれらに限定されない）に依存する場合があります。

- その機能が最新の第 1 世代の Horizon Cloud ポッド マニフェスト、Horizon ポッドのバージョン、または Horizon Cloud Connector のバージョンでのみ使用可能なシステム コードに依存するかどうか。
- 機能が初登場したときに、リリース ノートに記載されているように制限付きで機能へのアクセスが提供されるかどうか。
- 機能に特定のライセンスまたは SKU が必要かどうか。

このドキュメントに機能の記載があり、第 1 世代のコンソールにその機能が表示されない場合は、まずリリース ノートを読み、その機能のアクセスが制限されているかどうか、およびテナントで有効化をリクエストする方法について確認します。または、このドキュメントに記載されている機能を使用する資格があり、コンソールにその機能が表示されない場合は、VMware Horizon Cloud Service の担当者に問い合わせるか、担当者がいない場合は Customer Connect でサポート リクエストを発行する方法 (VMware KB 2006985)の記載内容に従って、サービス リクエストを Horizon Cloud Service チームに発行することができます。

前提条件と要件

ポッド関連の要件

この機能は、ポッド マニフェスト 2747.0 以降を実行している Microsoft Azure の Horizon Cloud ポッドでサポートされています。

この機能を使用するには、ポッドに `staging` タイプのファイル共有が必要です。これは、Microsoft Azure の Horizon Cloud ポッドの App Volumes 機能で使用するために Horizon Cloud によって構成されます。[ログの生成] アクションを実行すると、システムはその `staging` ファイル共有内のディレクトリにログ バンドルを書き込み、後でコンソールの [レポート] ページを使用して取得できるようにします。特定のポッドにこのファイル共有が存在することを確認するには、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移動します。ポッドの詳細ページの [ファイル共有] フィールドは、ポッドのファイル共有が存在することを示します。これは「2」である必要があります。表示されたハイパーリンク「2」をクリックし、情報ツールチップに `staging` タイプのファイル共有に関する情報が含まれていることを確認します。ツールチップにこの `staging` タイプのファイル共有が存在することが示されていない場合、[ログの生成] アクションは、VMware サポートに問い合わせるよう指示するメッセージを生成します。

仮想マシン関連の要件

[ログの生成] アクションは、インポートされた仮想マシン、ファーム ホスト仮想マシン、および VDI デスクトップ仮想マシンの仮想マシン タイプに対して提供されます。インポートされた仮想マシンの場合、その仮想マシンで [ログの生成] アクションを実行する前に、仮想マシンがペアリング プロセスを完了している必要があります。ペアリング プロセスについては、Microsoft Azure に Horizon Cloud ポッドのデスクトップ イメージを作成のペアリング手順を参照してください。

この機能によってログを取得できる仮想マシンの Horizon Agent の最小バージョンはバージョン 19.1 です。ただし、特定のポッド マニフェストは、特定のエージェント バージョンのセットとのみ相互運用できることに注意してください。仮想マシン内のエージェント バージョンがポッドのマニフェスト バージョンと互換性があることを常に確認する必要があります。ポッドとエージェントの相互運用性の概念については、Horizon Cloud ポッドの更新：エージェントの互換性とサポートを継続するための手順を参照してください。

仮想マシンで [ログの生成] アクションを呼び出すときは、仮想マシンのエージェントが実行中で、接続可能である必要があります。コンソールには、仮想マシンのエージェント ステータスとして アクティブ と表示されている必要があります。

生成されたログ バンドルについて

生成されたログ バンドルには、Horizon Agents Installer によってインストールされ、仮想マシンで [ログの生成] アクションが呼び出されるときに仮想マシンにインストールされているすべてのエージェントのログが含まれます。

[ログの生成] アクションが仮想マシンで呼び出されると、システム タスクがバックグラウンドで実行を開始し、ログ バンドルを生成および収集します。このバックグラウンド タスクは、完了するまでに少し時間がかかります。コンソールの [アクティビティ] ページには、タスクの進行状況が表示され、タスクがいつ 100% 完了するかを示します。また、バンドルをダウンロードする準備が完了するとコンソールに通知が作成されます。バンドルの準備ができたら、[レポート] ページの [ログ] タブを使用して、ファイルをローカル システムにダウンロードします。

ログ収集タスクが仮想マシンで完了した後、バックグラウンド タスクは、エージェント関連のログ バンドルをポッドの Microsoft Azure サブスクリプション内の `staging` ファイル共有（Horizon Cloud が App Volumes 機能で使用するために構成するファイル共有）にコピーします。ログ バンドルの平均サイズは 900 MB で、2 GB 近くになることがあります。

そのファイル共有で使用されるスペースを最小限に抑えるために、生成された各ログ バンドルには 1 時間の保持時間があり、保持時間を過ぎるとシステムはファイルを削除します。[レポート] ページの [ログ] タブには、生成された各ログ バンドルの有効期限が報告されます。

エージェント ログ バンドルの生成とダウンロード

1 目的の仮想マシンで [ログの生成] アクションを使用します。

2 コンソールの [アクティビティ] ページをチェックして、ログ バンドルを生成するアクティビティがいつ完了するかを確認します。

3 [レポート] - [ログ] からログ バンドル ファイルをローカル システムにダウンロードします。

`staging` ファイル共有のスペースを節約するため、[削除] アクションを使用して、有効期限が切れる前にバンドルを削除できます。

ファームまたは VDI デスクトップ割り当てのディスク サイズが増加した場合に必要な管理者のアクション

ファームまたは VDI デスクトップ割り当てを作成または編集するときに、OS のディスク サイズの値を増やすことができます。このオプションを使用すると、そのファームまたは割り当て内の各仮想マシンの OS ディスクが指定したサイズで作成されます。ただし、Microsoft Azure での仮想マシンのデフォルト動作の結果として、仮想マシン

のディスクが拡張されている場合でも、C ドライブを含むパーティションはディスク全体に拡張されません。仮想マシンのディスク上の新しい領域は、仮想マシンで操作を実行して、新しい領域を含むように C ドライブのパーティションを拡張するまで使用されません。

Microsoft では、パーティションを拡張してフル ディスクをカバーする方法をいくつか提供しています。次の Powershell コマンドは VMware によってテストされていません。これは、スクリプトを使用して拡張を実現できる方法の一例としてのみ提供されます。組織に最も適した方法を決定する必要があります。

```
$size = (Get-PartitionSupportedSize -DiskNumber 0 -PartitionNumber 2)
Resize-Partition -DiskNumber 0 -PartitionNumber 2 -Size $size.SizeMax
```

この例では、ディスク番号が 0 で、パーティション番号が 2 であると想定しています。これらの Powershell コマンドの詳細については、https://docs.microsoft.com/en-us/powershell/module/storage/resize-partition?view=win10-ps を参照してください。

Horizon Universal Console の最初のログイン画面で正常にログインできない

VMware Cloud services がメンテナンス中の場合、Horizon Cloud の管理コンソールにログインできません。

問題

https://cloud.horizon.vmware.com で Horizon Cloud にログインしようとすると、https://console.cloud.vmware.com の VMware Cloud Services のログインにリダイレクトされるように設計されています。ログイン画面には理由が示されていませんが、ログイン画面で有効なアカウント認証情報を入力すると、試行が失敗することがわかります。

原因

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を利用しています。そのサービスが必要な認証要求を完了できない場合、その期間中にコンソールにログインすると失敗します。

解決方法

- コンソールのメイン 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.workspaceone.com/) で Horizon Cloud 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。

ログに記録された Microsoft Windows Sysprep エラーを解決した後でも、イメージへの変換タスクがタイムアウト エラーで失敗する

イメージ仮想マシンの公開イメージへの変換時に、Microsoft Sysprep の問題の発生を防止する手順を実行した場合でも、その後の試行で変換タスクがタイムアウトになります。

問題

初めてイメージを公開しようとすると、[アクティビティ] ページには、appx パッケージに関連する Microsoft Sysprep の問題が原因で、イメージの変換プロセスがタイムアウト エラーで失敗したと表示されます。インポートされた仮想マシンの Windows オペレーティング システムをカスタマイズに記述されている最適化手順に従い、Microsoft Sysprep エラー ログに記述されている問題を解決した後、イメージを変換します。この 2 回目の試行で、[アクティビティ] ページには、「仮想マシンがパワーオフするまで 20 分待機しました。イメージを変換して仮想マシンに戻します (Waited 20 minutes for virtual machine to power off: Convert the image back to the virtual machine)」と表示されます。

原因

この状況は、Microsoft Sysprep プロセスを実行しようとする 2 回目の試行がハングするか応答しないために発生します。この問題を回避するには、次の手順を実行します。

解決方法

1 Microsoft Sysprep エラー ログのエラー メッセージおよび Microsoft KB 2769827 に従って Microsoft Sysprep の問題を確実に解決します。

2 イメージ仮想マシンで、VMware Horizon Agent サービスを調べ、起動タイプが [自動] に設定されていることを確認します。

   イメージが 1600 より前のマニフェストのポッドに配置されている場合、仮想マシンには VMware DaaS Agent サービスもあります。VMware DaaS Agent サービスの起動タイプが [自動] に設定されていることを確認します。

3 イメージ仮想マシンを再起動します。

4 再起動した仮想マシンで変換処理を再試行します。

Windows Server 2012 イメージの場合に、イメージ タスクへの変換がタイムアウト エラーで失敗する

公開ワークフローを実行する前に Windows Server 2012 イメージ仮想マシンをカスタマイズするためにアプリケーションをインストールした後、20 分後にタイムアウトのエラー メッセージで公開プロセスが失敗することがあります。

問題

Windows Server 2012 のイメージ仮想マシンにアプリケーションをインストールし、仮想マシンをログオフしてから公開ワークフローを開始した後に、Microsoft System Preparation (Sysprep) プロセスは実行中でありながら仮想マシンがパワーオフになりワークフローが失敗することがあります。

解決方法

1 Sysprep エラー ログのエラー メッセージおよび Microsoft KB 2769827 に従って Sysprep の問題を確実に解決します。

2 イメージ仮想マシンで、VMware Horizon Agent サービスを調べ、起動タイプが [自動] に設定されていることを確認します。

   イメージが 1600 より前のマニフェストのポッドに配置されている場合、仮想マシンには VMware DaaS Agent サービスもあります。VMware DaaS Agent サービスの起動タイプが [自動] に設定されていることを確認します。

3 仮想マシンを再起動します。

4 再起動した仮想マシンで変換処理を再試行します。

プライマリ ドメイン バインド アカウントがロックアウトされているときの通知

ロックされているプライマリ ドメイン バインド アカウントが原因で Horizon Cloud が認証エラーを検出すると、アカウントの状態を解決することを促すアラート通知が管理コンソールに表示されます。システムはプライマリ ドメイン バインド アカウントをサービス アカウントとして使用して、Active Directory (AD) サーバに接続し、Active Directory にクエリを行います。

管理者がコンソールに正常にログインするたびに、システムは、プライマリ ドメイン バインド アカウントが失敗した状態または非アクティブの状態であるかチェックします。システムによってアカウントが失敗した状態または非アクティブの状態であると判断されると、通知が作成されます。通知が作成されると [通知] ページに追加され、コンソールの右上隅にあるベル アイコンのカウントに反映されます（  ）。ベル アイコンをクリックするか、[通知] ページに移動することで、通知の詳細を確認することができます。

注： システムと Active Directory サーバ間の接続の接続状態は、15 分間キャッシュされます。このため、プライマリ ドメイン バインド アカウントがロックアウトの状態になってからコンソールに通知が反映されるまで、最大 15 分かかる場合があります。たとえば、コンソールにログインして、Active Directory サーバでプライマリ ドメイン バインド アカウントを手動でロックアウトする場合、通知がコンソールに表示されるのに最大で 15 分かかる場合があります。同様に、コンソールにロックアウト通知が表示されているときに Active Directory サーバでアカウントを修正する場合、その修正後最大 15 分間にアカウントのロックアウト通知がコンソールに表示され続ける可能性があります。

プライマリ ドメイン バインド アカウントがロックアウトになると、システムは Active Directory サーバへの接続を認証するためにフォールバックしてアクティブな構成済みの補助ドメイン バインド アカウントを使用します。プライマリ ドメイン バインド アカウントがロックアウトされているという通知が表示された場合、長い時間にわたり確実に正常なシステム接続が継続するように、プライマリ ドメイン バインド アカウントの状態を解決する必要があります。

新しいファームが進行中のままになる

[ファーム] ページから新しいファームの作成を開始すると、システムはファームとその RDSH 仮想マシン (VM) の作成を開始します。しかし、30 分経過してもページにはファームのステータスが進行中として表示されます。ファームの詳細ページにドリルダウンすると、その仮想マシンの 1 つがオフライン状態になっています。

問題

ファーム内の他の仮想マシンの状態がオンラインと表示されていても、1 台の仮想マシンがオフラインと表示され続けている場合、ファームの作成プロセスは完了できません。

原因

一時的なネットワークの切断が発生すると、仮想マシンの状態が Horizon Cloud でオフラインとして表示され、ファームの作成ワークフローは完了できません。

解決方法

1 ファームの [セッション ホスト] タブに移動します。

2 オフラインの仮想マシンの横にあるチェック ボックスをオンにして、[削除] をクリックします。

システムによって仮想マシンが削除されます。数分後に、システムは自動的に仮想マシンを再作成し、サーバ仮想マシンがオンラインになることでファームがオンライン状態に変わります。

フローティング VDI デスクトップ割り当てからデスクトップへの接続を試みると Windows のエラー メッセージが表示される

エンド ユーザーがフローティング VDI デスクトップ割り当てからデスクトップに接続しようとすると、「`Windows はシステム イベント通知サービスに接続できませんでした。システム管理者に連絡してください`」という Windows メッセージが表示されます。

問題

ユーザーがこのメッセージを確認して、表示されている [OK] ボタンをクリックすると、セッションは切断されます。[OK] をクリックした後も、ユーザーがデスクトップにログインできる場合があります。通常、[OK] をクリックした後は、ユーザーはデスクトップへのログインを再び試みることが可能であり、2 回目の試みは成功します。

原因

この問題は、既知の Microsoft Windows の問題であり、answers.microsoft.com のこのページに記載されています。

True SSO が構成され、ユーザーに証明書の失効ステータスに関するメッセージが表示される場合

True SSO が構成されていて、CRL が正しくない場合、ログイン中にエラー メッセージが表示されます。

問題

デスクトップ起動時のエンド ユーザーの画面に、「ログインの試行は無効です。ユーザー名または認証情報が正しくありません。認証に使用した証明書の失効ステータスを判別できませんでした」というメッセージが表示されます。

原因

True SSO が構成されている場合、CRL URL エンドポイントに問題があると、この問題が発生することがあります。

解決方法

ブラウザを使用して CRL URL に直接アクセスして、構成された CRL が正しいことを検証します。True SSO で認証するときに作成された証明書で、構成された CRL を確認できます。このアクセスが失敗した場合は、URL が正しいこと、およびその失効リストを提供しているサーバが動作しており、正しく機能していることを確認します。

ポッドがマニフェスト 1230 以降に更新されていないときに、インポートしたイメージにリモート接続するためのドメイン アカウントの機能を設定する方法

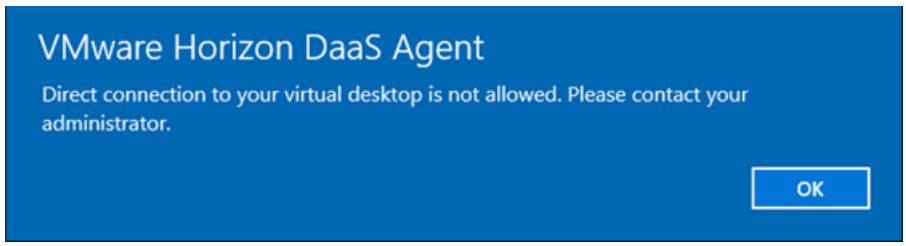
Microsoft Azure のポッドに使用するポッド マニフェスト バージョン 1230 以降では、ドメイン アカウントはエージェント ソフトウェアがインストールされているイメージ仮想マシンに直接接続できます。ポッド マニフェスト 1230 より前のバージョンでは、ドメインに参加した仮想マシンにインストールされたエージェント ソフトウェアにより、ドメイン アカウントをその仮想マシンに直接接続できませんでした。ポッドのマニフェスト 1230 以降、ドメイン アカウントを使用してログインし、イメージ仮想マシンをカスタマイズできます。ただし、ポッドのマニフェストが 1230 より前のバージョンでも、以下の手順を使用して、インポートしたイメージにリモート接続するためのドメイン アカウントの機能を設定することができます。

組織のニーズに応じてイメージをカスタマイズするには、Microsoft Azure にあるイメージの仮想マシンにリモートで接続してログインできる必要があります。イメージ仮想マシンが Active Directory ドメインに参加していて、組織のポリシーがドメインに参加した仮想マシンでローカル管理者アカウントを使用することを禁止している場合、イメージのカスタマイズに使用するドメイン アカウントを使用して DaaS Direct Connect Users ローカル グループを構成するまで、イメージ仮想マシンにログインすることはできません。

Microsoft Azure のイメージ仮想マシンに接続するには、Remote Desktop Protocol (RDP) ソフトウェアを使用します。イメージ仮想マシンを作成する全体的なプロセスの一環として、以下のアイテムが配置されます。

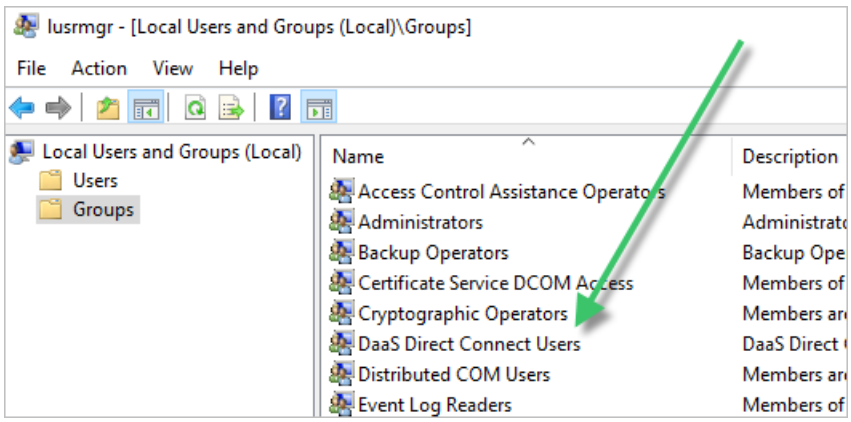
- 仮想マシンは、2019 年 12 月のサービス リリースより前に [仮想マシンのインポート] ウィザードを使用して作成された場合、常にドメインに参加します。また仮想マシンは、手動で作成して明示的にドメインに参加させることによって、あるいは 2019 年 12 月のサービス リリース後に [仮想マシンのインポート] ウィザードを使用して作成し、ドメインに参加するためのウィザード オプションを選択することによって、ドメインに参加します。2019 年 12 月のサービス リリースより前は、[仮想マシンのインポート] ウィザードは常に自動的に仮想マシンをドメインに参加させていました。
- Horizon Agent ソフトウェアは、仮想マシンの Microsoft Windows オペレーティング システムにインストールされます。

デフォルトでは、エージェント ソフトウェアは、エージェント ソフトウェアがインストールされた仮想マシンのローカル管理者アカウント以外のアカウントが仮想マシンのゲスト Microsoft Windows システムに対して RDP を実行することを許可しません。たとえば、ローカル管理者グループのメンバーであるドメイン管理者アカウントを使用してイメージ仮想マシンに対して RDP を実行しようとすると、最初に接続が行われても、Microsoft Windows セッションの開始時にメッセージが表示されます。メッセージには、仮想デスクトップへの直接接続が許可されないことが示されます。



ただし、一部の組織には通常、ドメインに参加した仮想マシン上でローカル管理者アカウントが使用されるのを禁止するポリシーがあります。RDP を実行してログインし、イメージ仮想マシンをカスタマイズする機能をドメイン アカウントに提供するため、エージェント ソフトウェアをインストールするときには DaaS 直接接続ユーザーという名前のローカル グループも作成されます。このグループにはローカル管理権限がありません。エージェントは、このグループのドメイン アカウントが直接 RDP 接続を使用してデスクトップに接続することを許可します。DaaS 直接接続ユーザー グループは作成時には空です。イメージをカスタマイズするために使用するドメイン アカウントに RDP 機能を提供するには、それらのドメイン ユーザーを DaaS Direct Connect Users ローカル グループに追加します。

次のスクリーンショットは、[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したイメージ仮想マシンの [ローカル ユーザーとグループ] ウィンドウに DaaS Direct Connect Users グループを表示した例です。



ローカル管理者アカウントを使用して仮想マシンに直接接続できない場合は、Active Directory 環境で Group Policy Object (GPO) ポリシーを使用して DaaS Direct Connect Users グループにドメイン アカウントを追加します。次の手順では、ドメインに参加した仮想マシンの DaaS Direct Connect Users グループにメンバーを追加するための GPO ポリシーの「制限付きグループ - Members Of」メソッドの使用方法について説明します。

1 Active Directory 環境で、新しい GPO を作成します。

2 GPO を右クリックして、[編集] を選択します。

3 グループ ポリシー管理エディタで、[コンピュータの構成] - [ポリシー] - [Windows 設定] - [セキュリティ設定] - [制限付きグループ] の順に移動します。

4 [制限付きグループ] を右クリックして、[グループの追加] を選択します。

5 [グループの追加] ダイアログで、DaaS 直接接続ユーザーを入力し、[OK] をクリックします。

6 プロパティ ダイアログで、[このグループのメンバー] 領域とその [追加] ボタンを使用して、イメージ仮想マシンに接続できるようにするドメイン アカウントを追加します。

7 [このグループのメンバー] 領域へのアカウントの追加が完了したら、[OK] をクリックしてプロパティ ダイアログを閉じます。

8 グループ ポリシー管理エディタとグループ ポリシー管理コンソールを終了します。

9 新しく作成した GPO を、イメージ仮想マシンに使用されているのと同じドメインにリンクします。

新しい GPO がドメインにリンクされたら、それらの指定されたドメイン アカウントの 1 つを使用してイメージ仮想マシンに対して RDP を実行し、カスタマイズすることができます。インポートされた仮想マシンの Windows オペレーティング システムをカスタマイズおよびそのサブトピックに記載されている手順に従います。

リビジョン履歴 - 変更ログ - Horizon Cloud のテナント環境とオンボーディングされたポッドの管理

11

このドキュメントのトピックでは、『Horizon Cloud のテナント環境とオンボーディングされたポッドの管理』への大幅な変更の履歴について説明します。

注： 2019 年 12 月 12 日以降にガイドのトピックに加えられた実質的かつ重要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。

2024 年 4 月

リビジョン	説明
2024 年 4 月 3 日	ユーザー インターフェイスのフィードバック アイコンの使用に関する参照を削除しました。そのアイコンと機能が第 1 世代 Horizon Universal Console から削除されたためです。

2024 年 1 月

リビジョン	説明
2024 年 1 月 9 日	アプライアンスでカスタム CA 署名証明書を構成した場合の Horizon Cloud Connector の更新に関して、これらのページの一部を更新しました。 ■ Horizon Cloud Connector 仮想アプライアンスの手動更新 ■ Horizon Cloud Connector 仮想アプライアンスの自動更新の構成

2023 年 11 月

リビジョン	説明
2023 年 11 月 14 日	2023 年 11 月の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「新機能」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	2023 年 10 月の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「新機能」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 1 月

リビジョン	説明
2022 年 1 月 11 日	Horizon Cloud リリース ノートの 2023 年 1 月の「更新」セクションに応じて新機能を更新しました。

2022 年 12 月

リビジョン	説明
2022 年 05 月 12 日	IT 組織が Azure Marketplace オファーの使用やマーケットプレイスでの購入に関する制限がある場合に実行する手順を説明する新しいドキュメント ページ (IT またはセキュリティ組織で、Horizon Cloud on Microsoft Azure 環境のサブスクリプションでの Azure Marketplace オファーの使用またはマーケットプレイスでの購入に制限がある場合、または環境で Azure China を使用している場合) を追加しました。

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。 また、既知の問題により、Horizon Cloud ポッドのゲートウェイ構成の Syslog 設定に対するコンソールの機能への以前の参照が削除されました。Horizon Cloud ポッドのゲートウェイ構成に関する既知の問題の既知の問題を参照してください。

2022 年 9 月

リビジョン	説明
2022 年 9 月 12 日	デプロイされたゲートウェイ構成と高可用性に関する情報を追加して Horizon Cloud on Microsoft Azure 環境の高可用性の特性 ページを更新しました。

2022 年 8 月

リビジョン	説明
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 `monitor.horizon.vmware.com` の行を追加しました。

2022 年 5 月 26 日

リビジョン	説明
2022 年 5 月 26 日	Universal Broker 機能に関する考慮事項と既知の制限ページに、2 要素認証を構成すると、エンド ユーザーは、Universal Broker 認証フローで Windows Active Directory 認証情報を 2 回入力するように求められるという情報を追加しました。

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 4 月 7 日	Universal Broker と Workspace ONE Access の統合のために Workspace ONE Access コンソールで必要なユーザー属性について説明するページを改訂し、属性の大文字と小文字が区別されることを明確にしました。 ■ Workspace ONE Access を使用する Horizon Cloud : Universal Broker が有効になっている Horizon Cloud テナントと統合するためのユーザー属性の構成

2022 年 3 月

リビジョン	説明
2022 年 3 月 28 日	Cloud Monitoring Service (CMS) の紹介ページを改訂し、一部の CMS 要件を更新して明確にしました。 ■ 2 章 第 1 世代のテナント - 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
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	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る、というガイダンスを提供する重要な注意事項を追加しました。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。 次のトピックに注意事項が追加されました。 ■ Microsoft Azure でのデスクトップ イメージと Horizon Cloud ポッドの作成 ■ 構成済みイメージ仮想マシンを割り当て可能なイメージに変換する
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 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 27 日

リビジョン	説明
2021 年 7 月 27 日	[役割と許可] ページに、Horizon Cloud のロールに割り当てることができる一意の Active Directory グループの最大数に関する記述を追加しました。更新されたトピックは Active Directory グループの個人が Horizon Cloud テナント環境に対して認証された後、その個人に対して Horizon Universal Console のどの部分を有効にするかを制御するロールをそのグループに割り当てるです。

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 7 月 9 日

リビジョン	説明
2021 年 7 月 9 日	Microsoft Azure の Horizon Cloud ポッドでの高可用性の有効化のトピックを更新しました。このワークフロー中のサービスのアクティビティに関する追加の前提条件と情報が追記されています。 また、制限が存在しないため、Horizon Cloud での App Volumes の既知の制限 から既知の制限を削除しました。

2021 年 6 月 29 日

リビジョン	説明
2021 年 6 月 29 日	Horizon Cloud リリース ノート の 2021 年 6 月 29 日の「新機能」に記載されている理由により、ポッド インフラストラクチャのアラートの E メール送信機能に関連した内容を削除しました。

2021 年 6 月 9 日

リビジョン	説明
2021 年 6 月 9 日	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。 ■ 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 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。

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 30 日

リビジョン	説明
2021 年 3 月 30 日	2021 年 3 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 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 2 月 23 日

リビジョン	説明
2021 年 2 月 23 日	2021 年 2 月 23 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 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 15 月 12 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 9 日

リビジョン	説明
2020 年 9 月 12 日	2020 年 12 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 11 月 30 日

リビジョン	説明
2020 年 11 月 30 日	2020 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。

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。また、次の更新も行われました。 すべての手動デスクトップ プール（管理対象および非管理対象）が、Horizon ポッドに基づくマルチクラウド割り当てに参加することができないことを示す情報を次のトピックに追加しました。 ■ Horizon ポッド - マルチクラウド割り当てに適したデスクトップ プールの作成 ■ Horizon ポッド - マルチクラウド割り当てに使用する既存のデスクトップ プールを準備する ■ Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成

2020 年 7 月 9 日 ～ 2020 年 10 月 7 日

リビジョン	説明
2020 年 9 月 15 日	非管理対象の手動デスクトップ プールが、Horizon ポッドに基づくマルチクラウド割り当てに参加することができないことを示す情報を次のトピックに追加しました。 ■ Horizon ポッド - マルチクラウド割り当てに適したデスクトップ プールの作成 ■ Horizon ポッド - マルチクラウド割り当てに使用する既存のデスクトップ プールを準備する ■ Horizon ポッド - VDI デスクトップのマルチクラウド割り当ての作成
2020 年 9 月 8 日	2020 年 9 月 9 日の Horizon Cloud リリース ノートに記載された新しいアイテムおよび顧客フィードバックに対応するために次のトピックに追加された情報に合わせて、このガイドを更新しました。 ■ 新しいサブスクリプション管理機能の新しいトピック：Horizon Cloud：Microsoft Azure サブスクリプション情報の削除、編集、および追加 ■ Microsoft Azure の Horizon Cloud ポッド - VDI マルチクラウド割り当ての詳細の表示 ■ Horizon Cloud Connector の既知の考慮事項
2020 年 9 月 2 日	2020 年 9 月 1 日の Horizon Cloud リリース ノートに記載された新しいアイテムおよび顧客からの問い合わせに対応するために次のトピックに追加された情報に合わせて、このガイドを更新しました。 ■ Horizon ポッド - Connection Server への Universal Broker プラグインのインストール ■ Universal Broker のシステム要件 ■ 第 1 世代テナント - Microsoft Azure にデプロイされた 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
2020 年 8 月 18 日	ドキュメントのバグに対処するための情報を以下のトピックに追加しました。 ■ Horizon Cloud Connector 仮想アプライアンスの自動更新の構成 ■ 作成ワークフローを使用して、App Volumes アプリケーションを Horizon Cloud テナントのインベントリに追加する
2020 年 8 月 10 日	さまざまな更新を行いました。 ■ 最適なリモート エクスペリエンスを実現するためのゴールド イメージの構成に関するトピックを追加しました：Horizon Cloud ファームとデスクトップから最適なリモート エクスペリエンス パフォーマンスを引き出すためにゴールド イメージで実行すべき 5 つの重要な手順 ■ 複数のトピックを改訂し、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。 ■ 大量のレポートをエクスポートするための新しいコンソールの機能強化に関する情報を次のトピックに追加しました：第 1 世代テナント - 第 1 世代 Horizon Universal Console の [レポート] ページ
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 ノートに記載された新しいアイテムに合わせて、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 ノートに記載された新しいアイテムに合わせて、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 ノートに記載されたサービス更新に合わせて、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。

リビジョン	説明
2020 年 5 月 5 日	トピック Horizon Cloud のクラウド接続されたポッドに対する外部およびフォレストの信頼のサポートについてを追加しました。
2020 年 4 月 28 日	更新されたトピック： ■ シリアル ポート リダイレクトおよびスキャナ リダイレクト オプションに関する誤った記述を 2 つのドキュメント トピック（手動で作成した仮想マシンでのエージェント関連のソフトウェア コンポーネントのインストールおよび Horizon Cloud とのペアリングおよび廃止 - ポッドのマニフェスト バージョンが 1600 未満の場合、エージェントに関連するソフトウェア コンポーネントをベース仮想マシンにインストールする）から削除しました。
2020 年 4 月 14 日	更新されたトピック： ■ ポッドがプロキシを使用して構成されている場合に、[マーケットプレイスからの仮想マシンの自動インポート] ウィザードを使用できないというメモを削除しました。ポッドがプロキシを使用して構成されている場合にウィザードが使用できなかった以前の制限は、対処済みです。 ■ ポッドのデプロイ ウィザードに Azure Germany クラウド環境の選択肢が表示されても、現在、Microsoft は標準グローバル リージョンのセットに German リージョンを持っており、個別の Azure Germany クラウド環境の使用は廃止されたため、この選択肢のサポートは終了しました。この点についてのメモを追加しました。VMware ナレッジベースの記事 KB77121 を参照してください。 ■ Universal Broker でサポートされているクライアント情報を更新しました。
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 12 月 12 日 ～ 2020 年 3 月 16 日

リビジョン	説明
2020 年 2 月 24 日	この紹介ページから古いグラフィックを削除し、クラウド ポッド アーキテクチャに基づく仲介の説明を削除し、システムに保持されたデフォルトの appx パッケージの説明をドキュメント トピック[デスクトップのインポート] ウィザードを使用する場合に [Windows ストア アプリを削除] オプションを使用するに追加しました。
2020 年 1 月 13 日	更新対象： ■ Horizon Universal Broker 機能に関する情報。この機能は、クラウド接続された Horizon 7 ポッドの初期可用性になりました。この機能は、マルチクラウドの割り当てに使用されます。システム要件と詳細情報については、VMware Horizon Service Universal Broker についてのトピックおよびクラウド接続された Horizon ポッドのマルチクラウド割り当てに関連するすべてのサブトピックを参照してください。 ■ 対応するオプションがユーザー インターフェイスに表示されるのは Horizon Cloud テナント アカウントが関連する機能で有効になっている場合のみであり、また、VMware の担当者に連絡してその機能を有効にするように明示的に要求する必要があることを示すため、注意事項とリマインダを Horizon Cloud Connector 仮想アプライアンスの自動更新の構成に追加しました。デフォルトでは、これらのオプションは、その機能へのアクセスを要求しない限りテナントに対して無効になっています。
2019 年 12 月 12 日	2019 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。