Administration of Your Horizon Cloud Tenant Environment and Your Fleet of Onboarded Pods

Updated for the service level starting October 8, 2020
VMware Horizon Cloud Service
You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/
Contents

Administration of Your Horizon Cloud Tenant Environment and Your Fleet of Onboarded Pods  9

1 Introduction to Horizon Cloud and Onboarding Pods to Become Cloud-Connected Pods  13
   High-Level Workflow When You are Onboarding an Existing Manually Deployed Horizon Pod as Your First Pod to Your Horizon Cloud Tenant Environment  17
   DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod  21
   High-Level Workflow for When Your Very First Horizon Cloud Cloud-Connected Pod is from Using the Pod Deployer to Deploy a Pod into Microsoft Azure  25

2 Getting Started Using Your Horizon Cloud Environment  32
   Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment  36
   Service Accounts That Horizon Cloud Requires for Its Operations  47
   Locating the Information Required for the Horizon Cloud Register Active Directory Workflow’s NETBIOS Name and DNS Domain Name Fields  50
   Horizon Cloud Support for Active Directory Domain Controllers That Have LDAP Server Signing Requirements  53
   About External and Forest Trust Support for Cloud-Connected Pods in Horizon Cloud  53
   Log In to the Horizon Cloud Administration Console to Perform Management Tasks on Your Horizon Cloud Environment  54
   About Authentication to a Horizon Cloud Tenant Environment  58
   Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud  61
   Register Additional Active Directory Domains  64
   Add Additional Auxiliary Domain Bind Accounts  70
   Best Practices about the Two Types of Roles You Give to People to Use the Horizon Cloud Administration Console to Work in Your Horizon Cloud Environment  72
   Give Administrative Roles to Individuals in Your Organization for Logging In To and Performing Actions in Your Horizon Cloud Tenant Environment Using the Horizon Cloud Administration Console  77
   Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment  79
   Enabling or Deactivating the Cloud Monitoring Service (CMS) for Your Horizon Cloud Tenant Environment  84
   Sharing Your Feedback with VMware  85
   Join or Leave the Customer Experience Improvement Program  86
   Remove the Active Directory Domain Registration  87

VMware, Inc.  3
3 Introducing the Cloud Monitoring Service's Unified Visibility, Health Monitoring, and Help Desk Features Provided in Horizon Cloud 90

- Cloud Monitoring Service (CMS) and Horizon Agents Installer (HAI) Options For Your Horizon Cloud Environment 91
- Health Visibility and Insights into Your Cloud-Connected Pods Provided by the Cloud Monitoring Service in Horizon Cloud 92
- The Horizon Cloud Administration Console's Dashboard Page - Overview Tab for a Horizon Cloud Tenant 92
- The Horizon Cloud Administration Console's Dashboard Page - Sessions Tab for a Horizon Cloud Tenant 97
- Horizon Cloud Administration Console's Dashboard Page - Users Tab for a Horizon Cloud Tenant 98

- Help Desk Features in Your Horizon Cloud Environment 100
  - Using the Console's Search Feature 101
  - About the User Card Feature in Your Horizon Cloud Environment 102

4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types 108

- Launch Horizon Console as a Cloud Service 116
- Deploying Pods Using the Capacity Page 117
  - Deploying Horizon Cloud Pods into Microsoft Azure from the Capacity Page 118
- Change a Cloud-Connected Pod's Associated Location, Name, and Description in Your Horizon Cloud Tenant Environment 149
- Removing Cloud-Connected Horizon Pods from Use with Horizon Cloud 150
  - Clear the Cloud-Managed Properties from a Horizon Pod that was Offline During the Process to Disconnect it from Horizon Cloud 151

5 Typical Administrative and Maintenance Tasks You Perform on the Horizon Cloud Connector After the Horizon Pod is Paired with Horizon Cloud 153

- Configure a CA-Signed Certificate for the Horizon Cloud Connector Virtual Appliance 155
- Update the Static IP for the Horizon Cloud Connector Virtual Appliance 157
- Set a Password Expiry Policy for the Horizon Cloud Connector Root User 158
- Enable or Deactivate SSH on the Horizon Cloud Connector Appliance Using the Configuration Portal 159
- Modify DNS Settings for Horizon Cloud Connector 160
- Modifying Proxy Settings for Horizon Cloud Connector 1.6 or Later 161
- Modifying Proxy Settings for Horizon Cloud Connector 1.5 or Earlier 162
- Synchronize the Horizon Cloud Connector Virtual Appliance with an NTP Server 164
- Manually Activate Horizon Cloud Services for Horizon Cloud Connector 1.8 or Later 166
- Monitoring the Horizon Subscription License 168
- Manually Update the Horizon Cloud Connector Virtual Appliance 170
- Configure Automated Updates of the Horizon Cloud Connector Virtual Appliance 174
- Troubleshoot the Horizon Cloud Connector Virtual Appliance Update 181
- Collecting Log Files for Horizon Cloud Connector 181
Horizon Cloud Connector Known Considerations 183

6 Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment 185

Introduction to Universal Broker and Single-Pod Broker 187

System Architecture and Components of Universal Broker 191

Known Limitations of Universal Broker 195

System Requirements for Universal Broker 196

Horizon Pods - Port and Protocol Requirements for Universal Broker 198

Setting Up a Brokering Method 199

Horizon Pods - Install the Universal Broker Plugin on the Connection Server 200

Horizon Pods - Configure Unified Access Gateway for Use with Universal Broker 204

Select a Brokering Method for End-User Assignments 205

Configure Universal Broker 208

High-Level Steps for Setting Up Horizon Cloud Multi-Cloud Assignments (MCA) for Your Horizon Cloud Tenant 218

Working with Sites in a Universal Broker Environment 219

Configuring Sites for Universal Broker 220

Configuring Home Sites for Universal Broker 222

Horizon Pods - Enabling a Cloud-Connected Pod for Multi-Cloud Assignments 224

Horizon Pods - Change a Pod to Managed State 225

Horizon Pods - Change a Pod to Monitored State 226

Creating and Managing Multi-Cloud Assignments in Your Horizon Cloud Tenant Environment 227

Horizon Pods - Preparing Desktop Pools for Multi-Cloud Assignments 227

Creating Assignments in a Universal Broker Environment 232

Managing Multi-Cloud Assignments in Your Horizon Cloud Tenant Environment 257

7 Introduction to Horizon Cloud Pods in Microsoft Azure 264

High Availability and Your Horizon Cloud Pod in Microsoft Azure 272

Enable High Availability on a Horizon Cloud Pod in Microsoft Azure 275

Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure 276

Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it with Horizon Cloud 281

Customize the Imported VM’s Windows Operating System 296

Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance from Horizon Cloud Farms and Desktops 307

Install NVIDIA Graphics Drivers in a GPU-Enabled VM Imported in Horizon Cloud 314

Convert a Configured Image VM to an Assignable Image in Horizon Cloud 316

Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud 319

Tech Preview - How To Configure a Microsoft Windows 10 Multi-Session Image for Use with App Volumes Features in Horizon Cloud Pods in Microsoft Azure 357

Using Microsoft Azure Disk Encryption with Your Farms and VDI Desktops in Your Horizon Cloud Environment 363

VMware, Inc.
Using Data Disks with Virtual Desktops from a Horizon Cloud Pod in Microsoft Azure 366
  Setting Up a Data Disk for an Image VM in Horizon Cloud 368
VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure 374
  Install the NSX Agent in the Horizon Cloud Imported Image VM 377
  Firewall Rules Required in NSX Manager for Pod-Provisioned VMs 382
  Add the Required Forwarding Policy in NSX Manager for the Pod-Provisioned VMs 382
Managing VM Types and Sizes for Farms and Assignments 383
Farms in Horizon Cloud 384
  Create a Farm 385
  Enable a Horizon Agent Policy to Allow Running Universal Windows Platform (UWP) Applications from Microsoft Windows 10 Enterprise Multi-Session RDSH VMs in Horizon Cloud 401
  Managing Farms in Horizon Cloud 403
  Example of Farm Rolling Maintenance 409
  About Power Management and Load Balancing for Farms in Horizon Cloud 410
Applications in Your Horizon Cloud Inventory 412
  App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites 413
  Remote Applications - Importing from RDSH Farms that are Provisioned by Horizon Cloud Pods in Microsoft Azure 428
  Remote Applications - Create a Remote Application Assignment for Remote Applications Provisioned By Horizon Cloud Pods in Microsoft Azure 431
About Desktop Assignments for Your Horizon Cloud Environment's Pods in Microsoft Azure 433
  Create an RDSH Session Desktop Assignment 434
  Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure 436
  Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure 450
Create a URL Redirection Customization and Assign it to Users 464
  Understanding What URL Content Redirection Is 468
  Configuring Agent-to-Client Redirection 469
Managing Published Images for Horizon Cloud Pods in Microsoft Azure 472
  Actions You Can Perform on Published Images from Horizon Cloud Pods in Microsoft Azure 473
  Change Images Used for Farms in Horizon Cloud 476
  Change Images Used for VDI Desktop Assignments 478
Managing Assignments Provisioned By Horizon Cloud Pods in Microsoft Azure 480
  Viewing the Assignments Currently Configured in Your Horizon Cloud Environment 485
  Edit an Assignment in Your Horizon Cloud Environment 486
  Delete an Assignment from Your Horizon Cloud Environment 487
  Resizing a VDI Desktop Assignment in Your Horizon Cloud Environment 489
  Prevent Deletions or Allow Deletions for a Dedicated Desktop Assignment 490
About Network Security Groups and Your VDI Desktops 491
Updating the Agent-Related Software Used by Horizon Cloud

Update Agent Software for RDSH Images in Horizon Cloud

Update Agent Software for Dedicated VDI Desktop Assignments

Update Agent Software for Images Used by Floating VDI Desktop Assignments

Managing Your Horizon Cloud Pods Deployed in Microsoft Azure

Obtain the Pod Gateway's Load Balancer Information to Map in your DNS Server

Changing Gateway-Related Items for a Deployed Horizon Cloud Pod in Microsoft Azure

Overview of Using Multiple Tenant Subnets with Your Horizon Cloud Pod for Your Farms and VDI Desktop Assignments

Change, Modify, and Update the Subscription Information Associated with Deployed Horizon Cloud Pods

Horizon Cloud — Deleting, Editing, and Adding Microsoft Azure Subscription Information

Examine a Subscription’s Current Usage of Your Microsoft Azure Limits Using the Horizon Cloud Administration Console

Updating Your Horizon Cloud Pod

Backup and Restore Service for Horizon Cloud Pods in Microsoft Azure

Change the Horizon Cloud Pod’s NTP Setting

Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs

DNS Requirements for a Horizon Cloud Pod in Microsoft Azure

Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release’s Manifest or Later

Ports and Protocols Requirements for a Horizon Cloud Pod Deployed Prior to the September 2019 Release

Default Network Security Group Rules for the VMs in a Horizon Cloud Pod Deployed in Microsoft Azure

Resource Groups Created For a Pod Deployed In Microsoft Azure

Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access

Configure a Horizon Cloud Pod in Microsoft Azure for Workspace ONE Access

Confirm End-User Access to Desktop Assignments in Workspace ONE Access

Configure True SSO for Use with Your Horizon Cloud Environment

Install and Configure a Windows Server 2012 R2 Certificate Authority

Set Up a Certificate Template on the CA

Download the Horizon Cloud Pairing Bundle

Set up the Enrollment Server

Complete Configuring True SSO for your Horizon Cloud Environment

End User Connections to Desktops and Applications Provided by Your Horizon Cloud Environment

Enable Time Zone Redirection for RDS Desktop and RDS-Based Application Sessions

Multiple-Monitor Support for Desktops and Remote Applications Provided By a Horizon Cloud Pod in Microsoft Azure

Horizon Cloud — Support of Media Optimization for Microsoft Teams
Access Desktops and Applications 684

8 About the Horizon Cloud Administration Console's Left-Hand Navigation Menus 690

About the Monitor Menu in the Horizon Cloud Administration Console 691
  Activity Page 692
  Reports Page 695
  Notifications Page 700
  Working with Audit Logs 701
About the Assignments Menu in the Horizon Cloud Administration Console 703
About the Inventory Menu in the Horizon Cloud Administration Console 704
  Imported VMs Page 706
About the Settings Menu in the Horizon Cloud Administration Console 706
  Customizable General Settings for Your Horizon Cloud Tenant Environment 708
  Domain Security Settings on General Settings Page 713
  File Share Page 723
  Licenses Page 723
  Identity Management Page in the Horizon Cloud Administration Console 724
  Broker-Related Settings for Your Horizon Cloud Tenant Environment 728
About the Horizon Cloud Getting Started Wizard 730

9 Using the Filter Field in the Horizon Cloud Administration Console 734

10 Troubleshooting for Administrators of Horizon Cloud Environments 736
  Required Administrator Actions When the Disk Size for a Farm or VDI Desktop Assignment is Increased 736
  Cannot Successfully Log In at the First Login Screen of the Horizon Cloud Administration Console 737
  Convert to Image Task Fails with Timeout Error Even After Addressing the Logged Microsoft Windows Sysprep Errors 737
  For a Windows Server 2012 Image, Convert to Image Task Fails with Timeout Error 738
  Notifications When the Primary Domain-Bind Account is Locked Out 739
  New Farm Remains In Progress 739
  Windows Error Message Appears When Trying to Connect to a Desktop from a Floating VDI Desktop Assignment 740
  Email Feedback Option Does Not Work 740
  Considerations For Using Nested Active Directory Domain Organizational Units 742
  When Your Pod is Not Yet Updated to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image 743

11 Revision History — Changelog — Administration of Your Horizon Cloud Tenant Environment and Your Fleet of Onboarded Pods 746
Administration of Your Horizon Cloud Tenant Environment and Your Fleet of Onboarded Pods

This Administration Guide explains how to use VMware Horizon® Cloud Service™ to administer the pods you have onboarded to the cloud service. Your overall Horizon Cloud tenant environment consists of the VMware-hosted cloud service and your pods deployed into their corresponding capacity environments and connected to the cloud service. To work with your tenant environment's fleet of cloud-connected pods and the desktop-as-a-service features that the service provides, you log in to and use the tenant environment's web-based administrative portal named the Horizon Cloud Administration Console, or the console for short.

The VMware Horizon services encompass various deployment modes. This document applies when you are using the web-based administrative console to work with the following items:

- VMware Horizon® pods that you installed on-premises and then connected to Horizon Cloud
- VMware Horizon pods that you manually installed in your VMware Cloud™ on AWS SDDC and then connected to Horizon Cloud.
- Pods in your Microsoft Azure cloud capacity that you automatically deployed and configured using Horizon Cloud

To find out more about all of the various Horizon Cloud deployment modes, see https://www.vmware.com/cloud-services/desktop.html.

See https://www.vmware.com/help/privacy.html for information about how VMware handles information collected through this product.

The information in this document describes how to use the Horizon Cloud capabilities after the cloud service is connected to one of the its supported environments: a VMware Horizon pod in VMware Cloud, a VMware Horizon pod on-premises, or a pod in Microsoft Azure. For information on how to connect a supported environment to the cloud service, see the Deployment Guide's Onboarding to Horizon Cloud for Microsoft Azure, Horizon On-Premises, and Horizon on VMware Cloud on AWS topic and its subtopics.
Important  This document describes features available in the Horizon Cloud Administration Console for the current release of the Horizon Cloud Service working with the connected environments. When you have pods that are not yet updated to the currently supported release level, you will not see all of the features that this document describes when those features depend on the latest pod software level. Also, in a particular release, Horizon Cloud might include separately licensed features. The console reflects the elements related to such features only when your license includes use of such features. When you are not seeing a feature in the console that you are expecting to see, contact your VMware account representative to verify whether your license entitled you use of that feature.

Revision History for these Administrative Topics

This documentation set of topics is updated with each release of the product or when necessary. For the set of significant revisions made to date, see Chapter 11 Revision History — Changelog — Administration of Your Horizon Cloud Tenant Environment and Your Fleet of Onboarded Pods.

Intended Audience

This document is intended for experienced IT system administrators who are familiar with virtual machine technology and datacenter operations.

Depending on your organization's needs and the type of pod you are working with, you might find it helpful to be familiar with these software products, software components, and their features:

- VMware Horizon
- VMware Cloud
- VMware Horizon® Cloud Connector™
- VMware Unified Access Gateway™
- VMware Workspace ONE® Access™
- VMware Workspace ONE Hub Services
- VMware Horizon® Client™
- VMware Horizon® HTML Access™
- Microsoft Azure and its Marketplace
- Azure VMware Solution
- Microsoft Active Directory
- VMware Dynamic Environment Manager™
About the Screenshots Used in This Document

The screenshots typically:

- Show only that portion of the overall user interface screen that corresponds to the text at which point the screenshot appears, and not necessarily the full user interface.
- Have blurred areas where appropriate to maintain data anonymity.

**Note** Some screenshots are taken at a higher resolution than others, and might look grainy when the PDF is viewed at 100%. However, if you zoom to 200%, those images start to look clear and readable.

Horizon Cloud Community

Use the following communities to ask questions, explore answers given for questions asked by other users, and access links to useful information.

- VMware Horizon Cloud Service community at https://communities.vmware.com/community/vmtn/horizon-cloud-service
- VMware Horizon Cloud on Microsoft Azure sub-community at https://communities.vmware.com/community/vmtn/horizon-cloud-service/horizon-cloud-on-azure, a sub-community of the VMware Horizon Cloud Service community.

Contacting VMware Support

Contact VMware Support when you need help with your Horizon Cloud environment.

- You can submit a support request to VMware Support online using your My VMware® account or by phone.
- **KB 2144012 Customer Support Guidelines** provides details for getting support depending on the issue encountered.
- After you have configured at least one cloud-connected pod, you can submit a support request by logging in to the cloud-based console and clicking > Support.

Selected Pod-Related Terminology Used in these Administration Guide Documentation Topics

Throughout the Horizon Cloud documentation topics, these phrases have the indicated meanings as follows.

**Horizon pod**
A pod that is constructed based on VMware Horizon product software, and which includes Horizon Connection Server software components.

**Horizon Cloud pod**

A pod that is constructed by running the Horizon Cloud pod deployment wizard which deploys the pod in Microsoft Azure.

**connection broker**

A connection broker is responsible for connecting end users' clients with a virtual desktop VM or farm VM for the purpose of setting up a connected session between each end-user client and the agent running in that VM. This noun — broker — is used because one general definition of the noun broker in the English language is one who negotiates a transaction. In desktop virtualization software's use cases, the connection broker running in a pod receives the end-user's client request to make a connection with a virtual desktop VM or farm VM. The connection broker then negotiates a connected session between the agent running in one of the VMs and that end-user client. The negotiation takes into consideration what types of pod-provisioned resources the end user is entitled to make connections with.

One of the responsibilities of the Horizon Connection Server in a Horizon pod is to serve as a connection broker. For a Horizon Cloud pod deployed in Microsoft Azure, one of the responsibilities of the pod manager VM is to serve as a connection broker.

**VMware Information Experience Glossary**

VMware Information Experience provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

**VMware Privacy Notices**

See https://www.vmware.com/help/privacy.html for information about how VMware handles information collected through this product.
Introduction to Horizon Cloud and Onboarding Pods to Become Cloud-Connected Pods

Your overall Horizon Cloud tenant environment consists of the VMware-hosted cloud service and your pods deployed into their corresponding capacity environments and connected to the cloud service. When a pod, consisting of VMware software deployed into a supported capacity environment, is appropriately onboarded, then it is a cloud-connected pod. When at least one pod is completely onboarded into your tenant environment, you can onboard additional pods to make for a fleet of cloud-connected pods. To work with your tenant environment's fleet of cloud-connected pods and the desktop-as-a-service features that the service provides, you log in to and use the tenant environment's cloud-based portal, named the Horizon Cloud Administration Console, or the console for short.

**Horizon Cloud**

A control plane hosted in the cloud by VMware for the central orchestration and management of virtual desktops and applications.

**cloud-connected pod**

VMware software deployed into a supported capacity environment and onboarded to the cloud control plane. Each of these supported capacity environments provides for a specific pod type:

- Pod in your Microsoft Azure subscription
- On-premises Horizon pod
- Horizon pod in an environment with a VMware-supported SDDC, including:
  - VMware Cloud on AWS
  - Azure VMware Solution (AVS)

Depending on the type of capacity environment you are using, you can use the cloud-based console for an automated pod deployment and connection to Horizon Cloud. For some of those pod types, even though they cannot be automatically deployed and configured, you can still onboard those pods to Horizon Cloud.

For a high-level overview of the pod-onboarding concept, see Deployment Guide.
Control Plane

VMware hosts the control plane in the cloud. This control plane provides services that enable the central orchestration and management of virtual desktops, remote desktop sessions, and remote applications for your users. The control plane enables the management of your pods. The pods are physically located in your provided capacity environments. When you log in to the cloud-based console, you can see all your cloud-connected pods and perform management activities across them, regardless of where they are physically located.

VMware is responsible for hosting the service and providing feature updates and enhancements for a software-as-a-service experience. Horizon Cloud is a multi-tenant environment, and has several regional control plane instances. Each regional control plane instance corresponds to its hosting geographic data center, as described in the service description document available from the VMware Horizon Service Description and Service Level Agreement page. Your tenant account is associated with a specific regional instance at the time the account is created.

The cloud control plane also hosts the common cloud- and web-based management user interface called the Horizon Cloud Administration Console, or console for short. This console runs in industry-standard browsers. It provides IT administrators with a single location for management and administrative tasks involving user assignments and the virtual desktops, remote desktop sessions, and applications. This console is accessible from anywhere at any time, providing maximum flexibility.

**Important**  The administrative console is dynamic and reflects what is available at the current service level. However, when you have cloud-connected pods that are not yet updated to the latest levels of the pod's software, the console does not display those features that depend on the latest pod software level. Also, in a particular release, Horizon Cloud might include separately licensed features or features that are only available for particular tenant account configurations. The console dynamically reflects the elements related to such features only when your license or tenant account configuration includes use of such features.

When you are expecting to see a feature in the administrative console and do not see it, contact your VMware account representative to verify whether your license and tenant account configuration entitles its usage.

Pod Types You Can Connect to Horizon Cloud

This Horizon Cloud release provides for the following deployment types.

**Note**  To connect a pod to Horizon Cloud or use the administrative console for an automated deployment, your customer account must have the appropriate licensing. For licensing information, contact your VMware account representative.
### Table 1-1. Pod Deployment Types

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Horizon pod located in your on-premises infrastructure</td>
<td>Deploy the Horizon Cloud Connector in your on-premises infrastructure and configure it to connect that pod to Horizon Cloud.</td>
</tr>
<tr>
<td>VMware Horizon pod that you manually installed and configured in your VMware Cloud on AWS SDDC</td>
<td>Deploy the Horizon Cloud Connector in your VMware Cloud on AWS SDDC and configure it to connect that pod to Horizon Cloud.</td>
</tr>
<tr>
<td>VMware Horizon pod that you deployed in your Azure VMware Solution (AVS) cloud</td>
<td>Deploy the Horizon Cloud Connector in your AVS cloud and configure it to connect that pod to Horizon Cloud.</td>
</tr>
<tr>
<td>Horizon Cloud pod deployed by Horizon Cloud into your Microsoft Azure cloud capacity</td>
<td>Deploy the pod using the administrative console’s automated deployment wizard.</td>
</tr>
</tbody>
</table>

**Important**  For production environments, ensure the VM models used for your farms and desktop assignments have a minimum of two (2) CPUs. VMware scale testing has shown that using 2 CPUs or more avoids unexpected end-user connection issues. Even though the system does not prevent you from choosing a VM model with a single CPU, you should use such VM models for tests or proof-of-concepts only.
Important  Before launching the pod deployment wizard and starting to deploy your pod, in addition to the requirements below, you must be aware of the following key points:

- Starting with the July 2020 service release, in brand new environments, new pods are required to deploy with at least one gateway configuration. If your customer account was created prior to the July 2020 release, but you have not yet deployed your first pod, deployment of that first pod will require configuring at least one gateway configuration at the time of pod deployment.

- Successful pod deployment requires that none of the Microsoft Azure Policies that you or your IT team have set in your Microsoft Azure environment block, deny, or restrict creation of the pod's components. Also you must verify that your Microsoft Azure Policies Built-in Policy definitions do not block, deny, or restrict creation of the pod's components. As an example, you and your IT team must verify that none of your Microsoft Azure Policies block, deny, or restrict creation of components on Azure storage account. For information about Azure Policies, see the Azure Policy documentation.

- The pod deployer requires that your Azure storage account allow for the deployer to use the Azure StorageV1 and StorageV2 account types. Ensure that your Microsoft Azure Policies do not restrict or deny the creation of content requiring the Azure StorageV1 and StorageV2 account types.

- As part of the pod and gateway deployment processes, unless you specify custom resource tags in the deployment wizard, Horizon Cloud creates resource groups (RGs) in your Microsoft Azure subscription that do not have tags on them, including the initial resource group that is created for the temporary jump box that orchestrates those deployment processes. As of the October 8, 2020 cloud plane refresh, the deployment wizard has a feature in which you can specify custom resource tags that you want applied to the deployer-created resource groups. If you do not specify custom resource tags and your Microsoft Azure subscription has any type of resource tag requirement, pod deployment will fail if you try to deploy a pod into that subscription, or it will fail at the time of pod updates or adding a gateway configuration to a pod. If you are not planning to use the deployment wizard’s custom resource tags feature, you must verify that your Microsoft Azure Policies allows creation of the pod’s untagged resource groups in the target subscription. For the list of RGs that the deployer creates, see the Administration Guide's Resource Groups Created For a Pod Deployed In Microsoft Azure topic.

- All cloud-connected pods must have line-of-sight to the same set of Active Directory domains at the time you deploy those pods.

Note  You must select a city from the system's autocomplete list. Currently, due to a known issue, the location names are not localized.

Note  The numbers in parentheses stated in each known issue refer to VMware internal issues tracking systems.

This chapter includes the following topics:
High-Level Workflow When You are Onboarding an Existing Manually Deployed Horizon Pod as Your First Pod to Your Horizon Cloud Tenant Environment

This list is a high level of the steps when you are onboarding your very first pod to your Horizon Cloud tenant environment and that pod is an existing manually deployed Horizon pod. A manually deployed pod is one that you manually installed and configured using either on-premises capacity or using a supported cloud capacity. After these onboarding steps are completed for your very first cloud-connected pod, the subscription license is applied to that onboarded Horizon pod. Additionally, if you selected the Full Feature option when deploying Horizon Cloud Connector, you can start using the cloud-hosted services that Horizon Cloud provides for that pod type, which include the Cloud Monitoring Service (CMS). At that point, you can also onboard additional pods.

The following diagram illustrates the overall flow.

Before beginning this workflow, you must have already installed and configured your Horizon pod. For information about manually installing a Horizon pod that you can use with this Horizon Cloud release:

- See the VMware Horizon software installation information according to the software edition that is running on the pod that you are going to connect to the cloud plane — Horizon 7 Documentation page or Horizon Documentation page.
- When manually installing pods using VMware Cloud on AWS capacity, see also the best practices guide for deploying Horizon pods on VMware Cloud on AWS, available from the Horizon on VMware Cloud on AWS product page.

You onboard an existing Horizon pod to the cloud for two primary use cases: to activate a subscription license for that pod and to activate your use of those cloud-hosted services that Horizon Cloud provides for this type of pod, such as the Cloud Monitoring Service (CMS). The CMS is one of the central services provided in Horizon Cloud. CMS provides for visibility, health monitoring, and help desk services with cloud-connected pods. For a high-level description of the process of onboarding a pod to the cloud control plane, see the Deployment Guide.

**Caution** Complete all of the steps below to fully connect your first pod to Horizon Cloud before you start deploying the Horizon Cloud Connector with any subsequent manually installed pod you want to connect. Due to a known issue in this release, if you finish connecting more than one pod to the cloud using the Horizon Cloud Connector before you complete the Active Directory domain registration and Super Administrators role assignment step at least once, the Active Directory domain registration step will fail. At that point, you will have to unplug all but one of your cloud-connected Horizon pods before you can successfully complete the required Active Directory domain registration and Super Administrators role assignment step.

1. Fulfill the prerequisites, which include obtaining a Horizon subscription license, such as the Horizon universal license. See the topics [VMware Horizon with Horizon Cloud Requirements Checklist - for Use with the December 2019 Service Release](#) and [Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using the Horizon Cloud Connector](#) in the Deployment Guide.

2. Verify you meet the DNS, ports, and protocol requirements for connecting a Horizon pod with Horizon Cloud. See [DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod](#).

3. If your environment requires use of a proxy server for the Horizon Cloud Connector virtual appliance to reach the Internet, obtain the required proxy settings so that you can specify them when you deploy the appliance into your pod's environment.
4 Optionally log in to the Horizon Cloud tenant portal and configure additional administrators for your tenant environment.

**Tip** Even though you can complete the next steps to onboard the pod solely using the My VMware account that is the one initially associated with your tenant environment, it is prudent to configure additional administrators at the start of this process. If only a single My VMware account is associated with your tenant account and you lose access to the credentials, delays might occur because you'll have to open a service request with VMware to associate a new My VMware account with the tenant account. To prevent such delays, log in to the tenant portal at cloud.horizon.vmware.com with the initially associated My VMware account and then follow steps described in *Add Administrators to Log in to Your Horizon Cloud Tenant Environment* using the row in the General Setup section of the screen.

5 Deploy the Horizon Cloud Connector virtual appliance into the pod's environment. Follow the steps described in the subtopics under Download and Deploy the Horizon Cloud Connector into Your Pod's Environment in the Deployment Guide.

6 After the virtual appliance is powered up, enable SSH access to the virtual appliance to remotely run commands in the appliance's operating system. Follow the steps in the topic Enable SSH Access to the Horizon Cloud Connector Prior to Pairing it with Connection Server in the Deployment Guide.

**Note** Those steps to enable SSH are used for the time when the pod is not yet successfully paired with Horizon Cloud. After the pod is successfully paired with Horizon Cloud, then you will be able to use the browser-based Horizon Cloud Connector's configuration portal to activate and deactivate SSH access to the virtual appliance.

7 If your environment requires use of a proxy and you did not specify proxy-related settings in the OVF deployment wizard, configure the proxy-related settings for the virtual appliance. See Modifying Proxy Settings for Horizon Cloud Connector 1.6 or Later for more details.

8 If you want to access the browser-based Horizon Cloud Connector configuration portal using a fully qualified domain name (FQDN) instead of using the Horizon Cloud Connector virtual appliance's IP address, create a forward and reverse lookup record in your DNS server that maps an FQDN to the virtual appliance's IP address.

9 Verify the health of the pod's system components and services by opening an SSH session to the Horizon Cloud Connector virtual appliance and running the `precheck.sh` diagnostics script. See the topic Verify the Horizon Pod and Virtual Appliance Are Ready to Be Paired in the Deployment Guide for more details.
10 Using either a mapped FQDN or the virtual appliance's IP address, log in to the browser-based Horizon Cloud Connector configuration portal and complete the onboarding steps that pair the connector with the pod's Connection Server. Follow the steps described in the topic **Complete Pairing the Horizon Pod with Horizon Cloud Using the Horizon Cloud Connector Configuration Portal** in the *Deployment Guide*.

**Tip** When the connector and Connection Server are successfully paired, the Horizon Cloud Connector configuration portal will display a Congratulations message. At this point, VMware will activate your subscription license. The activation is typically completed after 30 minutes but can take up to 4 hours in some cases. When the license is activated, you will see the message **Connected to License Service** in your pod's web-based console's **Product Licensing & Usage** screen.

11 Depending on your team standard practices and environment, optionally configure the Horizon Cloud Connector virtual appliance in areas such as configuring a CA-signed certificate and setting a password expiry for the appliance's root user. See the topic in the *Deployment Guide*.

12 Complete the Active Directory domain registration workflow within the Horizon Cloud administrative console, named Horizon Cloud Administration Console, or console for short. See **Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment**.

**Tip** Completing the Active Directory domain registration workflow enables you to take advantage of all the cloud-hosted services, such as the Cloud Monitoring Service (CMS). Until the pod's Active directory domain is registered with your tenant environment, the console's screens in which the CMS's monitoring data gets displayed are inaccessible.

13 Give the Horizon Cloud Super Administrators role to an Active Directory group that includes that domain-join account as a member. See **Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment**.

You can find in-depth details on how to accomplish each workflow step in the topics that are linked from each step above or in the companion guide. See the *Horizon Cloud Deployment Guide*.
DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod

When you are using the Horizon Cloud Connector virtual appliance with your Horizon pod, you must configure your firewalls to allow the appliance to access the Domain Name Service (DNS) addresses it needs. In addition, your proxy settings require configured ports and protocols and DNS must resolve specific names as described in this topic. Then, after the Horizon Cloud Connector virtual appliance is deployed and you have completed the steps to successfully connect the pod to Horizon Cloud, specific ports and protocols are required for ongoing operations between Horizon Cloud and the virtual appliance.

As described in When Onboarding a Horizon Pod to Use Horizon Subscription Licenses or Cloud-Hosted Services with that Pod, the Horizon Cloud Connector virtual appliance is used with VMware Horizon deployments to activate subscription licenses on Horizon and enable use of cloud-hosted services with your Horizon deployments.

Connectivity and DNS Requirements

The steps for connecting Horizon Cloud with your Horizon pod using the Horizon Cloud Connector include the step to use a browser to navigate to the Horizon Cloud Connector appliance's IP address and a login screen will appear. To see that login screen requires Internet connectivity between the Horizon Cloud Connector appliance and the Horizon Cloud cloud control plane. The appliance establishes a connection to the Horizon Cloud cloud control plane initially using HTTPS, and then opens a persistent WebSocket connection, using outbound Internet port 443. For ongoing operations, the connection between the Horizon Cloud Connector appliance and Horizon Cloud requires that outbound Internet connection using port 443 open all the time. You must ensure the following Domain Name Service (DNS) names are resolvable and reachable using the specific ports and protocols as listed according to the tables below.

**Important** Horizon Cloud Connector uses SSL certificates signed by DigiCert, an industry-trusted certificate authority (CA). These certificates use CRL (Certificate Revocation Lists) and OCSP (Online Certificate Status Protocol) queries that refer to specific DNS names on the DigiCert domain. To ensure Horizon Cloud Connector connectivity, you must configure these DNS names to be resolvable and reachable by the virtual appliance. If these DNS names are not reachable, you will not be able to access the Horizon Cloud Connector configuration portal. The specific names are determined by DigiCert, and therefore are not in VMware's control.

**Note** If you are going to enable use of Universal Broker with the pod, there might be additional connectivity requirements for that use case. For details, see System Requirements for Universal Broker and its related topics.
Your Welcome to Horizon Service email will indicate which regional control plane instance your
tenant account was created in. Due to a known issue that existed when the welcome email was
sent to you, the email you received might display the system string names used for the regions
instead of human-friendly names. If you see a system string name in your welcome email, you
can use the following table to relate what is shown in your email with the regional control plane
DNS names.

<table>
<thead>
<tr>
<th>Your welcome email says</th>
<th>Regional DNS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>cloud.horizon.vmware.com</td>
</tr>
<tr>
<td>EU_CENTRAL_1 or Europe</td>
<td>cloud-eu-central-1.horizon.vmware.com</td>
</tr>
<tr>
<td>AP_SOUTHEAST_2 or Australia</td>
<td>cloud-ap-southeast-2.horizon.vmware.com</td>
</tr>
<tr>
<td>PROD1_NORTHCENTRALUS2_CP1 or USA-2</td>
<td>cloud-us-2.horizon.vmware.com</td>
</tr>
<tr>
<td>PROD1_NORTHEUROPE_CP1 or Europe-2</td>
<td>cloud-eu-2.horizon.vmware.com</td>
</tr>
<tr>
<td>PROD1_AUSTRALIAEAST_CP1 or Australia-2</td>
<td>cloud-ap-2.horizon.vmware.com</td>
</tr>
<tr>
<td>Japan</td>
<td>cloud-jp.horizon.vmware.com</td>
</tr>
<tr>
<td>Source</td>
<td>Destination (DNS name)</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Horizon Cloud Connector</td>
<td>One of the following names, depending on which regional Horizon Cloud control plane instance is specified in your Horizon Cloud tenant account. The regional instance is set when the account is created, as described in Onboarding to Horizon Cloud for Microsoft Azure, Horizon On-Premises, and Horizon on VMware Cloud on AWS.</td>
</tr>
<tr>
<td></td>
<td>- cloud.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-us-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-ap-southeast-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-ap-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-jp.horizon.vmware.com</td>
</tr>
<tr>
<td>Horizon Cloud Connector</td>
<td>Depending on which regional Horizon Cloud control plane is specified in your Horizon Cloud account: North America: kinesis.us-east-1.amazonaws.com query-prod-us-east-1.cms.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- kinesis.eu-central-1.amazonaws.com query-prod-eu-central-1.cms.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- kinesis.ap-northeast-1.amazonaws.com query-prod-ap-northeast-1.cms.vmware.com</td>
</tr>
<tr>
<td>Horizon Cloud Connector</td>
<td>*.digicert.com</td>
</tr>
</tbody>
</table>
Note If your organization discourages the use of wildcards in allowable DNS names, you can allow specific names instead. For example, at the time of this writing, the specific DNS names required for certificate validation are:
- ocsp.digicert.com
- crl3.digicert.com
- crl4.digicert.com
- www.digicert.com/CPS
These DNS names are determined by DigiCert and subject to change. For instructions on how to obtain the specific names required by your certificates, refer to VMware Knowledge Base (KB) article 79859.

Ports and Protocols Required by the Horizon Cloud Connector Virtual Appliance
For ongoing operations between Horizon Cloud Connector and Horizon Cloud, the ports and protocols in the following table are required.

Table 1-3. Horizon Cloud Connector Ports

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Cloud Connector</td>
<td>Horizon Cloud</td>
<td>443</td>
<td>HTTPS</td>
<td>Used to pair the Horizon Cloud Connector with Horizon Cloud and transfer data.</td>
</tr>
<tr>
<td>Horizon Cloud Connector</td>
<td>Connection Server</td>
<td>443</td>
<td>HTTPS</td>
<td>API calls to Connection Server.</td>
</tr>
<tr>
<td>Horizon Cloud Connector</td>
<td>Connection Server</td>
<td>4002</td>
<td>TCP</td>
<td>Java Message Service (JMS) communication between the Cloud Connector and the Connection Server</td>
</tr>
<tr>
<td>New version of the Horizon Cloud Connector appliance</td>
<td>Existing version of the Horizon Cloud Connector appliance</td>
<td>22</td>
<td>SSH</td>
<td>Listen for requests to start the update process.</td>
</tr>
</tbody>
</table>
Table 1-3. Horizon Cloud Connector Ports (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browser</td>
<td>Horizon Cloud Connector</td>
<td>443</td>
<td>HTTPS</td>
<td>Listen for the initiation of the pairing process.</td>
</tr>
<tr>
<td>Cloud Monitoring Service agent in the desktop or server VMs that are from the cloud-connected Horizon pod on your network</td>
<td>Horizon Cloud Connector appliance</td>
<td>11002</td>
<td>TCP</td>
<td>For the Cloud Monitoring Service agent on a server or desktop VM to send data to the Horizon Cloud Connector</td>
</tr>
</tbody>
</table>

High-Level Workflow for When Your Very First Horizon Cloud Cloud-Connected Pod is from Using the Pod Deploayer to Deploy a Pod into Microsoft Azure

This is a high-level list of the steps when you are arriving at your very first cloud-connected pod by running the pod deployer to deploy a Horizon Cloud pod into your Microsoft Azure capacity. After that first cloud-connected pod is fully deployed and you have completed the steps to register Horizon Cloud with the pod’s intended Active Director domain, you can use all the features provided Horizon Cloud, especially for provisioning VDI desktops, RDSH session-based desktops, or RDSH-based remote applications to your end users from that pod. When your customer account is configured to use App Volumes features with your pods in Microsoft Azure, you can also provision applications from those App Volumes features and entitle those to your end users.

For an overall introduction to pods in Microsoft Azure, see Chapter 7 Introduction to Horizon Cloud Pods in Microsoft Azure.

Perform the following steps when you are deploying your very first cloud-connected pod and you are using the pod deployment wizard to deploy it into Microsoft Azure.

1. Fulfill the prerequisites. See VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist For New Pod Deployments.

2. Perform the preparatory tasks outside of Horizon Cloud. See Preparing to Deploy a Horizon Cloud Pod into Microsoft Azure.

3. Verify you meet the DNS, ports, and protocol requirements for deploying the pod. See DNS Requirements for a Horizon Cloud Pod in Microsoft Azure and Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later.

4. Deploy the pod. See Deploy a Horizon Cloud Pod into Microsoft Azure.

5. Register your Active Directory domain with the deployed pod, which includes providing the name of a domain-join account. See Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment.
6 Give the Horizon Cloud Super Administrators role to an Active Directory group that includes that domain-join account as a member.

**Important** You must ensure that the domain join account you enter when registering the domain is also in one of the Active Directory groups to which you assign the Horizon Cloud Super Administrators role. The system's domain-join operations with the pod depend on the domain join account having the Horizon Cloud Super Administrators role. See Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment

7 Select the type of brokering you want your tenant's pods to use when brokering pod-provisioned resources to your end users. See Introduction to Universal Broker and Single-Pod Broker and its related topics and subtopics.

**Attention** Completing this brokering selection step before deploying additional pods into Microsoft Azure is a best practice.

8 If you plan to use Workspace ONE Access with the pod or you plan to have Horizon Clients connecting directly to the pod (not through a pod gateway configuration), then perform these steps:

- In your DNS server, map a fully qualified domain name (FQDN) to the pod manager's Microsoft Azure load balancer IP address
- Obtain an SSL certificate based on that mapped FQDN
You will upload an SSL certificate to the pod that is based on the FQDN that you've mapped to the pod manager's Microsoft Azure load balancer IP address in your DNS so that connections that go to the pod manager VMs will make trusted connections. Such connections include Horizon Clients, for your users that you give that mapped FQDN to, and the Workspace ONE Access Connector that is used when you integrate Workspace ONE Access with the pod. The Workspace ONE Access Connector must connect to the pod using an FQDN that is mapped to the pod manager's Microsoft Azure load balancer IP address.

**Attention** When you are integrating Workspace ONE Access with the pod, you must upload an SSL certificate to the pod and configure your Workspace ONE Access to point to the pod, not to the pod's Unified Gateway Access configurations.

However, bear in mind that when you have uploaded an SSL certificate based on your DNS-mapped FQDN, if you try to connect by directly typing that FQDN into a browser — not going through a properly configured Workspace ONE Access — that pure FQDN use will appear as untrusted connections to the browser. The reason is because simply loading that FQDN into a browser is a connection using HTML Access (Blast), and that is how HTML Access (Blast) behaves. As a result, when you load that FQDN into a browser, it displays the typical untrusted certificate error.

In the absence of having Workspace ONE Access, to have connections using HTML Access (Blast) — using a browser basically — avoid the displayed untrusted certificate error, you must put a gateway configuration on the pod and have those connections use the load balancer and Unified Access Gateway instances from that gateway configuration. If you do not want to expose your FQDN to the Internet, you can deploy an internal Unified Access Gateway configuration. This internal Unified Access Gateway configuration uses a Microsoft Azure internal load balancer to which end users who are internal to your corporate network can make their connections.

9 Upload an SSL certificate to the pod directly, using the pod's summary page in the administrative console, if you plan to have one or both of the use cases described in the preceding step. See Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs.

**Tip** If the only access use case you will ever want to support is where connections will go to the pod's Unified Access Gateway instances through the load balancer connected to those instances, then uploading the SSL certificate to the pod directly is superfluous. Still, performing the immediately preceding step above and this step here is a recommended practice, because it ensures that if you do one day give out that FQDN to users to enter in their Horizon Clients, those clients can have trusted connections. Performing the immediately preceding step and this one here also provides you the ability to one day more quickly integrate the pod with Workspace ONE Access because you would have the FQDN mapped and the SSL certificate already in place on the pod.
10 Import a base image. On the Imported VMs page, use the **Reset Agent Pairing** action to pair the new image with Horizon Cloud. See **Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure**.

**Note**  Tech Preview: Use of Microsoft Windows 10 Enterprise multi-session operating system with App Volumes is currently in tech preview. To import a base image for that use case, use these steps instead: **Tech Preview - How To Configure a Microsoft Windows 10 Multi-Session Image for Use with App Volumes Features in Horizon Cloud Pods in Microsoft Azure**.

11 Depending on the type of end-user assignment the image will ultimately be used for, perform one or more of the following steps as appropriate.

- In an image VM that will be used for provisioning VDI desktops or native applications, install the third-party applications you want your end users to use in their VDI desktops, and configure other applicable customizations, such as setting desktop wallpaper, installing the NVIDIA GPU drivers (for GPU-enabled images), and so on. Also optimize the image for Microsoft Sysprep best practices, if not done as part of the import image process.

  - **For a Horizon Cloud Imported VM with a Microsoft Windows Client Operating System — Customize the VM for Your Organization's Needs.**

  - **Install NVIDIA Graphics Drivers in a GPU-Enabled VM Imported in Horizon Cloud.**

**Tip**  To further tune the image VM to provide an improved configuration for using VMware Blast Extreme in VDI use cases, a best practice is to read the **VMware Blast Extreme Optimization Guide** and perform additional tuning for codec options in the image according to that guide's recommendations for codec options.

- In a RDS-capable image that will be used for provisioning RDSH-based session desktops and remote applications, install the third-party applications you want to provide to your end users from that RDS image and configure other applicable customizations, such as setting desktop wallpaper, installing the NVIDIA GPU drivers (for GPU-enabled images), and so on. Also optimize the image for Microsoft Sysprep best practices, if not done as part of the import image process. If the imported VM is running one of the Microsoft Windows 10 Enterprise multi-session systems that includes Office 365 ProPlus by default, you should verify the VM is configured for shared computer activation for Office 365 ProPlus as described in the Microsoft documentation topic **Overview of shared computer activation for Office 365 ProPlus**. If Office 365 ProPlus is not configured for shared computer activation in the imported VM, use the method described in that Microsoft document that is appropriate for your situation.

  - **When using a Microsoft server operating system, see For a Horizon Cloud Imported VM with a Microsoft Windows Server Operating System — Customize the VM for Your Organization's Needs.**
When using a Microsoft Windows 10 Enterprise operating system, see For a Horizon Cloud Imported VM with a Microsoft Windows 10 Enterprise Multi-Session Operating System — Customize the VM for Your Organization’s Needs.

Install NVIDIA Graphics Drivers in a GPU-Enabled VM Imported in Horizon Cloud.

**Tip** To further tune the image VM to provide an improved configuration for using VMware Blast Extreme in VDI use cases, a best practice is to read the VMware Blast Extreme Optimization Guide and perform additional tuning for codec options in the image according to that guide's recommendations for codec options.

12 Convert that image into an assignable image, also known as sealing or publishing the image. See Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

13 To provision session-based RDSH desktops and remote applications from a published server image:
   a. Create a desktops RDSH farm to provide session desktops, and then create assignments to entitle end users to use those desktops. See Farms in Horizon Cloud and Create an RDSH Session Desktop Assignment.
   b. Create an applications RDSH farm to provide remote applications, add the applications to your application inventory, and then create assignments to entitle end users to use those remote applications. See Farms in Horizon Cloud, Remote Applications - Importing from RDSH Farms that are Provisioned by Horizon Cloud Pods in Microsoft Azure, and Remote Applications - Create a Remote Application Assignment for Remote Applications Provisioned By Horizon Cloud Pods in Microsoft Azure.

14 To provision VDI desktops from a published VDI desktop image, create a dedicated or floating VDI desktop assignment. See Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure and Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure.

15 To provision App Volumes applications to your end users, add the App Volumes applications to your application inventory and create an application assignment to entitle end users to use those applications. Then create a desktop assignment based on the same published image to entitle those end users to desktops in which they can launch those applications. See App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites.

16 When a pod is deployed with a gateway configuration, you must create a CNAME record in your DNS server that maps the fully qualified domain name (FQDN) that you entered in the deployment wizard to the appropriate Microsoft Azure load balancer resource that is configured in the pod for that gateway.

   For an external gateway enabled with a public IP address, map the FQDN that you entered in the deployment wizard to the gateway’s Microsoft Azure load balancer resource’s auto-generated public FQDN. Your DNS server record maps that Microsoft Azure load balancer’s auto-generated public FQDN with the FQDN that your end users
will use, and which is used in the uploaded certificate. The following code line
demonstrates an example. You locate the ID to use from the pod’s details page in the
console, after you have registered the Active Directory domain. If the external gateway
was deployed in its own VNet, use the ID that is displayed in the Deployment ID field.

ourApps.ourOrg.example.com   vwm-hcs-ID-uag.region.cloudapp.azure.com

- For an internal gateway or an external gateway without a public IP address, map the
  FQDN that you entered in the deployment wizard to the gateway’s Microsoft Azure load
  balancer resource’s private IP address. Your DNS server record maps that Microsoft
  Azure load balancer’s IP address with the FQDN that your end users will use, and which is
  used in the uploaded certificate. The following code line demonstrates an example.

ourApps.ourOrg.example.com   Azure-load-balancer-private-IP

After the pod is onboarded and you can access the Capacity page in the administrative
console, navigate to the Capacity page to see the vwm-hcs-ID-uag.region.cloudapp.azure.com
value needed to map your FQDN in your DNS.

For details on how to locate the Microsoft Azure load balancer’s FQDN in the console, see
Obtain the Pod Gateway’s Load Balancer Information to Map in your DNS Server.

When a pod is deployed to have RADIUS two-factor authentication for the pod’s gateways,
you must complete the following tasks:

- If you configured an external gateway with RADIUS settings and that RADIUS server is
  not reachable within the same VNet as used by the pod, or within the peered VNet
topology if you deployed the external gateway into its own VNet, verify, configure that
RADIUS server to allow client connections from the IP address of the external gateway’s
load balancer. In an external gateway configuration, the Unified Access Gateway
instances attempt contact with the RADIUS server using that load balancer address. To
allow the connections, ensure the load balancer resource’s IP address that is in that
external gateway’s resource group is specified as a client in your RADIUS server
configuration.

- If you configured an internal gateway, or an external gateway and your RADIUS server is
  reachable within the same VNet as used by the pod, configure the RADIUS server to
allow connections from the appropriate NICs that were created in the gateway’s resource
group in Microsoft Azure that must communicate with the RADIUS server. Your network
administrator determines the RADIUS server’s network visibility to the pod’s Azure Virtual
Network and subnets. Your RADIUS server must allow client connections from the IP
addresses of those gateway NICs that correspond to the subnet for which your network
administrator has given network visibility to the RADIUS server. The gateway’s resource
group in Microsoft Azure has four NICs that correspond to that subnet, two that are
currently active for the two Unified Access Gateway instances and two that are idle and
will become the active ones after the pod goes through an update. To support connectivity between the gateway and the RADIUS server both for ongoing pod operations and after each pod update, ensure the IP addresses of those four NICs are specified as clients in the RADIUS server configuration.

For information on how to obtain those IP addresses, see Update Your RADIUS System with the Required Horizon Cloud Pod Gateway Information.

After the above workflow steps are completed, your end users can launch their entitled desktops and remote applications using your FQDN in the Horizon Client or with HTML Access.

You can find in-depth details on how to accomplish each workflow step in the topics that are linked from each step above or in the companion guide. See Getting Started with VMware Horizon Cloud Service on Microsoft Azure.
Getting Started Using Your Horizon Cloud Environment

Your overall Horizon Cloud environment consists of the VMware-hosted cloud service, your provided capacity, and VMware software deployed into that capacity and connected to the cloud service. When the VMware software installed in that capacity is appropriately configured and connected to the cloud service, that configured entity is now a cloud-connected pod. Having at least one cloud-connected pod and completing the Active Directory registration process unlocks use of the cloud- and web-based Horizon Cloud Administration Console for management and administrative tasks involving those pods, including health monitoring, and help desk services.

For an overall introduction, see Introduction to Horizon Cloud and Onboarding Pods to Become Cloud-Connected Pods. Supported capacity environments are ones such as Microsoft Azure cloud or VMware Cloud™ on AWS or on-premises infrastructure. Each of these capacity environments provides for a specific pod type:

- **Pod in Microsoft Azure cloud**
- **Horizon pod connected using Horizon Cloud Connector** — the pod residing either on-premises or in VMware Cloud™ on AWS

Having at least one cloud-connected pod and completing the Active Directory registration process opens up use of the console for performing administrative tasks in the environment. The console provides an integrated view and centralized access to the cloud-based services that Horizon Cloud provides. This web-based console works in an industry-standard Web browser. For the list of supported Web browser types and versions, see Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud.

Depending on the type of capacity you have access to, you can use this same console for an automated pod deployment into that capacity and configure that pod for connection to Horizon Cloud. For some types of pods, even though they cannot be automatically deployed and configured, you can still cloud-connect those pods and work with them in this same administrative console, after performing some required connection steps.
Before you can use any cloud-hosted services or the console with a Horizon Cloud pod, you must:

- Connect your first pod to Horizon Cloud. Depending on the pod type you want to deploy first, see
  - Horizon pods — High-Level Workflow for Horizon Pods.
  - Horizon Cloud pods into Microsoft Azure — High-Level Workflow for Deploying a Pod into Microsoft Azure

- Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment to at least one of your Active Directory groups.

Registering the domain involves providing both:

- A primary domain-bind account and an auxiliary domain-bind account, used by Horizon Cloud to perform lookups in the Active Directory. By providing an auxiliary domain-bind account when you first register the domain, you prevent locking your administrator users out of the console if the primary bind account becomes inaccessible.

- A domain-join account, used by Horizon Cloud in pod operations that require joining virtual machines to the domain, such as when importing a VM from the Microsoft Azure Marketplace, creating farm RDSH instances, creating VDI desktop instances, and so on.

  **Note** In this release, the domain-join account is used by system operations primarily with pods in Microsoft Azure. Cloud-connected Horizon pods do not make use of the domain-join account that you specify in the Active Directory domain registration steps. However, even when you have only cloud-connected Horizon pods for your environment, it is prudent to complete the domain-join account step to ensure that the subsequent prompt to assign the Super Administrators role is activated. Assigning that role to an Active Directory domain group is a required step for all types of cloud-connected pods.

For the requirements on these domain-bind and domain-join accounts, see Service Accounts That Horizon Cloud Requires for Its Operations.

For details about the domain registration workflow, see Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment.
Afterwards, a best practice is to follow the recommended actions displayed in the Getting Started wizard.

**Important** Due to a known issue, when connecting Horizon pods on-premises and Horizon in VMware Cloud on AWS pods using Horizon Cloud Connector, unexpected results can occur if you do not complete the Active Directory domain registration process for the first pod before attempting to run the connector’s cloud-pairing workflow for subsequent pods. Even though the connector’s cloud-pairing workflow allows you to run it for multiple pods prior to completing the first Active Directory domain registration with Horizon Cloud, if you have not yet completed the first domain registration before running that cloud-pairing process on the next pod, this domain registration process might fail. In that case, you will have to:

1. Use the **Unplug** action in the web-based Horizon Cloud Connector configuration portal to remove the connection between each of the cloud-connected pods until you are down to a single cloud-connected pod.
2. Use the Horizon Cloud Administration Console to remove the failed registration, by following the steps in *Remove the Active Directory Domain Registration*.
3. Complete the first Active Directory domain registration process, related to that pod.
4. In the web-based Horizon Cloud Connector configuration portal, re-run the connector’s cloud-pairing workflow on the other pods.

After the first Active Directory domain is registered with Horizon Cloud for the pod’s use, you can subsequently **Register Additional Active Directory Domains as Cloud-Configured Active Directory Domains with Your Horizon Cloud Tenant Environment**. Registering additional Active Directory domains provides for the ability to specify those domains’ user accounts within the various
Horizon Cloud workflows that you perform using the administrative console, such as entitling your end users to pod-provisioned resources and assigning administrative roles to your administrative users. After the first Active Directory domain is registered, you can also configure additional auxiliary domain bind accounts and an auxiliary domain join account.

**Important** In this release, all pods must have line of sight to all of the cloud-configured Active Directory domains. When you register an Active Directory domain in the console, that domain is added to the set of cloud-configured Active Directory domains for your Horizon Cloud environment.

**Important** The administrative console is dynamic and reflects what is available at the current service level. However, when you have cloud-connected pods that are not yet updated to the latest levels of the pod's software, the console does not display those features that depend on the latest pod software level. Also, in a particular release, Horizon Cloud might include separately licensed features or features that are only available for particular tenant account configurations. The console dynamically reflects the elements related to such features only when your license or tenant account configuration includes use of such features.

When you are expecting to see a feature in the administrative console and do not see it, contact your VMware account representative to verify whether your license and tenant account configuration entitles its usage.

This chapter includes the following topics:

- Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment
- Log In to the Horizon Cloud Administration Console to Perform Management Tasks on Your Horizon Cloud Environment
- Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud
- Register Additional Active Directory Domains as Cloud-Configured Active Directory Domains with Your Horizon Cloud Tenant Environment
- Add Additional Auxiliary Bind Accounts for a Cloud-Configured Active Directory Domain in Horizon Cloud
- Best Practices about the Two Types of Roles You Give to People to Use the Horizon Cloud Administration Console to Work in Your Horizon Cloud Environment
- Give Administrative Roles to Individuals in Your Organization for Logging In To and Performing Actions in Your Horizon Cloud Tenant Environment Using the Horizon Cloud Administration Console
- Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment
- Enabling or Deactivating the Cloud Monitoring Service (CMS) for Your Horizon Cloud Tenant Environment
Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment

After your first successful pairing of your first pod with Horizon Cloud, you log in to Horizon Cloud at cloud.horizon.vmware.com to register an Active Directory domain with your Horizon Cloud environment. When the registration workflow is completed, that Active Directory domain is the first cloud-configured Active Directory domain in your Horizon Cloud customer account. The overall registration workflow is a multi-step process.

You should perform this Active Directory domain registration process immediately or shortly after cloud pairing your first pod with Horizon Cloud. A pod is cloud paired with Horizon Cloud either when pod deployment was initiated from Horizon Cloud, in the case of pods in Microsoft Azure, or initiated using the Horizon Cloud Connector, in the case of Horizon pods on-premises or in VMware Cloud on AWS. The overall steps of this registration workflow are:

1. Provide the Active Directory domain's name-related information, protocol-related information, and credentials of a domain-bind service account that Horizon Cloud can use to query that Active Directory domain. For information about what Horizon Cloud requires for that domain-bind account, see Domain Bind Account Requirements.

2. Provide the IP address for the DNS server that you want Horizon Cloud to use to resolve machine names, the organizational unit (OU) in which you want the pod's desktop-related virtual machines (VMs), and credentials of a domain-join service account that Horizon Cloud can use to join those desktop-related VMs. Such VMs include imported VMs, farm RDSH instances, and VDI desktop instances, and so on. For information about what Horizon Cloud requires for that domain-join account, see Domain Join Account Requirements.

3. Assign the Horizon Cloud Super Administrator role to an Active Directory domain group.

**Important** Please review all of the following bullet points for your understanding of the registration workflow.

- You must finish the entire Active Directory registration process for the first domain you are registering before you can move to other pages in the console. Main services are locked until you finish these tasks.

- Also, due to a known issue, when connecting Horizon on-premises and Horizon in VMware Cloud on AWS pods using Horizon Cloud Connector, unexpected results can occur if you do not complete this Active Directory domain registration process for the first pod before attempting to run the connector's cloud-pairing workflow for subsequent pods. Even though
the cloud-pairing workflow allows you to run it for multiple pods prior to completing the first Active Directory domain registration with Horizon Cloud, if you have not yet completed the first domain registration before running that cloud-pairing process on the next pod, this domain registration process might fail. In that case, you will have to:

- Use the Unplug action in the Horizon Cloud Connector configuration portal to remove the connection between each of the cloud-connected pods until you are down to a single cloud-connected pod.
- Remove the failed registration, by following the steps in Remove the Active Directory Domain Registration.
- Complete the first Active Directory domain registration process, related to that pod.
- Re-run the Horizon Cloud Connector workflow on the other pods.

Although in this release pods the domain-join account that you specify in these steps is used solely with pods in Microsoft Azure, when you have only cloud-connected Horizon pods for your environment, it is prudent to complete the domain-join account step to ensure that the subsequent prompt to assign the Super Administrator role is activated. Assigning that role to an Active Directory domain group is a required step for all cloud-connected pod types.

- Distribution groups are not supported, even if they are nested under a Security group. When creating Active Directory groups, always select Security for Group type.

**Important** In the Bind Username and Join Username text boxes related to the domain-bind and domain-join accounts, provide the account name itself, such as ouraccountname, like the user logon name without the domain name.

**Prerequisites**

Ensure that the Active Directory infrastructure is synchronized to an accurate time source to prevent the domain-join account step from failing. Such a failure might require you to contact VMware Support for assistance. If the domain-bind step succeeds, but the domain-join step fails, you can try resetting the domain and then investigate whether you need to adjust the time source. To reset the domain, see the steps in Remove the Active Directory Domain Registration.

Verify that your first pod is successfully deployed. The Capacity section of the Getting Started wizard indicates whether the first pod is successfully deployed by displaying a green checkmark icon (✓).
For the required primary and auxiliary domain-bind accounts, verify you have the information for two Active Directory user accounts that adhere to the requirements described in Domain Bind Account Requirements.

**Caution** To prevent accidental lockouts that would prevent you from logging in to the cloud-based console to manage your Horizon Cloud environment, you must ensure that your domain-bind accounts cannot expire, change, or be locked out. You must use this type of account configuration because the system uses the primary domain-bind account as a service account to query your Active Directory domain to verify credentials to log in to the console. If the primary domain-bind account becomes inaccessible for some reason, the system then uses the auxiliary domain-bind account. If both the primary and auxiliary domain-bind accounts expire or become inaccessible, then you will not be able to log in to the console and update the configuration to use an accessible domain-bind account.

The primary and auxiliary domain bind accounts are always assigned the Super Administrator role, which grants all the permissions to perform management actions in the console. You should ensure that your specified domain bind accounts are not accessible to users that you do not want to have Super Administrator permissions.

For the domain-join account, verify the account meets the requirements described in Domain Join Account Requirements. The domain-join account also must reside in an Active Directory group that you add to the Super Administrator role in the console. The Horizon Cloud roles can be assigned at a group-level only.

**Caution** This point is critical for system operations involving pods in Microsoft Azure. If the domain-join account you provide in the Active Directory domain registration's domain-join account step is not already in one of the Active Directory groups to which you can assign the Super Administrator role, create an Active Directory group for that account so that you can ensure the Super Administrator role can be assigned to that domain-join account.

If you only have one Active Directory group with the Super Administrator role assigned, do not remove that group from the Active Directory server. Doing so can cause issues with future logins.

**Important** For a pod in Microsoft Azure, this domain-join account must be in one of the Active Directory groups to which you grant the Super Administrator role. If the domain-join account is not in a group granted the Super Administrator role, system operations that involve joining the pod's virtual machines to the domain will fail, such as when importing base images or creating RDSH farms and virtual desktops.

Verify you have the Active Directory domain's NetBIOS name and DNS domain name. You will provide these values in the console's Register Active Directory window in the first step of this workflow. For an example of how to locate these values, see Locating the Information Required for the Horizon Cloud Register Active Directory Workflow's NetBIOS Name and DNS Domain Name Fields.
For future thinking, keep in mind that if you plan to later use the same Horizon Cloud customer account to connect other Horizon pods or deploy pods into Microsoft Azure for one unified environment, those pods will need to have line-of-sight to this same Active Directory domain at the time you connect or deploy those pods.

Procedure

1. Using a browser, log in to the cloud-based console at cloud.horizon.vmware.com using your preferred method.
   - In the My VMware Credentials section of the login page, enter My VMware account's credentials. The account credentials are the primary email address, such as user1@example.com, and the password that are set in the account's profile. This choice sends the authentication request to the Horizon Cloud control plane.
   - In the VMware Cloud Services section of the login page, click VMWARE CLOUD LOGIN. Clicking that button redirects the authentication request to VMware Cloud Services, to authenticate you according to your organization's configuration there. Your organization might have asked you to access their Horizon Cloud tenant using VMware Cloud Services.

The following screenshot illustrates logging in by entering My VMware account's credentials.
If you have not previously accepted the Horizon Cloud terms of service using those My VMware credentials, a terms of service notification box appears after you click the Login button. Accept the terms of service to continue.

When your login is successfully authenticated, the console opens and displays the Getting Started wizard.

If the Getting Started wizard is not displayed when you first log in, open it by clicking Settings > Getting Started.

2 In the Getting Started wizard, expand General Setup section if it is not already expanded.

3 Under Active Directory, click Configure.

4 In the Register Active Directory dialog box, provide the requested registration information.

**Important** Use Active Directory accounts that adhere to the guidelines for the primary and auxiliary domain-bind accounts as described in the prerequisites.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| NETBIOS Name            | - When the first cloud-connected pod in your customer account is a Horizon pod, at this step, the system displays a selection menu that is populated with the names of all of the Active Directory domains that the Horizon pod can see. Select the Active Directory domain that you want to register first.  
- When the first cloud-connected pod in your customer account is a pod in Microsoft Azure, at this step, the system displays a text box. Type in the NetBIOS name for the Active Directory domain that the pod can see. Typically this name does not contain a period. For an example of how to locate the value to use from your Active Directory domain environment, see Locating the Information Required for the Horizon Cloud Register Active Directory Workflow's NETBIOS Name and DNS Domain Name Fields.  
**Note** Keep in mind that if you plan to use this same Horizon Cloud customer account to connect additional Horizon pods or deploy pods into Microsoft Azure for one unified environment, those subsequent pods will need to have line-of-sight to this same Active Directory domain at the time when you connect or deploy those pods. |
| DNS Domain Name         | - When the first cloud-connected pod in your customer account is a Horizon pod, the system automatically displays the fully qualified DNS domain name for the Active Directory domain selected for NETBIOS Name.  
- When the first cloud-connected pod in your customer account is a pod in Microsoft Azure, the system displays a text box. Type in the fully qualified DNS domain name of the Active Directory domain you specified for NETBIOS Name. For an example of how to locate the value to use from your Active Directory domain environment, see Locating the Information Required for the Horizon Cloud Register Active Directory Workflow's NETBIOS Name and DNS Domain Name Fields. |
| Protocol                | Automatically displays LDAP, the supported protocol.                                                                                         |
## Register Active Directory

The following screenshot illustrates the Register Active Directory window when your first cloud-connected pod is in Microsoft Azure. The fields have values for an example Active Directory domain with NetBIOS name of ENAUTO and DNS domain name of ENAUTO.com.

### Table: Register Active Directory Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind Username</td>
<td>User account in the domain to use as the primary LDAP bind account.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Only provide the user name itself. Do not include the domain name here.</td>
</tr>
<tr>
<td>Bind Password</td>
<td>The password associated with the name in the <strong>Bind Username</strong> text box.</td>
</tr>
<tr>
<td>Auxiliary Account #1</td>
<td>In the <strong>Bind Username</strong> and <strong>Bind Password</strong> fields, type a user account in the domain to use as the auxiliary LDAP bind account and its associated password.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Only provide the user name itself. Do not include the domain name here.</td>
</tr>
<tr>
<td>Port</td>
<td>The default is LDAP -&gt; 389. You do not need to modify this text box unless you are using a non-standard port.</td>
</tr>
<tr>
<td>Domain Controller IP</td>
<td>(Optional) If you want Active Directory traffic to use a specific domain controller, type the preferred domain controller IP addresses, separated by commas. If this text box is left blank, the system uses any domain controller available for this Active Directory domain.</td>
</tr>
<tr>
<td>Context</td>
<td>LDAP naming context. This text box is autopopulated based on the information provided in the DNS Domain Name text box.</td>
</tr>
</tbody>
</table>
5 Click **Domain Bind**.

When the domain-bind step succeeds, the Domain Join dialog box appears and you can continue to the next step.

**Important**  If the domain-bind step fails, but you proceed to add the domain-join account and the system goes ahead to the Super Administrators role step, the registration process is not fully complete, even if the system proceeded to the next step. If this situation occurs, follow the steps in Remove the Active Directory Domain Registration and then start again with step 4.
6  In the Domain Join dialog box, provide the required information.

**Note**
- You must complete the required fields in this step when doing this Active Directory domain registration process regardless of pod type. Even though in this release the domain-join account is primarily used for system operations involving VMs located in pods in Microsoft Azure, completing this step ensures the next required step of granting the Super Administrator role gets completed.
- Use an Active Directory account that adheres to the guidelines for the domain-join account described in the prerequisites.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary DNS Server IP</strong></td>
<td>The IP address of the primary DNS Server that you want Horizon Cloud to use to resolve machine names. For a pod in Microsoft Azure, this DNS server must be able to resolve machine names inside of your Microsoft Azure cloud as well as resolve external names.</td>
</tr>
<tr>
<td><strong>Secondary DNS Server IP</strong></td>
<td>(Optional) IP of a secondary DNS Server</td>
</tr>
<tr>
<td><strong>Default OU</strong></td>
<td>Active Directory organization unit (OU) that you want used by the pod's desktop-related virtual machines such as imported VMs, farm RDSH VMs, VDI desktop instances. An Active Directory OU is of the form such as OU=NestedOrgName, OU=RootOrgName, DC=DomainComponent. The system default is CN=Computers. You can change the default to match your needs, like CN=myexample. For a description of nested organization names, see Considerations For Using Nested Active Directory Domain Organizational Units. Each individual entered OU must be 64 characters long or less, not counting the OU= portion of your entry. Microsoft limits an individual OU to 64 characters or less. An OU path that is longer than 64 characters, but with no individual OU having more than 64 characters, is valid. However, each individual OU must be 64 characters or less.</td>
</tr>
<tr>
<td><strong>Join Username</strong></td>
<td>User account in the Active Directory that has permissions to join computers to that Active Directory domain. <strong>Note</strong> Only provide the user name itself. Do not include the domain name here.</td>
</tr>
<tr>
<td><strong>Join Password</strong></td>
<td>The password associated with the name in the <strong>Join Username</strong> text box.</td>
</tr>
</tbody>
</table>
7 (Optional) Specify an auxiliary domain-join account.

If the primary domain-join account you specified becomes inaccessible, the system uses the auxiliary domain-join account for those operations in pods in Microsoft Azure that require joining the domain, such as importing image VMs, creating farm RDSH instances, creating VDI desktop instances, and so on.

**Note**
- Use an Active Directory account that adheres to the same guidelines for the primary domain-join account described in the prerequisites. Ensure that this auxiliary domain-join account has a different expiration time from the primary domain-join account, unless both accounts have **Never Expires** set. If both the primary and auxiliary domain-join accounts expire at the same time, the system's operations for sealing images and provisioning farm RDSH VMs and VDI desktop VMs will fail.
- You can add only one auxiliary domain-join account for each Active Directory you register with Horizon Cloud.
- If you do not add an auxiliary domain-join account at this time, you can add one later using the console.
- You can update or remove this account later.
- The agent-related software on a desktop-related virtual machine — such as a sealed image, farm RDSH instance, or VDI desktop instance — must be version 18.1 or later for the system to use the auxiliary domain-join account with that virtual machine.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auxiliary Join Username</strong></td>
<td>User account in the Active Directory that has permissions to join systems to that Active Directory domain.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> Only provide the account name in this field, such as ouraccountname, like the user logon name without the domain name. Entering slashes or at-signs will display an error.</td>
</tr>
<tr>
<td><strong>Auxiliary Join Password</strong></td>
<td>The password associated with the name in the <strong>Auxiliary Join Username</strong> text box.</td>
</tr>
</tbody>
</table>

8 Click **Save**.

When the domain-join step succeeds, the Add Super Administrator dialog box appears and you can continue to the next step.

**Important** If the domain-join step fails, the registration process is not fully complete. If this situation occurs, follow the steps in **Remove the Active Directory Domain Registration** and then start again with step 4.
9  In the Add Super Administrator dialog box, use the Active Directory search function to select
the Active Directory administrator group you want performing management actions on your
environment using this console.

This assignment ensures that at least one of your Active Directory domain's user accounts is
granted the permissions to log in to this console now that the Active Directory domain is
configured for this customer account.

Important To the Super Administrator role, add the Active Directory group which includes
the domain-join account, as described in the prerequisites. If the domain-join account is not in
any of the Active Directory groups that have the Super Administrator role, those system
operations for pods in Microsoft Azure that involve joining virtual machines to the domain will fail.

Caution After assigning this Active Directory group to the Super Administrator role, never
remove the specified administrator group from your Active Directory system or change its
GUID as it appears in your Active Directory system unless you have added another
administrator group to this Super Administrator role, as described in Assign Roles to Active
Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are
Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud
Tenant Environment. This Super Administrator role governs which of your AD user accounts
can log in to your Horizon Cloud tenant account and perform administrative operations in the
console. If you remove the group from your Active Directory system or change its GUID in
your Active Directory system, that change will not be communicated to the Horizon Cloud
control plane, and Horizon Cloud's knowledge of that AD group having the Super
Administrator role will be broken. If that group is the only group assigned to this Super
Administrator role, none of your AD accounts that used to have Super Administrator access
will be able to log in to your Horizon Cloud tenant account with the access to perform
administrative operations, which will block you from the ability to assign the role to another
AD group to regain administrative access. At which point, you'll have to contact VMware
Support to assist you in recovering administrative access to your tenant account.

10 Click Save.

When you click Save, the system returns you to the login screen. Now that you have
registered the pod with your Active Directory domain, the system requires you to log back in,
to enforce use of an Active Directory account along with the My VMware credentials. For
example, this time, you log in with your My VMware account and then with the Active
Directory account credentials of a user that is in the Active Directory group to which you just
assigned the Super Administrator role.

Results

The following items are now in place:

- The Active Directory domain is configured in the cloud plane as the first cloud-configured
  Active Directory domain associated with this Horizon Cloud customer account.
For a pod in Microsoft Azure, Horizon Cloud has the necessary domain-join account needed for those system operations involving joining desktop-related virtual machines to that domain. Also, the domain-join account has the required Super Administrator role, so that those operations operate properly.

Management activities in the console are now accessible.

The login flow as you log in to the console is changed, now that the Horizon Cloud tenant has its first registered Active Directory domain. For an overview of the login flow, see About Authentication to a Horizon Cloud Tenant Environment.

Users in the group to which you granted the Super Administrator role will be able to access the console and perform management activities when they log in using the associated My VMware account. To enable those administrators to use their own My VMware account credentials to authenticate with Horizon Cloud, complete the steps described in Give Administrative Roles to Individuals in Your Organization for Logging In To and Performing Actions in Your Horizon Cloud Tenant Environment Using the Horizon Cloud Administration Console.

User accounts from the registered Active Directory domain can be selected for assignments involving resources from pods in Microsoft Azure.

The console's help desk features can be used with user accounts from that registered Active Directory domain.

What to do next

From this point, you typically perform the following tasks:

Add additional auxiliary bind accounts to this Active Directory domain configuration. If the primary and first bind accounts you specified become inaccessible, the system uses the next auxiliary bind account to connect to the Active Directory. Having auxiliary bind accounts avoids locking out your administrator users from the console in situations where the primary bind account is inaccessible in the Active Directory domain. Add Additional Auxiliary Bind Accounts for a Cloud-Configured Active Directory Domain in Horizon Cloud.

Grant access to additional users to administer your environment. First add their My VMware accounts with associated Horizon Cloud roles, and then give their Active Directory accounts the appropriate Horizon Cloud role. See Give Administrative Roles to Individuals in Your Organization for Logging In To and Performing Actions in Your Horizon Cloud Tenant Environment Using the Horizon Cloud Administration Console and Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment.

Continue with the Getting Started wizard’s steps. See About the Horizon Cloud Getting Started Wizard.
Navigate to the Dashboard and other areas of the console to explore or perform other management tasks. See Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud.

If you have additional Active Directory domains with users to whom you want to grant management access to the console or end users to whom you want to give assignments, you can register those Active Directory domains also. See Register Additional Active Directory Domains as Cloud-Configured Active Directory Domains with Your Horizon Cloud Tenant Environment.

Assign the demo administrator role to those users in this domain to whom you want to grant read-only access to the console. See Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment.

Service Accounts That Horizon Cloud Requires for Its Operations

Horizon Cloud requires use of two accounts in your Active Directory (AD) domain to use as service accounts. This topic describes the requirements that those two accounts must meet.

Horizon Cloud requires that you specify two AD accounts to use as these two service accounts.

- A domain bind account that is used to perform lookups in your AD domain.
- A domain join account that is used for joining computer accounts to the domain and performing Sysprep operations.

**Note** For pods in Microsoft Azure, the system uses this domain join account in operations that require joining virtual machines to the domain, such as when importing an image from the Microsoft Azure Marketplace, creating farm RDSH instances, creating VDI desktop instances, and so on.

You use the cloud-based administrative console to provide the credentials for these accounts to Horizon Cloud.

You must ensure that the Active Directory accounts you specify for these service accounts meet the following requirements that Horizon Cloud requires for its operations.

**Important** You must ensure that your domain bind and domain join accounts continue to have the permissions as described here on all the OUs and objects that you are using and expect to use with the system. Horizon Cloud cannot pre-populate or predict in advance which Active Directory groups you might want to use in the environment. You must configure Horizon Cloud with the domain bind account and domain join account using the console.

**Domain Bind Account Requirements**

- The domain bind account cannot expire, change, or be locked out. You must use this type of account configuration because the system uses the primary domain bind account as a service
account to query Active Directory. If the primary domain bind account becomes inaccessible for some reason, the system then uses the auxiliary domain bind account. If both the primary and auxiliary domain bind accounts expire or become inaccessible, then you cannot log in to the cloud-based console and update the configuration.

**Important** If both the primary and auxiliary domain bind accounts expire or become inaccessible, then you cannot log in to the console and update the configuration with working domain bind account information. If you do not set **Never Expires** on the primary or auxiliary domain bind accounts, you should make them have different expiration times. You must keep track as the expiration time approaches and update your Horizon Cloud domain bind account information before the expiration time is reached.

- The domain bind account requires the `sAMAccountName` attribute. The `sAMAccountName` attribute must be 20 characters or less and cannot contain any of the following characters: `"\[;:|=, + * ? < >`

- The domain bind account must have read permissions which can look up AD accounts for all the AD organizational units (OUs) that you anticipate using in the Desktop-as-a-Service operations that Horizon Cloud provides — operations such as assigning desktop VMs to your end users. The domain bind account needs the ability to enumerate objects from your Active Directory. The domain bind account requires the following permissions on all the OUs and objects that you anticipate and expect to use with Horizon Cloud:
  - List Contents
  - Read All Properties
  - Read Permissions
  - Read `tokenGroupsGlobalAndUniversal` (implied by the Read All Properties permission)

**Important** Generally speaking, the domain bind accounts should be granted the default out-of-the-box read-access-related permissions that are typically granted to Authenticated Users in a Microsoft Active Directory deployment. In an out-of-the-box Microsoft Active Directory deployment, those default settings typically granted to Authenticated Users usually give a standard domain user account the ability to do the required enumeration that Horizon Cloud needs for the domain bind account. However, if your organization's AD administrators have chosen to lock down read-access-related permissions for regular users, you must request those AD administrators preserve the Authenticated Users standard defaults for the domain bind accounts you will use for Horizon Cloud.

- The domain bind account is always assigned the Super Administrator role, which grants all the permissions to perform management actions in the console. You should ensure that the domain bind account is not accessible to users that you do not want to have Super Administrator permissions.

**Domain Join Account Requirements**

- The domain join account cannot change or be locked out.
Ensure that you meet at least one of the following criteria:

- In your Active Directory, set the domain join account to **Never Expires**.
- Alternatively, configure an auxiliary domain join account that has a different expiration time than the first domain join account. If you choose this method, ensure that the auxiliary domain join account meets the same requirements as the main domain join account you configure in the console.

**Caution** If the domain join account expires and you have no working auxiliary domain join account configured, Horizon Cloud operations for sealing images and provisioning farm RDSH VMs and VDI desktop VMs will fail.

- The domain join account requires the **sAMAccountName** attribute. The **sAMAccountName** attribute must be 20 characters or less and cannot contain any of the following characters: "/\[\];|=\,*\?\<\>
- The domain join account needs the AD permissions in the following list.

**Important**

- Some of the AD permissions in the list are typically assigned by Active Directory to accounts by default. However, if you have limited the security permission in your Active Directory, you must ensure that the domain join account has these permissions for the OUs and objects that you anticipate and expect to use with Horizon Cloud.
- In Microsoft Active Directory, when you create a new OU, the system might automatically set the **Prevent Accidental Deletion** attribute which applies a **Deny** to the Delete All Child Objects permission for the newly created OU and all descendant objects. As a result, if you explicitly assigned the Delete Computer Objects permission to the domain join account, in the case of a newly created OU, Active Directory might have applied an override to that explicitly assigned Delete Computer Objects permission. Because clearing the **Prevent Accidental Deletion** flag might not automatically clear the **Deny** that Active Directory applied to the Delete All Child Objects permission, in the case of a newly added OU, you might have to verify and manually clear the **Deny** permission set for Delete All Child Objects in the OU and all child OUs before using the domain join account in the Horizon Cloud console.

The system performs explicit permission checks on the domain join account within the OU you specify in the Active Directory registration workflow (in the **Default OU** text box in that workflow) and within the OUs you specify in the farms and VDI desktop assignments you create, if those farm and VDI desktop assignment **Computer OU** text boxes are different from the default OU in the Active Directory registration.
To cover the cases where you might ever use a sub-OU, a best practice is for you to set these permissions to apply for all descendant objects of the Computer OU. The AD permissions required on the domain join account are shown in the table below.

<table>
<thead>
<tr>
<th>Access</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>List Contents</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Read All Properties</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Write All Properties</td>
<td>All descendant objects</td>
</tr>
<tr>
<td>Read Permissions</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Reset Password</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Create Computer Objects</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Delete Computer Objects</td>
<td>This object and all descendant objects</td>
</tr>
</tbody>
</table>

**Caution** Although you can set Full Control instead of setting all the permissions separately, it is still recommended that you set the permissions separately.

**Locating the Information Required for the Horizon Cloud Register Active Directory Workflow's NETBIOS Name and DNS Domain Name Fields**

This topic gives an example for how you can locate the information required for the **NETBIOS Name** and **DNS Domain Name** fields. These fields are required in the workflow for registering your Active Directory domain with your Horizon Cloud environment.

When you begin the workflow for the Active Directory domain registration, the console displays the Register Active Directory window. The following screenshot shows the top portion of the window.

**Register Active Directory**

Provide the Active Directory domain information and domain bind account credentials. Principals will automatically be granted Super Administrator access for recovery purposes.

<table>
<thead>
<tr>
<th>NetBIOS Name:*</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Domain Name:*</td>
<td></td>
</tr>
</tbody>
</table>
You can obtain the information required for the **NETBIOS Name** and **DNS Domain Name** fields from your Active Directory domain environment. For a typical Active Directory domain environment, the NetBIOS name is the one that appears in the **Domain name (pre-Windows 2000)** field as viewed in an Active Directory management tools interface, such as when using the Active Directory Users and Computers snap-in to the Microsoft Management Console (MMC). You can also obtain the DNS domain name from that same snap-in.

This topic describes one method for locating the required information using the Active Directory Users and Computers MMC snap-in. When that snap-in installed on a Microsoft Windows server with Active Directory Domain Services or Remote Server Administration Tools installed, you can open the snap-in by running `dsa.msc`.

**Procedure**

1. Open the Active Directory Users and Computers configuration window to where you can see the domain configuration.

   The following screenshot is an example of the window for an Active Directory domain that has a DNS domain name of `ENAUTO.com`.

   ![Active Directory Users and Computers](image)

2. View the domain's properties by right-clicking the domain-name icon and clicking **Properties**.

   The following screenshots are examples.
The domain's NetBIOS name is the name in the **Domain name (pre-Windows 2000)** field. Typically this name does not include a period (.), You provide this name in the Register Active Directory window's **NETBIOS Name** field.

The name at the top of the Properties name is the domain's full DNS name. Typically this name does contain a period, like in the name **ENAUTO.com**. You provide this full DNS name in the Register Active Directory window's **DNS Domain Name** field.
The following screenshot is the console's Register Active Directory window when registering the example ENAUTO.com domain shown in the preceding screenshots. This domain's NetBIOS name is ENAUTO and its DNS domain name is ENAUTO.com.

<table>
<thead>
<tr>
<th>NetBIOS Name:*</th>
<th>ENAUTO</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Domain Name:*</td>
<td>ENAUTO.com</td>
</tr>
</tbody>
</table>

**Horizon Cloud Support for Active Directory Domain Controllers That Have LDAP Server Signing Requirements**

Horizon Cloud supports the use of Active Directory Domain Controllers that have the *Domain controller: LDAP server signing requirements* security policy setting set to *Require signing*.

Horizon Cloud uses secure Generic Security Services Application Program Interface (GSSAPI) LDAP binds, with both signing and sealing enabled. This feature provides both LDAP data integrity and privacy. This feature also gives Horizon Cloud pods the ability to connect to Domain Controllers that have the *Domain controller: LDAP server signing requirements* security policy setting set to *Require signing*.

**About External and Forest Trust Support for Cloud-Connected Pods in Horizon Cloud**

In a complex Active Directory environment, your organization might have a scenario in which your pod-provisioned resources are joined to a domain in one forest while your user accounts are in a domain in another forest, and you have an external or forest trust that allows users in their domain to access resources in the other domain. This topic describes the Horizon Cloud support for traversing those external trusts or forest trusts that are between your domains of different forests.

In the administrative console, you create what are called assignments to entitle users and groups to your pod-provisioned resources. When you use the console to create a VDI desktop assignment or a farm, you specify in which of the cloud-registered domains to locate the resulting desktop VMs or farm session-host VMs. You also use the console to configure the assignments to provide use of those resources to users and groups in your Active Directory domains. To accommodate use of complex domain environments for these assignments, Horizon Cloud provides support for:

- Entitling pod-provisioned resources that are joined to a domain in one forest to users and groups joined to a domain in a different forest.
- One-way trusts.

**Important** Use of domain local groups for Horizon Cloud assignments is not supported. To entitle groups from different forests to the same assignment, you must register one universal group from each forest.
For Horizon Cloud support of your external and forest trusts, you must:

- Register with Horizon Cloud all domains from all forests that contain accounts that you wish to use with resources provisioned from the cloud-connected pods. The system cannot validate a forest’s groups unless the group’s domain is registered with Horizon Cloud. See Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment and Register Additional Active Directory Domains as Cloud-Configured Active Directory Domains with Your Horizon Cloud Tenant Environment. As described in those topics, all of the cloud-connected pods must have line-of-sight to every cloud-registered Active Directory domain.

- Register forest root domains from both sides of a forest trust. This requirement must be met even if you have no users or desktops in the forest root domains. This requirement allows Horizon Cloud to connect to the forest roots and decode the relevant TDOs (Trusted Domain Objects).

- Enable global catalog for at least one of the registered domains in each forest. For optimal performance, all registered domains should have global catalog enabled.

- To enable entitling groups from different forests to the same assignment in Horizon Cloud, register at least one universal group from each forest.

- Follow a hierarchical structure for the forest domains’ DNS name and root naming context. For example, if the parent domain is called example.edu, a child domain could be called vpc.example.edu but not vpc.com.

- Avoid having a domain from an externally trusted forest with a NETBIOS name that clashes with another registered domain, because such domains are excluded from the system’s enumeration. The registered NETBIOS name will take precedence over a clashing NETBIOS name found during the system’s enumeration of a trusted forest’s domains.

Log In to the Horizon Cloud Administration Console to Perform Management Tasks on Your Horizon Cloud Environment

You perform management and administrative tasks on your cloud-connected pods using the cloud-based Horizon Cloud Administration Console. The console is a browser-based interface provided by the cloud service. You use an industry standard browser to log in to the console.
Some details of the login steps vary depending on the configuration of your specific environment.

**Note**  Login authentication into the cloud-based console relies on authenticating account credentials either with the My VMware account system or VMware Cloud Services system. If those systems are experiencing a system outage and cannot take authentication requests, you will not be able to log in to the console during that time period. If you encounter issues logging in to the console's first login screen, check the Horizon Cloud System Status page at [https://status.horizon.vmware.com](https://status.horizon.vmware.com) to see the latest system status. On that page, you can also subscribe to receive updates.

See [About Authentication to a Horizon Cloud Tenant Environment](#) for an overview of the authentication flows used to access the console.

**Prerequisites**

Verify that you have the credentials of a My VMware account that is associated with the Horizon Cloud tenant environment.

When an Active Directory domain is already registered with the Horizon Cloud tenant, verify that you have the credentials for an Active Directory account in that domain that has access permissions.

**Procedure**

1. Navigate to the cloud service at [https://cloud.horizon.vmware.com/](https://cloud.horizon.vmware.com/) and log in using your preferred method.

   The methods are described in [About Authentication to a Horizon Cloud Tenant Environment](#). The following screenshot illustrates the login screen, using the My VMware credentials section of the login window.
If you have not previously accepted the Horizon Cloud terms of service using those My VMware credentials, a terms of service notification box appears after you click the Login button. Accept the terms of service to continue.

2 Follow the on-screen flow, according to the authentication flow that is applicable to the Horizon Cloud tenant's state. For details about the tenant states and flows, see About Authentication to a Horizon Cloud Tenant Environment.
Results

The console appears.

Important

- If you submit your correct Active Directory credentials in the Active Directory login screen and the My VMware login screen re-appears and displays an error message that states AD permissions mismatch. Please contact your main administrator to review your assigned roles. This means that your Active Directory user account is in an Active Directory group that has been Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment that provides fewer permissions than the role assigned to you in the My VMware section of the Customizable General Settings for Your Horizon Cloud Tenant Environment. This discrepancy prevents you from logging in. To correct this issue, a person in your organization that has administrator privileges for the Horizon Cloud tenant can log in and change your assigned role in the My VMware section of the General Settings page so that the permissions are consistent with the permissions for your role selected on the Roles & Permissions page. For information about how the two types of roles work together, see Best Practices about the Two Types of Roles You Give to People to Use the Horizon Cloud Administration Console to Work in Your Horizon Cloud Environment.

That message will not appear when the My VMware account entered in the first login screen is the one marked as the Owner in the cloud plane's tenant record for the environment. The system allows that owning account to log in even if there is a role permissions mismatch with the Active Directory group's role.

- If maintenance is being performed on your environment, a message appears on the login screen indicating that you are unable to log in during the maintenance period.

- If you mistype the Active Directory user name or password, the system redisplays the My VMware login screen. In this situation, you have to go through the My VMware login screen again to get to the Active Directory login screen and try again.

What to do next

If applicable, perform the Active Directory domain registration process to register your Active Directory domain with your Horizon Cloud customer account. See Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment. You must finish the entire Active Directory registration process before you can work with any other services.

Note  The default time period for which an administrator can be logged in to the console is 30 minutes. After that time has elapsed, the authenticated session ends and the administrator must log back in. When you have at least one pod in Microsoft Azure, you can adjust this time in the General Settings page's Session Timeout section, by editing the Admin Portal Timeout value. When you have only Horizon pods in your environment, you cannot change the 30 minutes default. See Customizable General Settings for Your Horizon Cloud Tenant Environment.
About Authentication to a Horizon Cloud Tenant Environment

You manage a Horizon Cloud tenant environment using its administrative console. Ability to access that console relies on an authentication flow that provides for authentication of a My VMware account that has authorization to access that Horizon Cloud tenant and for authentication using an Active Directory domain that is registered to the same tenant.

For the login steps and a screenshot depicting the login screen, see Log In to the Horizon Cloud Administration Console to Perform Management Tasks on Your Horizon Cloud Environment.

When you have integrated your Horizon Cloud environment with your Workspace ONE environment, you can log into your Horizon Cloud tenant using either Workspace ONE or the Horizon Cloud login screen.

**Note** Users created with Just-in-Time user provisioning are not able to log in using the Horizon Cloud login screen. These users must log in using Workspace ONE.

In all of the following tenant states, the login screen provides two methods for authenticating to the tenant and accessing the console.

- In the **My VMware Credentials** section of the login screen, enter My VMware account’s credentials. The account credentials are the primary email address, such as `user@example.com`, and the password that are set in the account's profile. This choice sends the authentication request to the Horizon Cloud control plane.

- In the **VMware Cloud Services** section of the login screen, click **VMWARE CLOUD LOGIN**. Clicking that button redirects the authentication request to VMware Cloud Services, to authenticate you according to your organization's configuration there. Your organization might have asked you to access their Horizon Cloud tenant using VMware Cloud Services and has the appropriate configuration in VMware Cloud Services to provide that access.

After using one of the above methods, the specific authentication flow that you see will vary depending on the state of the Horizon Cloud tenant at the time you are logging in — whether you are logging in before the tenant has any cloud-connected pods, after it has a single cloud-connected pod but no registered Active Directory domains, when the tenant has one registered Active Directory domain, and so on.

**Initial Tenant State — No Cloud-Connected Pods**

After you authenticate to the tenant, the console displays the Getting Started wizard with the **Capacity** section expanded by default. Until you cloud connect a pod, the Getting Started wizard is the only accessible user-interface page. At this point in time, you need to onboard a pod to Horizon Cloud to move the tenant beyond this initial state. For information about onboarding a pod, see Onboarding to Horizon Cloud for Microsoft Azure, Horizon On-Premises, and Horizon on VMware Cloud on AWS and its subtopics.

The following screenshot illustrates the console when the tenant is in this initial state.
Tenant with One Cloud-Connected Pod and Zero Registered Active Directory Domains

After you authenticate to the tenant, the console's display might look little different than in the initial state. The Getting Started wizard is displayed with the Capacity section expanded by default and is the only accessible user-interface page. However, now you have access to configure your organization's Active Directory domain with this Horizon Cloud tenant. To move the tenant beyond this state, complete the steps in Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment.

Tenant with a Single Registered Active Directory Domain

In this state, the authentication flow is different depending on which method you choose to use in the login screen.

- Using the My VMware Credentials section of the login screen — after a successful authentication with the cloud plane using the provided credentials, the Horizon Cloud Active Directory login window is displayed with the name of the Active Directory domain that is registered with the tenant. In this Active Directory login window, provide credentials of your Active Directory account. After a successful authentication in this login screen, the console is displayed. The following screenshot illustrates this login window when a domain named EXAMPLEDOMAIN is registered with the tenant.
Clicking the **VMware Cloud Services** button — the authentication request is sent to VMware Cloud Services. After a successful authentication with VMware Cloud Services, one of two things happens:

- If the registered Active Directory domain that is registered with the Horizon Cloud tenant is also configured in VMware Cloud Services for federated identity management, the authentication flows according to that configuration. The authentication flow omits the Horizon Cloud Active Directory login window. After you authenticate according to what your organization configured in VMware Cloud Services for federated identity management, the console is displayed.

- If the registered Active Directory domain is not federated in VMware Cloud Services, your browser is redirected to the Horizon Cloud Active Directory login window. In this Active Directory login window, provide credentials of your Active Directory account. After a successful authentication in this login screen, the console is displayed.

**Note**  
As of May 2020, this federated identity management feature is in Limited Availability and is currently qualified for use only when the Horizon Cloud tenant's cloud-connected pods are all pods in Microsoft Azure.
Tenant with More than One Registered Active Directory Domains

In this state, the authentication flow has these differences compared with the above single registered Active Directory domain state.

- In the authentication flow where the Horizon Cloud Active Directory login window is displayed, you use the drop-down list to select the domain for which your provided credentials are valid. The following screenshot illustrates an example where the Horizon Cloud tenant has two registered Active Directory domains, DOMAIN-A and DOMAIN-B.

![Welcome to VMware Horizon Cloud](image)

- If you use the VMware Cloud Services authentication flow and your account belongs to an Active Directory domain that is both registered with the tenant and also configured for federated identity management, the authentication flow omits the Horizon Cloud Active Directory login window as described in the previous section. However, if your account belongs to an Active Directory domain that is registered with the tenant but your organization has not configured that domain for federated identity management, your browser is redirected to the Horizon Cloud Active Directory login window. In this case, you select your domain in the drop-down and provide your Active Directory credentials to log in.

**Note**  As of May 2020, this federated identity management feature is in Limited Availability and is currently qualified for use only when the Horizon Cloud tenant's cloud-connected pods are all pods in Microsoft Azure.

Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud

This cloud- and web-based console is the user interface for your single point of control for managing and monitoring your Horizon Cloud environment and your cloud-connected pods.
Browser Experience

The console is compatible with recent versions of Google Chrome, Mozilla Firefox, and Microsoft Edge. Use of the console in Microsoft Internet Explorer 11 is deprecated and will give a sub-optimal experience. The console is not supported for use in Apple Safari, although you can try using the console in Apple Safari. If you attempt to access the console using a non-modern browser such as Microsoft Internet Explorer 11, the console displays an information message to use an up-to-date browser. For the best user experience, use the most recent versions of Google Chrome, Mozilla Firefox, and Microsoft Edge.

Navigation and Functional Areas

On the left side of the interface is the Navigation bar, providing a hierarchy for navigating to the main areas of the user interface. The following table describes each area starting with at the top of the bar.

<table>
<thead>
<tr>
<th>Category</th>
<th>Functional Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor</td>
<td>The Monitor category provides access to the unified dashboard, activity monitoring, reports, and notifications. For an overview of the pages in this category, see About the Monitor Menu in the Horizon Cloud Administration Console and topics Health Visibility and Insights into Your Cloud-Connected Pods Provided by the Cloud Monitoring Service in Horizon Cloud, Activity Page, Reports Page, and Notifications Page.</td>
</tr>
<tr>
<td>Assignments</td>
<td>The Assignments category provides access to assignments and assignment-related actions and workflow. For an overview of the pages in this category and links to the various assignment-related workflows you can do with assignments, see About the Assignments Menu in the Horizon Cloud Administration Console.</td>
</tr>
</tbody>
</table>
The Inventory category provides access to desktop-as-a-service artifacts from your pods, such as imported base VMs, sealed images, farms, and applications. For an overview of the pages in this category and tasks you can do in them, see About the Inventory Menu in the Horizon Cloud Administration Console.

**Note**  Most of this category's pages are only applicable to pods in Microsoft Azure.

The Settings category provides access to pages that involve settings and configurations in your environment. For an overview of the pages in this category and the tasks you can do in them, see About the Settings Menu in the Horizon Cloud Administration Console.

**Important**  The administrative console is dynamic and reflects what is available at the current service level. However, when you have cloud-connected pods that are not yet updated to the latest levels of the pod's software, the console does not display those features that depend on the latest pod software level. Also, in a particular release, Horizon Cloud might include separately licensed features or features that are only available for particular tenant account configurations. The console dynamically reflects the elements related to such features only when your license or tenant account configuration includes use of such features.

When you are expecting to see a feature in the administrative console and do not see it, contact your VMware account representative to verify whether your license and tenant account configuration entitles its usage.

For example, in this release, some areas of the console are applicable only for pods deployed in Microsoft Azure. When your cloud-connected pods consist only Horizon pods deployed on-premises or into VMware Cloud on AWS, those areas that are applicable only for pods in Microsoft Azure display a graphic and message. The following screenshot is a portion of what is displayed.

When your cloud-connected pods include both pods in Microsoft Azure and Horizon pods, you might see an explanatory banner on various pages.
Upper Toolbar

In addition to the Logout action under the logged-in user name, the upper part of the console provides:

- The console's search feature to search users or VMs ( ). For more information, see Using the Console's Search Feature.
- Notifications ( ). For more information, see Notifications Page.
- Feedback ( ). For more information, see Sharing Your Feedback with VMware.
- Support-related information ( ) such as what's new in the current service level, Web-based documentation, build information, and requesting support.
- Language selector, to display the console in its supported languages.

Register Additional Active Directory Domains as Cloud-Configured Active Directory Domains with Your Horizon Cloud Tenant Environment

You can optionally register additional Active Directory domains with your Horizon Cloud customer account. Registering the Active Directory domain adds that domain to the set of cloud-configured domains associated with that Horizon Cloud customer account. When the domain is in the set of cloud-configured domains, then you can enable user accounts and groups from that domain to use features that the system provides, such as help desk administrators using the help desk features or end users using the desktop-related features.

**Important** In the Bind Username and Join Username text boxes related to the domain-bind and domain-join accounts, provide the account name itself, such as ouraccountname, like the user logon name without the domain name.

**Note** Distribution groups are not supported, even if they are nested under a Security group. When creating Active Directory groups, always select Security for Group type.

**Prerequisites**

Ensure that the Active Directory infrastructure is synchronized to an accurate time source to prevent the domain-join account step from failing. Such a failure might require you to contact VMware Support for assistance. If the domain-bind step succeeds, but the domain-join step fails, you can try resetting the domain and then investigate whether you need to adjust the time source. To reset the domain, see the steps in Remove the Active Directory Domain Registration.
For the required primary and auxiliary domain-bind accounts, verify you have the information for two Active Directory user accounts that adhere to the requirements described in Domain Bind Account Requirements.

**Caution** To prevent accidental lockouts that would prevent you from logging in to the cloud-based console to manage your Horizon Cloud environment, you must ensure that your domain-bind accounts cannot expire, change, or be locked out. You must use this type of account configuration because the system uses the primary domain-bind account as a service account to query your Active Directory domain to verify credentials to log in to the console. If the primary domain-bind account becomes inaccessible for some reason, the system then uses the auxiliary domain-bind account. If both the primary and auxiliary domain-bind accounts expire or become inaccessible, then you will not be able to log in to the console and update the configuration to use an accessible domain-bind account.

The primary and auxiliary domain bind accounts are always assigned the Super Administrator role, which grants all the permissions to perform management actions in the console. You should ensure that your specified domain bind accounts are not accessible to users that you do not want to have Super Administrator permissions.

For the domain-join account, verify the account meets the requirements described in Domain Join Account Requirements. The domain-join account also must reside in an Active Directory group that you add to the Super Administrator role in the console. The Horizon Cloud roles can be assigned at a group-level only.

**Caution** This point is critical for system operations involving pods in Microsoft Azure. If the domain-join account you provide in the Active Directory domain registration's domain-join account step is not already in one of the Active Directory groups to which you can assign the Super Administrator role, create an Active Directory group for that account so that you can ensure the Super Administrator role can be assigned to that domain-join account.

If you only have one Active Directory group with the Super Administrator role assigned, do not remove that group from the Active Directory server. Doing so can cause issues with future logins.

Verify you have the Active Directory domain's NetBIOS name and DNS domain name. You will provide these values in the console's Register Active Directory window in the first step of this workflow. For an example of how to locate these values, see Locating the Information Required for the Horizon Cloud Register Active Directory Workflow's NETBIOS Name and DNS Domain Name Fields.

**Caution** When you register an additional Active Directory domain, ensure that all of your cloud-connected pods have line-of-sight to that domain. All of the pods the same customer account record need to be able to reach the same set of cloud-configured Active Directory domains that are registered with that account. All of the pods need to be able to reach the same Active Directory servers and the DNS configuration needs to resolve all of those cloud-configured Active Directory domains.
Procedure

1. In the console, select **Settings > Active Directory**.
2. Click **Register**.
3. In the Register Active Directory dialog box, provide the requested registration information.

   **Important** Use Active Directory accounts that adhere to the guidelines for the primary and auxiliary domain-bind accounts as described in the prerequisites.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| NETBIOS Name       | ■ When you have cloud-connected Horizon pods, at this step, the system displays a selection menu that is populated with the names of all of the Active Directory domains that the Horizon pod can see. Select the Active Directory domain that you want to register first.  
                      ■ When your only cloud-connected pods are in Microsoft Azure, at this step, the system displays a text box. Type in the NetBIOS name for the Active Directory domain that you want to register. Typically this name does not contain a period. For an example of how to locate the value to use from your Active Directory domain environment, see Locating the Information Required for the Horizon Cloud Register Active Directory Workflow's NETBIOS Name and DNS Domain Name Fields. |
| DNS Domain Name    | ■ When you have cloud-connected Horizon pods, the system automatically displays the fully qualified domain name for the Active Directory domain selected for **NETBIOS Name**.    
                      ■ When your only cloud-connected pods are in Microsoft Azure, the system displays a text box. Type in the fully qualified DNS domain name of the Active Directory domain you specified for **NETBIOS Name**. For an example of how to locate the value to use from your Active Directory domain environment, see Locating the Information Required for the Horizon Cloud Register Active Directory Workflow's NETBIOS Name and DNS Domain Name Fields. |
| Protocol           | Automatically displays LDAP, the supported protocol.                                                                                         |
| Bind Username      | User account in the domain to use as the primary LDAP bind account.  
                      **Note** Only provide the user name itself. Do not include the domain name here.                                                     |
| Bind Password      | The password associated with the name in the **Bind Username** text box.                                                                     |
| Auxiliary Account #1 | In the **Bind Username** and **Bind Password** fields, type a user account in the domain to use as the auxiliary LDAP bind account and its associated password.  
                          **Note** Only provide the user name itself. Do not include the domain name here.                                                       |

4. Click **Domain Bind**.

   When the domain-bind step succeeds, the Domain Join dialog box appears and you can continue to the next step.
5 In the Domain Join dialog box, provide the required information.

**Note** Use an Active Directory account that adheres to the guidelines for the domain-join account described in the prerequisites.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary DNS Server IP</td>
<td>The IP address of the primary DNS Server that you want Horizon Cloud to use to resolve machine names. For a pod in Microsoft Azure, this DNS server must be able to resolve machine names inside of your Microsoft Azure cloud as well as resolve external names.</td>
</tr>
<tr>
<td>Secondary DNS Server IP</td>
<td>(Optional) IP of a secondary DNS Server</td>
</tr>
<tr>
<td>Default OU</td>
<td>Active Directory organization unit (OU) that you want used by the pod’s desktop-related virtual machines such as imported VMs, farm RDSH VMs, VDI desktop instances. An Active Directory OU is of the form such as OU=NestedOrgName, OU=RootOrgName,DC=DomainComponent. The system default is CN=Computers. You can change the default to match your needs, like CN=myexample.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> For a description of nested organization names, see Considerations For Using Nested Active Directory Domain Organizational Units. Each individual entered OU must be 64 characters long or less, not counting the OU= portion of your entry. Microsoft limits an individual OU to 64 characters or less. An OU path that is longer than 64 characters, but with no individual OU having more than 64 characters, is valid. However, each individual OU must be 64 characters or less.</td>
</tr>
<tr>
<td>Join Username</td>
<td>User account in the Active Directory that has permissions to join computers to that Active Directory domain.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Only provide the user name itself. Do not include the domain name here.</td>
</tr>
<tr>
<td>Join Password</td>
<td>The password associated with the name in the <strong>Join Username</strong> text box.</td>
</tr>
</tbody>
</table>
6 (Optional) Specify an auxiliary domain-join account.

If the primary domain-join account you specified becomes inaccessible, the system uses the auxiliary domain-join account for those operations in pods in Microsoft Azure that require joining the domain, such as importing image VMs, creating farm RDSH instances, creating VDI desktop instances, and so on.

**Note**
- Use an Active Directory account that adheres to the same guidelines for the primary domain-join account described in the prerequisites. Ensure that this auxiliary domain-join account has a different expiration time from the primary domain-join account, unless both accounts have **Never Expires** set. If both the primary and auxiliary domain-join accounts expire at the same time, the system's operations for sealing images and provisioning farm RDSH VMs and VDI desktop VMs will fail.
- You can add only one auxiliary domain-join account for each Active Directory you register with Horizon Cloud.
- If you do not add an auxiliary domain-join account at this time, you can add one later using the console.
- You can update or remove this account later.
- The agent-related software on a desktop-related virtual machine — such as a sealed image, farm RDSH instance, or VDI desktop instance — must be version 18.1 or later for the system to use the auxiliary domain-join account with that virtual machine.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auxiliary Join Username</strong></td>
<td>User account in the Active Directory that has permissions to join systems to that Active Directory domain.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> Only provide the account name in this field, such as ouraccountname, like the user logon name without the domain name. Entering slashes or at-signs will display an error.</td>
</tr>
<tr>
<td><strong>Auxiliary Join Password</strong></td>
<td>The password associated with the name in the <strong>Auxiliary Join Username</strong> text box.</td>
</tr>
</tbody>
</table>

7 Click **Save**.

At this point, if the domain-join step succeeds, the Add Administrator dialog box appears and you can continue to the next step.
8 In the Add Super Administrator dialog box, use the Active Directory search function to select the Active Directory administrator group you want performing management actions on your environment using the console.

This assignment ensures that at least one of your Active Directory domain's user accounts is granted the permissions to log in using Log In to the Horizon Cloud Administration Console to Perform Management Tasks on Your Horizon Cloud Environment now that the Active Directory domain is configured for this customer account.

**Important** To the Super Administrator role, add the Active Directory group which includes the domain-join account, as described in the prerequisites. If the domain-join account is not in any of the Active Directory groups that have the Super Administrator role, those system operations for pods in Microsoft Azure that involve joining virtual machines to the domain will fail.

9 Click Save.

**Results**

The following items are now in place:

- The Active Directory domain is one of the cloud-configured Active Directory domains associated with this Horizon Cloud customer account.

- For a pod in Microsoft Azure, Horizon Cloud has the necessary domain-join account needed for those system operations involving joining desktop-related virtual machines to that domain. Also, the domain-join account has the required Super Administrator role, so that those operations operate properly.

- After logging in to Horizon Cloud using your My VMware credentials, in the Active Directory login window, users in that Active Directory that have an assigned Horizon Cloud role can select the domain that corresponds to their Active Directory account.

- Users in the group to which you granted the Super Administrator role will be able to access the console and perform management activities when they use the associated My VMware account for the first login screen. To enable those administrators to use their own My VMware account credentials for the first login step, complete the steps described in Give Administrative Roles to Individuals in Your Organization for Logging In To and Performing Actions in Your Horizon Cloud Tenant Environment Using the Horizon Cloud Administration Console.

- User accounts from the registered Active Directory domain can be selected for assignments involving resources from pods in Microsoft Azure.

- The console's help desk features can be used with user accounts from that registered Active Directory domain.
What to do next

From this point, you typically perform the following tasks:

- Grant access to additional users in this domain to administer your environment. First add their My VMware accounts with associated Horizon Cloud roles, and then give their Active Directory accounts the appropriate Horizon Cloud role. See Give Administrative Roles to Individuals in Your Organization for Logging In To and Performing Actions in Your Horizon Cloud Tenant Environment Using the Horizon Cloud Administration Console and Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment.

- Assign the demo administrator role to those users in this domain to whom you want to grant read-only access to the console. See Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment.

Add Additional Auxiliary Bind Accounts for a Cloud-Configured Active Directory Domain in Horizon Cloud

When you register the first Active Directory domain with your Horizon Cloud environment, one auxiliary domain-bind account is required in the configuration. Having at least one auxiliary domain-bind account prevents the situation of locking out your administrator users from the administrative console if the primary bind account becomes inaccessible in the Active Directory domain. You can optionally configure additional auxiliary bind accounts for the cloud-configured Active Directory domains. Then if both the primary and first auxiliary bind accounts configured for a domain become inaccessible, the system uses the next auxiliary bind account to connect to that Active Directory domain.

Prerequisites

Verify that the Active Directory domain is one of your Horizon Cloud account's cloud-configured domains by navigating to Settings > Active Directory and seeing if the domain is listed on that page.

Verify that you have the user name and password information for the following accounts that are already configured in the console for the domain, because the user interface requires you confirm the existing passwords when performing this task:

- Password for the already configured bind account
- Password for the domain join account already configured in the user interface
Verify that you have the user name and password information for the bind account you are adding and that it adheres to the requirements described in Domain Bind Account Requirements. As described in that section, the primary and auxiliary domain bind accounts are always assigned the Super Administrator role, which grants all the permissions to perform management actions in the console. You should ensure that the domain bind account is not accessible to users that you do not want to have Super Administrator permissions.

**Caution** To prevent accidental lockouts over time, ensure that your domain-bind account meets the stated criteria, especially that the account password cannot expire, change, or be locked out. You must use this account configuration because the system uses this account as a service account to query Active Directory.

**Procedure**

1. In the console, click **Settings > Active Directory**.
2. Click the Active Directory domain for which you want to add the auxiliary bind account.
3. Click **Edit** next to the displayed domain bind settings.
4. In the Edit Active Directory dialog box, entering the password for the primary bind account. Entering the password here makes the **Domain Bind** button available to click to save the changes.
5. Expand the advanced properties and click **Add Auxiliary Bind Account**. A section for the auxiliary account information is added to the dialog box.
6. Type the account credentials. 
   **Note** In the field for the user name, only provide the user name itself, for example ourbindaccount2. Do not include the domain name here.
7. Click **Domain Bind**.
8. In any subsequent windows that appear, confirm the existing settings by clicking **Save** in each window.
   If the **Domain Join** window appears, type the password of the domain-join account before clicking **Save**.

**Results**

The auxiliary bind account is available for the system to use if the primary an auxiliary bind accounts become inaccessible.

You can add multiple auxiliary bind accounts by repeating the steps. To change an auxiliary bind account's password or to remove it, use the corresponding links displayed in the **Edit Active Directory** window's advanced properties area.
Best Practices about the Two Types of Roles You Give to People to Use the Horizon Cloud Administration Console to Work in Your Horizon Cloud Environment

This documentation topic describes the best practices for the two types of roles you must give to people when you want them to log in to the Horizon Cloud Administration Console and work in your Horizon Cloud environment. One type of role is used to enable or deactivate different parts of the Horizon Cloud Administration Console user interface itself. The other type of role is used to determine what actions can be invoked by people who have that assigned role. You must ensure the final combination of the two roles that you give to a specific individual reflects the outcome you want for that particular individual.

**Important** Because one type of role governs what the user can see in the console and the other type of role governs the invocation of actions, you must ensure that the overall combination of the two roles that a specific individual has reflects the outcomes you want for that particular individual. The best-practice combinations are described in the following sections. If you do not follow those best practices, contradictions might occur. For example, if the assigned roles do not match according to the guidance described here, an individual might log in to the console and not be able to perform the actions that you want them to perform — or the individual might log in and be able to perform actions that you do not want them to do. Therefore, it is important that you ensure that you align the individual's role in the **General Settings** page's **My VMware Accounts** area with the role assigned to that individual's Active Directory group in the **Roles & Permissions** page.

The following sections describe the two types of roles and the best-practice combinations to use based on the standard scenarios in typical organizations.

Roles that Enable or Deactivate Different Parts of the Console's User Interface for People in the Active Directory Group that Has that Assigned Role

These roles are predefined in the system, and relate to your Active Directory groups. When an individual logs in to a Horizon Cloud Tenant Environment, the console detects in which Active Directory group that individual's account is located. The console also identifies which of these roles is assigned to that Active Directory group on the console's Roles & Permissions page. Then, as the person navigates through the console's user-interface pages, tabs, and windows, those items display as enabled or deactivated according to the person's Active Directory group's assigned role.

**Important** This point that these roles can be assigned to only groups and not to individual Active Directory user accounts also means that you must avoid assigning two of these roles to the same Active Directory domain group. If you give two of these roles to the same Active Directory group and an individual from that group logs in, when the console identifies that both roles are assigned to that person's group, as they navigate through the user-interface pages, they might see deactivated items as one of the two roles prevents their access to those items.
You apply each of these roles at an Active Directory group-level. Because they are applied at a group level instead of an individual level, all individuals in the same Active Directory group will get the role that you assign to that group. You control which individuals are in your Active Directory groups in your Active Directory environment. Therefore, when you move individuals in your Active Directory environment from one Active Directory group to another, you must ensure that they are moved to a group that has one of the roles that continues to align with their other assigned role —the one that is assigned to their My VMware account. When you move an individual from one Active Directory group to another, you must verify whether the other type of role, the one that is assigned to that individual's My VMware account, might need to be adjusted to stay aligned with the role from this role type that is assigned to the individual's new Active Directory group.

An example of one of these roles is the Help Desk Read Only Administrator role. When an Active Directory group is assigned that role on the Roles & Permissions page, the console enables individuals in that group to navigate to the user cards for end users and view the information, but not perform operations on the desktops.

Roles that Determine Which Actions Can Be Invoked by People Who Have that Role Assigned to Their My VMware Account

Like the other role type, these roles are predefined in the system. These roles relate to the My VMware accounts that are configured in the General Settings page's My VMware Accounts area. When an individual about authentication to a Horizon Cloud Tenant Environment, the console detects which role is assigned to the My VMware account that was used to authenticate the logged-in session. Then, when the person tries to invoke an action in the console, the system either allows the API call to go through or prevents the API call, depending on this role that is assigned to the logged-in person's My VMware account in the General Settings page.

As a result, after the initial authentication to the console, this assigned role often works in tandem with the other type of assigned role:

1. The person navigates through the console's user-interface pages, tabs, and windows, and sees user-interface elements displayed as enabled or deactivated according to the person's Active Directory group's assigned role.
When that person clicks a button that would invoke an API call to perform an action, if the role assigned to their My VMware account does not allow that action to be performed, the API call will not go through and the action will not complete.

**Important** Given that in the console, this role works in tandem with the role assigned to a person’s Active Directory group — the latter determining which console elements are active and the former determining which actions are allowed to complete when an element is clicked — you must ensure that the overall combination of the two roles that a specific individual has reflects the outcomes you want for that particular individual. Otherwise, contradictory results can occur. When you move an individual from one Active Directory group to another, confirm that the role on their My VMware account is aligned with the role on their new Active Directory group and adjust it as needed. The standard best-practice combinations are described in the following sections.

### The Four Standard Best-Practice Role Combinations

Because contradictory behavior can occur when a person’s two role are not aligned according to the table below, it is recommended that you align the roles granted to your organization’s individuals according to the following table. The system does not prevent you from assigning a role to an Active Directory group that is more permissive than the role assigned to the My VMware accounts of the individuals in that group. If an individual belongs to multiple Active Directory groups, ensure that the roles assigned to those groups on the Roles & Permissions page are also aligned with each other and with the role on the individual’s My VMware account.

<table>
<thead>
<tr>
<th>Role on the Person’s My VMware Account in the General Settings page</th>
<th>Role on the Person’s Active Directory Group in the Roles and Permissions page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Administrator</td>
<td>Super Administrator</td>
<td>Full access to view all areas of the console and perform all actions in the console.</td>
</tr>
<tr>
<td>Customer Administrator Readonly</td>
<td>Demo Administrator</td>
<td>Ability to view all areas of the console, view settings and select options to see additional choices, and without the ability to invoke actions that change the environment, such as deleting items. An example of using this combination is to allow people in your organization to log in and demonstrate the capabilities of the system to others, while avoiding changes being made to the system.</td>
</tr>
<tr>
<td>Customer Helpdesk</td>
<td>Help Desk Administrator</td>
<td>Access to view the help-desk-related areas of the console and perform all help-desk-related actions that the console provides. The purpose of this combination is for people to work with the user card features to see the status of end user sessions and perform troubleshooting operations on the sessions.</td>
</tr>
<tr>
<td>Customer Helpdesk Readonly</td>
<td>Help Desk Read Only Administrator</td>
<td>Access to view the help-desk-related areas of the console and see the status of end user sessions in the user card, while preventing the ability to invoke the help-desk-related actions.</td>
</tr>
</tbody>
</table>
When You Want to Restrict a Person to have Read-Only, Viewing Access to the Console for All of the Console’s Areas

If you want an individual to be able to browse all of the console’s user-interface pages and open dialogs and view reports, and also restrict them from invoking actions that change things in your tenant environment, you must ensure that both of the following conditions are met:

- In the General Settings page’s **My VMware Accounts** area, assign the **Customer Administrator Read-Only** role to their My VMware account. If that individual’s account lists a different role there, you can remove their row from the **My VMware Accounts** section and add it back, this time specifying **Customer Administrator Read-Only** role.

- In the Roles & Permissions page, assign the **Demo Administrator** role to that individual’s Active Directory group.

When both of those conditions are met, the individual will be able to log in to the console, navigate to all of the console’s pages, browse the pages, open dialogs and view reports, and also be restricted from invoking actions that change things in the environment.

**Note** Because the Roles & Permissions page works at the Active Directory group level, and not at an individual account level, you must ensure the Active Directory group has the appropriate individual accounts in it, according to your organizational requirements.

When You Want to Restrict a Person to have Access to the Help Desk Features of the Console and Also Have the Ability to Perform Actions in the User Card

If you want an individual to be able to log into the console and be restricted to access only the help-desk-related features, and not all of the areas of the console, while also allowing them to perform the help-desk-related actions, you must ensure that both of the following conditions are met:

- In the General Settings page’s **My VMware Accounts** area, assign the **Customer Helpdesk** role to their My VMware account. If that individual’s account lists a different role there, you can remove their row from the **My VMware Accounts** section and add it back, this time specifying **Customer Helpdesk** role.

- In the Roles & Permissions page, assign the **Help Desk Administrator** role to that individual’s Active Directory group.

When both of those conditions are met, the individual will be able to log in to the console, see help-desk-related features, and perform the help-desk-related actions.

**Note** Because the Roles & Permissions page works at the Active Directory group level, and not at an individual account level, you must ensure the Active Directory group has the appropriate individual accounts in it, according to your organizational requirements.
When You Want to Restrict a Person to have Read-Only Access for the Help Desk Features of the Console

If you want an individual to be able to log into the console and be restricted to access only the help-desk-related features on a read-only basis and restricted from performing any help-desk-related actions, you must ensure that both of the following conditions are met:

- In the General Settings page’s **My VMware Accounts** area, assign the **Customer Helpdesk Read-Only** role to their My VMware account. If that individual's account lists a different role there, you can remove their row from the **My VMware Accounts** section and add it back, this time specifying **Customer Helpdesk Read-Only** role.

- In the Roles & Permissions page, assign the **Help Desk Read Only Administrator** role to that individual's Active Directory group.

When both of those conditions are met, the individual will be able to log in to the console and use the help-desk-related features on a read-only basis.

**Note**  Because the Roles & Permissions page works at the Active Directory group level, and not at an individual account level, you must ensure the Active Directory group has the appropriate individual accounts in it, according to your organizational requirements.

When You Want a Person to Have Full Access to the Console, for All of the Console's Areas and Actions

If you want an individual to have full access to the console to view all of its areas and invoke actions that change things in your tenant environment, ensure that both of the following conditions are met:

- In the General Settings page’s **My VMware Accounts** area, assign the **Customer Administrator** role to their My VMware account. If that individual's account lists a different role there, you can remove their row from the **My VMware Accounts** section and add it back, this time specifying **Customer Administrator** role.

- In the Roles & Permissions page, assign the **Super Administrator** role to that individual's Active Directory group.

When both of those conditions are met, the individual will be able to log in to the console, navigate to all of the console's pages and invoke actions that change things in the environment.

**Note**  Because the Roles & Permissions page works at the Active Directory group level, and not at an individual account level, you must ensure the Active Directory group has the appropriate individual accounts in it, according to your organizational requirements.
Give Administrative Roles to Individuals in Your Organization for Logging In To and Performing Actions in Your Horizon Cloud Tenant Environment Using the Horizon Cloud Administration Console

In the process of authenticating to the cloud-based administrative console, the first login screen requires an existing My VMware account that is associated with your Horizon Cloud environment. To grant other users in your company or organization the ability to log in to that first login screen, you associate the individual users' My VMware accounts with your environment. You also associate each My VMware account with an appropriate role. The role that you assign to an individual's account should align with the types of actions that you want to permit that individual to perform in your environment using the console.

**Important** Because this role described here governs what the actions can be performed in the authenticated session while the other, Active Directory domain-related, role governs which areas of the console are visible in the session, you must ensure that the overall combination of the two roles continues to reflect the outcomes you want for a particular individual, even as the individual moves to different job positions and Active Directory groups within your organization. For details of the two types of roles and the best-practice pairings of the role assignments, see **Best Practices about the Two Types of Roles You Give to People to Use the Horizon Cloud Administration Console to Work in Your Horizon Cloud Environment**.

The role that you assign using the steps here is one of the two types of roles that the console uses to determine both what a person's authenticated session allows that person to view in the console and what actions they can perform on what they can see in the console. The role assigned to the My VMware account determines the following items:

- Whether an individual has the ability to authenticate to the console using the My VMware login screen.
- Whether the person can view all of the console's areas or a subset of the areas, such as the Help Desk Features in Your Horizon Cloud Environment.
- The specific actions the person is able to invoke in the console, within the areas they can view.

In addition to the role associated with an My VMware account, when Register Additional Active Directory Domains as Cloud-Configured Active Directory Domains with Your Horizon Cloud Tenant Environment, the role that is assigned to a person's Active Directory group grants their user account with access that works in tandem with the role associated with their My VMware account. The role assigned to the Active Directory group to which the user account belongs controls which of the console's elements are accessible to that person after they log in using their Active Directory account credentials at the console's second login screen. For a list of those roles, see **Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment**.
In the console, you associate My VMware accounts with your environment using either the My VMware Accounts area in the General Setup Section of the Horizon Cloud Administration Console’s Getting Started Wizard or the Customizable General Settings for Your Horizon Cloud Tenant Environment.

**Important** Even though you can perform these steps before the My VMware accounts are created at vmware.com, the accounts must be created at vmware.com before they can be used to log in to the console. My VMware accounts are created using the registration process at https://my.vmware.com/web/vmware/registration.

**Procedure**

1. In the console, use one of these methods to associate My VMware accounts with your environment.
   - From the Getting Started wizard, click General Setup > My VMware Accounts > Add.
   - Click Settings > General Settings > Edit and scroll to the My VMware Accounts area.

   The list of My VMware Accounts already associated with your environment is displayed.

2. Add a row to the list by clicking the plus icon (➕) that is visible by the list's bottom entry.

   A new row appears with fields for entering a first name, last name, the My VMware account ID, and selecting a Horizon Cloud role.

3. Make a row for each My VMware account you want to associate with your environment and enter the requested information in each row, including selecting a Horizon Cloud role.

   The role defaults to Customer Administrator unless you select a different one. If you want to prevent the person from invoking actions in the console that result in anything more than viewing information, assign one of the read-only roles.

<table>
<thead>
<tr>
<th>Role on the Person’s My VMware Account</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Administrator</td>
<td>All actions in the console can be performed, including onboarding a pod or deleting items.</td>
</tr>
<tr>
<td>Customer Administrator Readonly</td>
<td>Prevents the invocation of actions that would change the environment, such as onboarding a pod or changing a general setting.</td>
</tr>
<tr>
<td>Customer Helpdesk</td>
<td>Within the console's help-desk-related areas, all of the help-desk-related actions can be performed.</td>
</tr>
<tr>
<td>Customer Helpdesk Readonly</td>
<td>Within the console's help-desk-related areas of the console, can only view information. Prevents the invocation of actions that would change things within those console areas.</td>
</tr>
</tbody>
</table>

4. Click **Save** to save the information to the system.
Results

If all of the added My VMware account IDs exist at vmware.com, they can be used to authenticate in the first Horizon Cloud login screen.

**Important** The steps you just completed do not create the actual My VMware accounts. My VMware accounts are created using the registration process at https://my.vmware.com/web/vmware/registration.

What to do next

If the added users' Active Directory accounts are in Active Directory groups which do not yet have an associated Horizon Cloud role, complete the steps described in Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment. Follow the best-practice pairings described in Best Practices about the Two Types of Roles You Give to People to Use the Horizon Cloud Administration Console to Work in Your Horizon Cloud Environment.

**Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment**

In the process of authenticating to the cloud-based administrative console, after authenticating to the initial login screen using a My VMware account, the individual from your organization enters their Active Directory user account credentials in the second login screen, according to the Active Directory domain you have registered with the environment. The system provides predefined roles that you can assign to your various Active Directory groups. These Active Directory domain-related roles control which areas of the console are viewable and enabled or viewable and deactivated, as the logged-in person navigates through the console. You must assign a role to your organization’s appropriate Active Directory groups so that the users in that group can use the console to do the work activities you want them to do.

The role that you assign using the steps here is one of the two types of roles that the console uses to determine both what a person's authenticated session allows that person to view in the console and what actions they can perform on what they can see in the console. In the Log In to the Horizon Cloud Administration Console to Perform Management Tasks on Your Horizon Cloud Environment, the console's first login screen uses My VMware accounts, which are associated with roles using the General Settings page. The second login screen uses Active Directory credentials, which are associated with roles using this Roles & Permissions page. These Active Directory domain-related roles determine the visibility of the console's features and elements. This role also determines which user-interface elements might appear deactivated as the person navigates through the console. For example, a person in an Active Directory group that is
assigned the **Help Desk Read Only Administrator** role can navigate to the user cards for end users and view the information, but not perform operations on the desktops. A person in an Active Directory group that is assigned the **Help Desk Administrator** role can navigate to the user cards and perform troubleshooting operations as well as view the information.

These Active Directory domain-related roles work tandem with the roles on the My VMware accounts that people in your organization use to log in using the standard login workflow. Therefore, you must ensure that the overall combination of the two roles continues to reflect the outcomes you want for a particular individual, even as the individual moves to different job
positions and Active Directory groups within your organization. For details of the two types of roles and the best-practice pairings of the role assignments, see Best Practices about the Two Types of Roles You Give to People to Use the Horizon Cloud Administration Console to Work in Your Horizon Cloud Environment.

**Note**  Role changes that you make using the Horizon Cloud Service platform — through VMware Cloud services at cloud.vmware.com — do not appear in the Horizon Cloud Administration Console. You must make role changes directly in the Horizon Cloud Administration Console as described below.

**Caution**  Keep in mind that the Super Administrator role governs which of your AD user accounts can log in to your Horizon Cloud tenant account and perform administrative operations in the console, including the steps here to assign roles to your AD groups. If you have only a sole, single AD group assigned to the Super Administrator role, do not remove that administrator group from your Active Directory system or change its GUID as it appears in your Active Directory system until you have added another administrator group to this Super Administrator role. If you remove the group from your Active Directory system or change it such that its GUID in your Active Directory system changes, that change will not be communicated to the Horizon Cloud control plane, and Horizon Cloud's knowledge of that AD group having the Super Administrator role will be broken. If that group is the sole group you have assigned to the Super Administrator role, it might possibly result in none of your AD accounts that used to be able to log in with Super Administrator access level will be able to log in and perform administrative operations, including the operation to assign the role to an AD group to re-establish a set of AD accounts with Super Administrator access. The domain-bind account is always assigned the Super Administrator role. If you have removed your sole, single AD group assigned to the Super Administrator role, and the domain-bind account was not in that group, you can try logging in to the console using the domain-bind account credentials and performing the steps to assign the Super Administrator role to a new AD group. However, if you cannot successfully log in using the domain-bind account, you'll have to contact VMware Support to assist you in recovering administrative access to your tenant account.
Important These Horizon Cloud roles can be assigned to groups only. The system does not provide a way for you to choose individual Active Directory user accounts for each role.

- It is critical to understand this point when it comes to the domain-join account when your cloud-connected pods are in Microsoft Azure. If the domain-join account that you registered for your initial pod in Microsoft Azure is not already in one of your Active Directory groups, create an Active Directory group for that account so that you can ensure the Super Administrator role can be assigned to that domain-join account. That domain-join account must be given the Super Administrator role so that those system operations that involve joining virtual machines to the domain will work properly for pods in Microsoft Azure. For more details, see Service Accounts That Horizon Cloud Requires for Its Operations.

- This point that the roles can be assigned only to groups and not individual accounts also means you must avoid assigning two roles to the same Active Directory domain group. The Super Administrator role is intended to grant all the permissions to perform all management actions in the console and the Demo Administrator role is a read-only role. If you give both of those roles to the same Active Directory group, all of the users in that group will not receive the permissions of the Super Administrator role. Their actions are restricted in the console, which might prevent availability of full management of your environment.

The following predefined roles are provided by default. The predefined roles cannot be modified.

Table 2-1. Horizon Cloud Role-Based Access Control Groups

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Administrator</td>
<td>A mandatory role that you must assign to at least one group in your Active Directory domain and optionally to others. This role grants all the permissions to access all areas of the console and perform management actions in the console.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>Ensure that the domain-join account that you specified when registering the Active Directory domain with the first pod is in one of the groups given the Super Administrator role. For the end-to-end success of operations involving images and domain join operations, that domain-join account must be granted this Super Administrator role.</td>
</tr>
<tr>
<td></td>
<td>The primary and auxiliary domain bind accounts are always assigned the Super Administrator role, which grants all the permissions to perform management actions in the console. You should ensure that your specified domain bind accounts are not accessible to users that you do not want to have Super Administrator permissions.</td>
</tr>
<tr>
<td>Help Desk Administrator</td>
<td>A role that you can optionally assign to one or more groups. The purpose of this role is to provide access to the console so that your Active Directory groups with this role can work with the user card features to:</td>
</tr>
<tr>
<td></td>
<td>- See the status of end user sessions.</td>
</tr>
<tr>
<td></td>
<td>- Perform troubleshooting operations on the sessions.</td>
</tr>
</tbody>
</table>
### Table 2-1. Horizon Cloud Role-Based Access Control Groups (continued)

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk Read Only Administrator</td>
<td>A role that you can optionally assign to one or more groups. When paired with the <a href="https://www.vmware.com/support/pubs/">Give Administrative Roles to Individuals in Your Organization for Logging In To and Performing Actions in Your Horizon Cloud Tenant Environment Using the Horizon Cloud Administration Console</a>, the users in this group can view the settings and select options to see additional choices in the console, but the selections do not change the configuration settings.</td>
</tr>
</tbody>
</table>

### Prerequisites

**Caution** Prior to assigning roles to your existing Active Directory groups, review the user account membership in the Active Directory groups to ensure a user account receives only one of these Horizon Cloud roles. Create specific Active Directory groups if needed. Because these roles are assigned at the level of the Active Directory group, some unexpected results can occur if a user’s Active Directory account belongs to two Active Directory groups and each group is assigned a different role. The console's features are visible according to this precedence order:

1. **Super Administrator**
2. **Help Desk Administrator**
3. **Demo Administrator**
4. **Help Desk Read Only Administrator**

As a result of this precedence order, if a user’s Active Directory account belongs to both Active Directory groups ADGroup1 and ADGroup2, and you assign the **Super Administrator** role to ADGroup1 and assign the **Help Desk Read Only Administrator** role to ADGroup2, the console will display all of the features according to the **Super Administrator** role, instead of the subset of features for the other role, because the **Super Administrator** role takes precedence.

Also, review the roles assigned to the group’s members’ My VMware accounts to ensure those roles are aligned with the role you are assigning to their Active Directory group. Follow the best-practice pairings described in [Best Practices about the Two Types of Roles You Give to People to Use the Horizon Cloud Administration Console to Work in Your Horizon Cloud Environment](https://www.vmware.com/support/pubs/).

### Procedure

1. In the console, navigate to **Settings > Roles & Permissions**.
2. Select one of the predefined roles and click **Edit**.
3. Use the search box to search for and select an Active Directory group.
   - You must type at least three characters into the search box to have results appear.
   - The group is added to the set of selected groups.
4. Click **Save**.
What to do next

Ensure the users in the domain group have the appropriate roles on their My VMware accounts. See Best Practices about the Two Types of Roles You Give to People to Use the Horizon Cloud Administration Console to Work in Your Horizon Cloud Environment and Give Administrative Roles to Individuals in Your Organization for Logging In To and Performing Actions in Your Horizon Cloud Tenant Environment Using the Horizon Cloud Administration Console.

Enabling or Deactivating the Cloud Monitoring Service (CMS) for Your Horizon Cloud Tenant Environment

Before you can obtain the data that gives you the ability to monitor capacity, usage, and health within and across your tenant’s fleet of cloud-connected pods, the Cloud Monitoring Service (CMS) must be enabled. CMS is one of Horizon Cloud’s central services. The CMS is enabled at a tenant level, and its setting applies for all of the pods that are connected to that Horizon Cloud tenant. The activation of CMS is one of the key things that provides all of the visual pod-related, session-related, and user-related data that gets presented in the administrative console’s Dashboard page’s charts and graphs, the Reports page’s reports, and in the user cards for the help desk features.

The Cloud Monitoring Service (CMS) collects and stores session, application, and desktop data from cloud-connected pods for monitoring and reporting purposes. The data is presented in various console pages, as described in Chapter 3 Introducing the Cloud Monitoring Service’s Unified Visibility, Health Monitoring, and Help Desk Features Provided in Horizon Cloud.

Tip  The CMS is typically turned on by default at your first use of your Horizon Cloud tenant. If you are not seeing visual data displayed on those console pages, first follow these steps below to confirm that the CMS is turned on in the General Settings page.

When the Cloud Monitoring Service is enabled for your tenant, you can also optionally choose to opt in or opt out of tracking user information related to your end users' sessions. Typical information that CMS collects about user sessions includes the times they logged in, session durations, and average session length per user.

- When you opt in to the collection of user data, Horizon Cloud collects this information and maintains it for the duration of your use of Horizon Cloud. If you decide later that you do not want to collect user data, you can stop the collection and also delete any collected data by disabling the Session Data toggle.

- When you opt out of the collection of user data but leave the CMS enabled, Horizon Cloud collects session data for a limited period and hashes the user name to allow real-time administration while disabling historical and aggregated viewing of information. As a result, some reports, such as the User Usage report, are not available. In this case, the system also continues to collect other data related to applications and desktops in connected pods.
Disabling these toggles also deletes any data that was previously collected. Disabling the **Session Data** toggle by itself deletes the previously collected user-related data, and leaves the other types of collected data, such as the pod-level and session-related data. Disabling the **Cloud Monitoring Service** toggle deletes all collected data for the tenant.

**Caution** If you have cloud-connected Horizon pods that are sending desktop data to vRealize Operations Manager, enabling CMS causes data to be sent to the Cloud Monitoring Service instead. To continue using vRealize Operations Manager to collect that desktop session data, deactivate CMS.

**Prerequisites**

Before you can activate the Cloud Monitoring Service for any of your cloud-connected Horizon pods or pods in Microsoft Azure, you must have completed the pod onboarding steps for at least one pod. The onboarding steps are specific to the type of pod. See the workflow links in **Pod Types You Can Connect to Horizon Cloud**.

**Procedure**

1. Navigate to the console’s General Settings page by clicking **Settings > General Settings**.
2. Scroll down the page to locate the Monitoring section.

   ![Monitoring Settings](image)

   - **Cloud Monitoring Service**: Yes
   - **Allow Data Collection**: Yes
   - **Session Data**: Yes

3. Click the pencil icon to change the Cloud Monitoring Service settings.
   - Use the **Cloud Monitoring Service** toggle to activate or deactivate all of the data collection for your tenant environment. When deactivated, the CMS does not collect any data from your entire fleet of cloud-connected pods in that tenant environment.
   - Use the **Session Data** toggle to opt in or opt out of tracking user information related to your end users’ sessions.
4. Click **Save** to save your changes.

**Sharing Your Feedback with VMware**

VMware In-Product Feedback is a feature you use to share your feedback directly with the VMware team to help us improve the product you are using.
There are two ways to share feedback with us:

- At any time, you can click the Feedback icon at the top of the console to open the Share Your Feedback window. You can either enter information in the window and click Submit or click the email link in the lower portion of the window to send us an email.

- A Share Your Feedback window might appear after you log in to the console. You can either enter information in the window and click Submit or click the email link in the lower portion of the window to send us an email.

Here is an example of the Share Your Feedback window:

![Share Your Feedback Window](image)

Join or Leave the Customer Experience Improvement Program

The VMware Customer Experience Improvement Program (CEIP) provides information that VMware uses to improve its products and services, to fix problems, and to advise you on how best to deploy and use VMware products.

This product participates in the VMware CEIP. Information about the data collected through CEIP and how VMware uses it are in the Trust & Assurance Center at [http://www.vmware.com/trustvmware/ceip.html](http://www.vmware.com/trustvmware/ceip.html).
The CEIP appears the first time you log in to the Horizon Cloud Administration Console after registering an Active Directory domain with your environment’s Horizon Cloud customer account. You must then make a selection about the CEIP. You can change your selection to join or leave the CEIP at any time after that initial selection.

Procedure

1. In the console, click > CEIP.
2. Move the slider next to Join Customer Experience Improvement Program to No to leave CEIP or Yes to join.
   - The default is Yes.
3. Click Save.

Remove the Active Directory Domain Registration

In some situations, you might need or want to remove the Active Directory domain association from your Horizon Cloud customer account. The administrative console labels this action Delete and you might hear people refer to it as resetting the Active Directory domain that’s bound to the tenant environment. Immediately, or shortly after, your first pod is paired with your Horizon Cloud customer account, you register an Active Directory domain. When that registration process is complete, that domain is a cloud-configured domain for your overall Horizon Cloud customer account. All of the pods that you deploy from Horizon Cloud or connect to Horizon Cloud using the same customer account are also associated with that first cloud-configured Active Directory domain through the customer account record. All pods that share the same customer account record must have line-of-sight to the cloud-configured domains in that record.

Examples of situations where you might want to delete (also known as reset) the domain that is bound to the tenant are:

- You deployed your initial pod in Microsoft Azure and started the domain-bind step. Then something went wrong and left the domain registration in an incomplete state. In this situation, some of the Active Directory domain information gets written to your customer account record in the cloud. However, because the information is incomplete, you find you cannot proceed to finish the domain registration using the console.

- You ran a proof-of-concept by deploying a pod in Microsoft Azure, registering a test Active Directory domain, and ran many of the workflows. Then you deleted that pod to start fresh and create your production pod with your production domain. However, because the initial test Active Directory domain is still a cloud-configured domain in your customer account, the system expects to associate that test Active Directory domain with your new pods.

- You ran the Horizon Cloud Connector’s onboarding workflow for multiple Horizon pods using this Horizon Cloud customer record, before logging in to the administrative console to complete the Active Directory domain registration process. The Horizon Cloud Connector’s onboarding workflow creates a partial configuration in Horizon Cloud of the Active Directory domains known to the Horizon pods’ Connection Servers. That partial configuration is
completed when you perform the initial Active Directory domain registration workflow in the console. Due to a known issue in this release, connecting multiple Horizon pods to Horizon Cloud prior to completing the domain registration workflow in the console can cause the registration workflow to fail. In this situation, you must undo the cloud pairing for all but one of those pods using the Unplug action in the connector's configuration portal and remove the partial Active Directory domain registration before attempting to register the domain.

The administrative console displays the buttons for removing the Active Directory domain information when the following conditions are true.

- The Getting Started page shows that only one pod is deployed, or paired, in your environment or you have deleted all of your initial pods and no pods are visible on the Capacity page.

**Important** If you have deleted all of your initial pods and you had a True SSO configuration, the button for removing the Active Directory domain information is not enabled. Before you delete your last pod, ensure that you remove any True SSO configurations from the Active Directory page in the console so that the system will enable the Delete button for the Active Directory configuration.

- If you have a pod in Microsoft Azure, that pod does not have any of the following items, such as:
  - Imported VMs listed on the Imported VMs page
  - Sealed images listed on the Images page
  - Farms listed on the Farms page
  - VDI desktop assignments, listed on the Assignments page
  - Any True SSO configuration shown on the Active Directory page
  - Any identity management configuration shown on the Identity Management page
  - More than one Active Directory domain shown on the Active Directory page

**Procedure**

- Perform one of the following steps in the console.
  - If you are resetting the domain because the domain-bind step or domain-join step of your first Active Directory domain registration workflow was not successfully completed, expand the General Setup section in the Getting Started page. In the Active Directory row, click Delete.
  - Otherwise, if the Settings menu is visible, you can navigate to the Active Directory page using Settings > Active Directory. Then click Delete.

**Results**

The system logs you out and presents its initial login screen.
What to do next

Log back in as described in Log In to the Horizon Cloud Administration Console to Perform Management Tasks on Your Horizon Cloud Environment.
Introducing the Cloud Monitoring Service's Unified Visibility, Health Monitoring, and Help Desk Features Provided in Horizon Cloud

The Cloud Monitoring Service (CMS) is one of the central services provided in Horizon Cloud. The CMS gives you the ability to monitor capacity, usage, and health within and across your fleet of cloud-connected pods, regardless of the deployment environments in which those individual pods reside. Wherever your cloud-connected pods and the agent-running VMs live — whether in your private data centers or in industry cloud capacities — the Cloud Monitoring Service obtains the capacity, health, and usage-related data from those pods and agent-running VMs. The CMS presents that data to you within the Horizon Cloud Administration Console. That console is your single pane of glass for working with your tenant's fleet of cloud-connected pods. The CMS feeds data into the various Dashboard page's tabs to help you see overall health and drill-down into the health, capacity, and usage metrics at various levels. The CMS also provides the data for many of the reporting views within the console's Reports page, as well as within the user cards, in which you perform help desk operations to support your individual end users.

Note The CMS requires the instances for the Horizon Connection Server and the Horizon Cloud Connector to reside in a VMware SDDC-based environment. A VMware SDDC-based environment is an environment such as vSphere, VMware Cloud on AWS, or Azure VMware Solution. As described in the Horizon 7 version 7.13 Release Notes, you can now run a Horizon pod's virtual desktops that run on Hyper-V hypervisor. As long as your Horizon pod meets the requirement of having the Horizon Connection Server and Horizon Cloud Connector instances in a VMware SDDC-based environment, the standard CMS features that relate to data reported from the virtual desktops are supported for such virtual desktops that reside on all supported third-party hypervisors. For information about the currently supported third-party hypervisors for this use case, see the Horizon documentation at Horizon 7 Documentation and Horizon Documentation.

Before you can use the console for all of the visibility, health monitoring, and help desk features that the CMS provides, you must have in your tenant environment a minimum of the following:

1. One cloud-connected pod.
A completed Active Directory domain registration for at least one Active Directory domain to which that pod has line of sight.

The Super Administrators role assigned to at least one group in that Active Directory domain.

The Cloud Monitoring Service (CMS) enabled for your tenant environment. The console's General Settings page provides the switches for enabling or disabling the CMS for your Horizon Cloud tenant environment. The same switch controls the use of CMS for all of the cloud-connected pods in the same tenant environment. See Customizable General Settings for Your Horizon Cloud Tenant Environment.

If your Horizon pod is cloud-connected using Horizon Cloud Connector 1.8 or later, the CMS is enabled for that pod if you deployed Horizon Cloud Connector with the Full Feature profile or if you deployed with the Basic Feature profile and then manually activated the Connection Server Monitoring Service. For more information, see Manually Activate Horizon Cloud Services for Horizon Cloud Connector 1.8 or Later.

The types of pods that you can connect to Horizon Cloud are described in Chapter 1 Introduction to Horizon Cloud and Onboarding Pods to Become Cloud-Connected Pods. For the high-level steps needed to get useful cloud-connected pods that can leverage the Cloud Monitoring Service, see the suggested workflow for the pod type you want:

- High-Level Workflow When You are Onboarding an Existing Manually Deployed Horizon Pod as Your First Pod to Your Horizon Cloud Tenant Environment
- High-Level Workflow for When Your Very First Horizon Cloud Cloud-Connected Pod is from Using the Pod Deployer to Deploy a Pod into Microsoft Azure

Use the following topics and their subtopics to learn about the unified visibility, health monitoring, and help desk features that the Cloud Monitoring Service provides.

This chapter includes the following topics:

- Cloud Monitoring Service (CMS) and Horizon Agents Installer (HAI) Options For Your Horizon Cloud Environment
- Health Visibility and Insights into Your Cloud-Connected Pods Provided by the Cloud Monitoring Service in Horizon Cloud
- Help Desk Features in Your Horizon Cloud Environment

Cloud Monitoring Service (CMS) and Horizon Agents Installer (HAI) Options For Your Horizon Cloud Environment

Availability of user card and reports information depends on whether you have Cloud Monitoring Service (CMS) enabled in your Horizon Cloud tenant and which options you selected when installing software using the Horizon Agents Installer (HAI).
To display historical session data, you should enable CMS and install the vRealize Operations Desktop Agent in HAI. To show live session data, you should also install the Help Desk Plugin in HAI.

**Note** The RDP protocol provides for a limited set of metrics when compared with the other protocols supported in Horizon Cloud. The vRealize Operations Desktop Agent will return data for those metrics that the RDP protocol provides.

- **Historical session data** refers to:
  - Session information for logged off sessions over the previous seven days.
  - Performance trend data (CPU, memory, latency, disk trend) for active, idle, and disconnected sessions over the previous 15 minutes.

- When live session data does not appear, you still see VM relative information and log in time breakdowns, but do not see:
  - Client information.
  - User experience information.
  - Real-time performance trends.
  - Process/Application information.

**Note** If you have cloud-connected Horizon pods that are sending desktop data to vRealize Operations Manager, enabling CMS causes data to be sent to the Cloud Monitoring Service instead. To continue using vRealize Operations Manager to collect that desktop session data, deactivate CMS.

### Health Visibility and Insights into Your Cloud-Connected Pods Provided by the Cloud Monitoring Service in Horizon Cloud

The Horizon Cloud Administration Console provides the Dashboard page as your one-stop place from which you can get a visual sense of the overall health of your entire fleet of cloud-connected pods, as well as access real-time metrics and health information for all of the pods in your Horizon Cloud tenant environment. The data is provided by the Cloud Monitoring Service (CMS), which is one of the central services in Horizon Cloud. The Dashboard page is available from the console's **Monitor** icon.

#### The Horizon Cloud Administration Console's Dashboard Page - Overview Tab for a Horizon Cloud Tenant

Use the Dashboard page's Overview tab to get a snapshot health view for what is happening in your entire fleet of cloud-connected pods, and then optionally drill-down to see more details. The Cloud Monitoring Service (CMS), one of Horizon Cloud's central services, provides the data that
you see on the Overview tab. The CMS obtains this data from all of the cloud-connected pods in your Horizon Cloud tenant environment and presents the data for your use.

**Note** The charts of session data depict historical data and trends only when the Cloud Monitoring Service feature is enabled for your Horizon Cloud environment. That feature collects and stores session, application, and desktop data from cloud-connected pods for monitoring and reporting purposes. When the Cloud Monitoring Service feature is deactivated for your environment, historical data is not collected and therefore not available to display. In that case, the charts of session data you see are based on data from current sessions only. The Cloud Monitoring Service feature is active by default. If the feature is not activated in your environment and you want to use the service to collect session data over time, you can activate the feature on the General Settings page. See Customizable General Settings for Your Horizon Cloud Tenant Environment.

The following screenshot illustrates the Overview tab with four cloud-connected pods. The screenshot depicts two pods using Microsoft Azure capacity, one on-premises Horizon pod, and one Horizon pod using VMware Cloud on AWS capacity. The on-premises Horizon pod is located in Paris, and is reporting two issues.

The system refreshes the information every few minutes. You can also refresh the page manually.

**Important** For pods deployed into Microsoft Azure, these reports do not reflect user-related data until an hour has passed from the time you deployed the pod or from the time you enabled monitoring user session information.
Global Footprint

The upper portion of the Dashboard page contains the interactive Global Footprint map, which has two view options: Issues and Session. This map visually depicts your pods’ geographic city locations and shows additional information when you hover on a location. The map supports the typical industry-standard map interactivity features, such as panning and zooming in or out to view the map at different scales. Zooming in for more detail is especially useful to see those pods which are clustered together at the same location. When you first display the map, the zoom defaults to a scale that will show all your connected pods in a single view.

When your environment has pods of different types, you can use the filter function at the bottom right of the map area to selectively show or hide pods of specific types.

**Important**  The system uses the location information that is associated with the pod from one of the following ways:

- In the process of deploying and connecting the pod to Horizon Cloud, you specified a city name.
- For all pods, according to the city name specified for the pod’s associated location in its pod details. To associate a location with an already onboarded pod, see [Change a Cloud-Connected Pod’s Associated Location, Name, and Description in Your Horizon Cloud Tenant Environment](#).

The system uses its city lookup table to get the latitude and longitude coordinates associated with the specified city, and places the pod at those coordinates on the map.

Click on Issue or Session to the right of the map to select a view of the Global Footprint. Based on the view selected, the pod icons in the Global Footprint map depict health-related or session-related data. Hovering over the pod icons will show data relevant to the pods’ issues or sessions, depending on the view. The two views are described below.
When the Issue view is selected (as it is by default), the map has the title Global Footprint - Health. Each main visual icon represents the set of pods at that geographic city location along with the total number of pods there. Hovering over an icon displays a list of the pods at that location, along with an icon indicating the type of pod and a green dot indicating a healthy deployment or a red dot indicating an unhealthy deployment of that pod. Clicking on the VIEW link in that pod list opens the Global Footprint - Health page showing detailed information for issues reported for the pods at that location.

The area to the right of the map shows the total number of current issues at the top and lists the top five issues below. Hovering on an issue in this area opens the pod information pop-up on the map for the location where the issue is occurring. For Horizon pods, the pod name is a link that you can click to launch Horizon Console for that pod's Horizon Connection Server, as described in Launch Horizon Console as a Cloud Service. Clicking on the VIEW link at the bottom of the issue list opens the Global Footprint - Health page showing detailed information for issues.

On the Global Footprint - Health page, the list of issues displayed can be filtered by location and pod. There are also sort and filter functions for each column of information. The issue list window has multiple tabs:

- The Total Issues tab lists all of the issues and details about each one, such as which pod has the issue, the pod type, and so on. For Horizon pods, the pod name is a link that you can click to launch Horizon Console for that pod's Horizon Connection Server, as described in Launch Horizon Console as a Cloud Service.
- The Delivery tab lists issues related to components of the pod itself, such as the Connection Server.
- The Infrastructure tab lists issues related to non-pod components that are used with, connect to, or which underlie the pod, such as your Active Directory domain, NTP service, the Microsoft Azure service, and so on.
- The User Experience tab lists issues related to user experiences.

When the Session view is selected, the map has the title Global Footprint - Sessions. Each main visual icon represents the set of pods at that geographic city location along with the total number of sessions in those pods. This total includes connected, active, and idle sessions. Hovering over an icon displays a list of the pods with an icon indicating the type of pod and displays session data. If the Cloud Monitoring Service feature is enabled, the pop-up displays the session trend and session count details for the pods at that location. If you have deactivated the Cloud Monitoring Service feature, the pop-up displays a pie chart of current sessions by session type and the session count details for the pods at that location. Clicking on the VIEW link under the list of pods opens the Global Footprint - Sessions page for that location.

The area to the right of the map shows the total number of end-user sessions for your pods. This total includes connected, active, and idle sessions. It then lists the pods with the number of sessions for each. Hovering on a pod in the list opens the information pop-up on the map for the location where that pod is located. For Horizon pods, the pod name is a link that you can click to launch Horizon Console for that pod's Horizon Connection Server, as described in Launch Horizon Console as a Cloud Service. Clicking on the VIEW link at the bottom of the pod list opens the Global Footprint - Sessions page.

The Global Footprint - Sessions page contains a chart for each session type showing sessions by status and a list of sessions with detailed information for each. The list of sessions displayed can be filtered by location and pod. There are also sort and filter functions for each column of information.
Utilization

Pods Using Microsoft Azure Capacity

For your pods in Microsoft Azure, the Utilization graph displays those pods' allocated capacity and their utilization of allocated desktops and RDS-based remote applications. Roll over the square to see the charted data. In the charted data, the overall capacity percentage is updated once an hour. The capacity percentages for the desktop and application sessions is updated every hour.

By default, the charted data is:

- The last 24 hours of data. One point corresponds to one hour.
- Data averaged over the pods in your environment within the last 24 hours, on an hourly basis.

The system's definition of utilization is the number of active sessions divided by the maximum possible number of sessions (ActiveSessions / MaxPossibleSessions).

Cloud-Connected Horizon Pods

For your cloud-connected Horizon pods, the Utilization graph displays the maximum values for Average CPU, Memory, and Disk Usage. Roll over the square to see the charted data.

By default, the charted data is:

- The last 24 hours of data. One point corresponds to one minute.
- Data averaged over the pods in your environment within those 24 hours, on a minute-by-minute basis.

Sessions

This area shows the breakdown of active and idle sessions for all of your pods' VDI desktops, RDSH desktops, and RDSH applications.

Connection Statistics

This area displays the breakdown of the protocols, Horizon client types, and forms of network access in use by end-user connections to all of your pods.

The Horizon Client chart includes a type labeled Other. The system labels a connection as Other when:

- The connection is using an older version of the Horizon Agent that cannot report the client type.
- The connection is using a VMware-certified Thin Client or Zero Client to access the desktops and applications in cloud-connected Horizon 7 version 7.7 pods.
The Horizon Cloud Administration Console's Dashboard Page - Sessions Tab for a Horizon Cloud Tenant

Use the Sessions tab for working with detailed data about the end-user sessions delivered from your pods. The Cloud Monitoring Service (CMS), one of Horizon Cloud's central services, provides the data that you see on the Sessions tab. The CMS obtains this data from all the cloud-connected pods in your Horizon Cloud tenant environment and presents the data for your use.

**Note** When the Cloud Monitoring Service feature is deactivated for your environment, the Sessions tab does not appear. The Cloud Monitoring Service feature is activated by default. If the feature is not enabled in your environment and you want to use the service to collect session data over time, you can enable the feature on the General Settings page. See [Customizable General Settings for Your Horizon Cloud Tenant Environment](#).

The top of the Sessions tab shows total numbers for sessions and users. The rest of the tab contains several charts representing detailed information about the sessions in your environment.

- You can filter this data by time period, location, deployment type, pod, and pool.
  
  In the Pods filter, selecting All Pods shows session distribution across different pods, and selecting a particular pod shows session distribution across different pools in the selected pod. In both cases, the two colors in each bar represent current session count and remaining unused session count.

- Pointing to chart elements (trend lines, bars) displays numerical data.

- Clicking the **View** link in the bottom left of any of these charts opens a list page that shows a detailed breakdown of the chart data. These pages also indicate the status of each session or VM: green for normal, yellow for warning, or red for critical.
Chart | Description
---|---
Count by Session Status | Trend lines showing number of sessions over time by session status (Total Sessions, Active, Idle, Disconnected).
Resource Consumption | Use the drop-down menus in the upper right of the chart to select the resource (CPU, Memory, IOPS) and deployment type.
  - When the deployment type is Microsoft Azure:
    - The trend lines show resource consumption over time by session type (Total Sessions, Total Desktop Sessions, Total Application Sessions).
    - To the right of the trend line chart is a bar showing the number of sessions per pod (if data for multiple pods is shown) or number of sessions per assignment/farm (if data for a single pod is shown).
  - When the deployment type is On-Premises or VMware Cloud:
    - The trend line shows resource consumption over time for all sessions.
    - To the right of the trend line chart is a pie chart showing resource utilization per pod (if data for multiple pods is shown) or resource utilization per pool/farm (if data for a single pod is shown).

**Note** You can also see detailed information for resource consumption in the CPU Utilization, Memory Utilization, Disk IOPS Utilization charts.

| Metric | Description |
---|---|
CPU Utilization | Number of VMs with different levels of CPU utilization. |
Memory Utilization | Number of VMs with different levels of memory utilization. |
Disk IOPS Utilization | Number of VMs with different levels of disk IOPS utilization. |
Disk Latency | Number of VMs with different levels of disk latency. |
Logon Duration | Number of sessions with different logon durations. |
Latency (Blast) | Number of Blast sessions with different levels of latency. |
Latency (PCoIP) | Number of PCoIP sessions with different levels of latency. |

**Horizon Cloud Administration Console's Dashboard Page - Users Tab for a Horizon Cloud Tenant**

The Users tab displays detailed information about your users and issues they are encountering. The Cloud Monitoring Service (CMS), one of Horizon Cloud's central services, provides the data that you see on the Users tab. The CMS obtains this data from all of the cloud-connected pods in your Horizon Cloud tenant environment and presents the data for your use.

**Customer Issues Included in the Data**

There are three main types of issues included in the data displayed on the Users tab. If any of the following metrics are out of the acceptable range, it counts as a user having an issue:
<table>
<thead>
<tr>
<th>Issue Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latency</td>
<td>Disc latency is outside acceptable range.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol latency or packet loss is outside acceptable range.</td>
</tr>
<tr>
<td>Slow Logon</td>
<td>Logon duration is outside acceptable range.</td>
</tr>
</tbody>
</table>

**Data Filters**

There are filters at the top of the tab that allow you to select the information displayed:

- **Location filter** - If you have multiple locations, you can select a single location to view. All locations are included by default.
- **Deployment filter** - If you have multiple deployment types, you can select a single deployment type to view. All deployment types are included by default.
- **Pod filter** - If you have multiple pods, you can select a single pod to view. All pods are included by default.
- **Pool filter** - If you have multiple pools, you can select a single pool to view. All pools are included by default.

**Global Metrics**

The following values appear in the box closest to the top of the tab.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique Users</td>
<td>Total unique users. This value includes active, idle, and disconnected sessions.</td>
</tr>
<tr>
<td>User Sessions</td>
<td>Total sessions. This value includes active, idle, and disconnected sessions.</td>
</tr>
<tr>
<td>Active Sessions</td>
<td>Total active sessions.</td>
</tr>
<tr>
<td>Issues</td>
<td>Number of users impacted by user experience related issues.</td>
</tr>
</tbody>
</table>

**User Distribution**

This bar chart shows the distribution of users impacted by issues across pods, pools, or assignments.

- If you have **All Pods** selected in the pod filter at the top of the tab, the chart shows users by pod. Clicking the bar for a pod changes the pod filter to select that pod. The tab then shows data only for that pod, and the User Distribution chart shows only users in that pod, broken down by pool.
- If you have a particular pool selected in the pool filter at the top of the tab, the tab shows data only for that pool, and the User Distribution chart shows only users in that pool.

Click the **View** link at the bottom left of the chart to show a list of the users included in the chart with information about issues being encountered.
**Users by Consumption**

List of users by consumption of resources.

- Use the drop-down menu in the top right of the chart to select a resource (CPU, Memory, or Disk IOPS).
- Placing the pointer on the value in the **Utilization by Sessions** column displays the utilization value.
- Click the View link at the bottom left of the chart to show a detailed list of the users included in the chart data. On the list page, there is an additional filter at the top of the page that allows you to select a particular resource (CPU, Memory, or Disk IOPS) to be shown. You can also click the value in the Sessions column to view session details for the user.

**Issues**

Bar chart showing the number of affected users broken down by type of issue (Latency, Protocol, Slow Logon).

Click the View link at the bottom left of the chart to show details for the issues included in the chart data.

- There is an additional filter at the top of the page that allows you to select a particular type of issue (Latency, Protocol, Slow Logon) to be shown.
- Clicking a bar for a particular issue type in the chart sets the issue type filter to that type, so that only those issues are shown.
- The list at the bottom of the page shows the values for the main metrics (Disc Latency, Protocol Latency, and Login Duration), and values for Bandwidth, Frame Rate, and Packet Loss.

**Help Desk Features in Your Horizon Cloud Environment**

The administrative console provides a single pane to use for monitoring an end user's use of virtual desktops and applications and troubleshooting issues. After you configure the role-based access to the console for your help desk administrators, they can log in and use the console's Search feature to look up users. For a particular user, the help desk administrator can then look up that user's sessions to troubleshoot problems and perform some specific desktop maintenance operations.

In your organization, you might have people in the role of helping your end users with any issues those end users might have when using their virtual desktops and remote applications provided by your environment. You might also have people who you want monitoring the end users' sessions or monitoring the desktop instances and farm RDSH instances to identify issues that might potentially impact the sessions.
In the console, the following items support performing those help-desk-related tasks:

- Give your help desk workers' My VMware accounts access to the console with the appropriate help-desk-related role. The About Authentication to a Horizon Cloud Tenant Environment uses My VMware account credentials. For the My VMware accounts, Horizon Cloud provides two predefined help-desk-related roles: Customer Helpdesk and Customer Helpdesk Readonly. You add your help desk workers' My VMware accounts using the console's General Settings page or the Getting Started page. For the steps, see Give Administrative Roles to Individuals in Your Organization for Logging In To and Performing Actions in Your Horizon Cloud Tenant Environment Using the Horizon Cloud Administration Console.

- Give your help desk workers' Active Directory accounts the appropriate Horizon Cloud help-desk-related role. The About Authentication to a Horizon Cloud Tenant Environment also involves Active Directory account credentials. For the Active Directory accounts, Horizon Cloud provides two predefined help-desk-related roles: Help Desk Administrator and Help Desk Read Only Administrator. For the steps, see Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment.

  **Note** Horizon Cloud roles are assigned at the Active Directory group level. The help desk workers' Active Directory accounts must be in an Active Directory group to be granted the roles.

- The console's search feature. The help desk workers can use this feature to search for a specific end user or VM (desktop instance or farm RDSH instance).

- The user card feature. Using a particular user's user card, help desk workers can examine that user's sessions to troubleshoot problems and perform some specific desktop maintenance operations. The operations available to the help desk worker depend on the help-desk-related role assigned that person's Active Directory account.

## Using the Console's Search Feature

Use the administrative console's search feature to locate a specific user or virtual machine (VM) by name in your environment.

**Note** In this release, the VM search is applicable only for VMs located in pods in Microsoft Azure.

You can search within either users or VMs. After selecting whether to search users or VMs, type into the search text box. When you have entered at least three (3) characters in the search text box, names that begin with those characters are displayed. You can continue entering more characters to narrow down the results.
Note  With the VMs search, you can search for RDS server VMs in farms and VDI desktop VMs that are located in your Horizon Cloud inventory.

When you see the one you are searching for, you can click it to get more details about the user or VM. The screen that is displayed depends on whether you clicked a user or a VM:

- For a user, the card for that user is displayed. For details, see About the User Card Feature in Your Horizon Cloud Environment.
- For a VM, the system displays the screen on which you can locate that VM. For example, if you click on a VM in the results list that is an RDS server VM in a farm, the system displays the Servers tab of that farm's details page.

About the User Card Feature in Your Horizon Cloud Environment

Use the administrative console's user card feature as a dashboard to work with a specific user's assigned resources, such as that user's desktops.

Important  To use the user card feature with a Horizon pod, you must configure an event database for the pod's Connection Server after you have installed the Connection Server instance. The event database stores information about Horizon pod-related events as records in a database rather than in a log file. See the Horizon product's Installation guide for information about configuring an event database for events reporting.

You use the console's search feature to display the card for a specific user. See Using the Console's Search Feature for how to search for a user. When you click on a user in the search results, that user's card is displayed.
Use the tabs at the top of the user card to work with those items in your environment that are related to that user.

**Note** In this release, some tabs of the user card are applicable only for items provisioned by pods deployed in Microsoft Azure. When you do not have a pod in Microsoft Azure, those areas display a graphic and message that describes that page is available only when you have deployed a pod in Microsoft Azure. For an example of the displayed graphic, see *Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud*.

### User Card Tabs

<table>
<thead>
<tr>
<th>Sessions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists current and historical user sessions, aggregated from all of your cloud-connected pods. Provides actions you can perform on the listed sessions. For details about these actions, see <em>Actions You Can Take on Sessions</em>.</td>
<td></td>
</tr>
<tr>
<td>By default, only current sessions are shown.</td>
<td></td>
</tr>
<tr>
<td>For sessions provisioned from pods in Microsoft Azure, you can use the drop-down on the left to show historical data for up to seven days.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Since by default current sessions are shown, the Sessions tab will show a value of 0 at the top when there is no current session. When you adjust the display to show historical data, this number is updated to the number of sessions in the selected period.</td>
<td></td>
</tr>
<tr>
<td>Click on a session to open its dashboard. From a session’s dashboard, you can monitor the user session for troubleshooting. See <em>Working with the Session Dashboard</em>.</td>
<td></td>
</tr>
</tbody>
</table>

| Assignments | Lists the user’s assignments. |
| **Note** URL redirection customization assignments are not listed in the user card. |
User Card Tabs | Description
--- | ---
**Desktops** | Lists the user's:
- Active sessions to VDI floating desktops
- Active sessions to RDSH session desktops
- VDI dedicated desktops that have been assigned to this user, even when the user does not have an active session to that desktop.

**Note**  The system assigns a VDI dedicated desktop to a user in one of two ways:
- You explicitly assign that specific dedicated desktop to this particular user, using the **Assign** action in the VDI dedicated desktop assignment's page
- The user claims the desktop from the set that is defined by the VDI dedicated desktop assignment to which that user is entitled. You can entitle a user to a VDI dedicated desktop assignment without explicitly assigning a specific dedicated desktop to that user. You entitle users using the assignment’s **Users/Groups** area. Then when an entitled user launches a desktop from the set of desktops in that assignment for the first time, that user has claimed that VDI dedicated desktop, and the system permanently assigns that VDI dedicated desktop to that user.

On this tab, you can use the standard virtual machine (VM) action buttons to perform actions on the desktops' underlying virtual machines.

**Applications** | Lists the user's entitled remote applications.
**Activity** | Displays the user's activity for selected time periods.

### Actions You Can Take on Sessions

The available actions you can take on a listed session vary based on the type of session, the pod type, and the permissions of the administrator.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Horizon VDI Desktop</th>
<th>Horizon Session-based Desktop</th>
<th>Microsoft Azure VDI Desktop</th>
<th>Microsoft Azure Session-based Desktop</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Send Message</strong></td>
<td>Send a message to the logged-in user. When sent, the message appears on the user’s screen.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Remote Assistance</strong></td>
<td>Available for sessions from a Horizon pod. Initiate a remote assistance session.</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Restart</strong></td>
<td>Available for VDI desktop sessions. Restart the VM.</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Disconnect</strong></td>
<td>Disconnect the session.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Horizon</td>
<td>Horizon</td>
<td>Microsoft Azure</td>
<td>Microsoft Azure</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>---------</td>
<td>---------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Logoff</td>
<td>Log the user off the session.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reset</td>
<td>Resets the VM.</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Working with the Session Dashboard**

When you click one of the active sessions listed on the user card's Sessions tab, the dashboard for that session is displayed. This dashboard has tabs Details and Processes.

**Details tab**

The Details tab provides data about various session-related details that can be used to monitor the end user's session for troubleshooting purposes, such as CPU usage, memory usage, network latency, disk performance, and so on. Scroll through the dashboard and use the **Less** and **More** links to change how many details are displayed on the screen.

*Note* Limited metrics are available for the RDP protocol. If the active session is using the RDP protocol, fewer metrics are available than for the other supported protocols.

The following screenshot shows an example of some of the types of data and actions that are available in the session dashboard.
### LAKSALES0000

#### Details
- **User Name**: ssmin
- **Client IP**: 192.168.1.14
- **Client Name**: ssmin-w02

#### VM
- **Computer Name**: LA4SALSES0001
- **OS Version**: Windows 10 64 bit
- **Desktop Manager**: 100124BC667A4
- **Session Duration**: 6 Minutes
- **State Duration**: 6 Minutes
- **Logon Duration**: 4.96 s
- **Gateway Address**: la4apps.example.com
- **Agent Version**: 19.1.0
- **Pool**: la4sales
- **Pod**: MontereyStores
- **Session State**: Connected
- **Logon Time**: 2/22/19, 6:13 PM
- **Gateway Name**: uag:www.example.com

#### User Experience Metrics

### CPU Usage

![CPU Usage Graph]

### Memory Usage

![Memory Usage Graph]
The User Experience Metrics area of the Details tab displays performance data and provides actions that super administrators and help desk administrators can use to troubleshoot issues in the session.

**Note** In the User Experience Metrics area, for a connected session from a pod in Microsoft Azure, a **Performance Data** menu appears on the right that you can use to select whether real-time or historical data is displayed. In this release, historical data is provided only for pods in Microsoft Azure.

**Processes**

The Processes tab lists the processes and applications that are running in the session and provides an **End Task** button to end a troublesome process or application.

**When the Help Desk Feature Is Not Installed in the Desktop or Farm VM**

When a VDI desktop VM or farm's RDSH VM is based on an image that does not have the Help Desk feature installed, an information alert is displayed when you open the dashboard for a session connected to that VM.

In this case, the VM's data is not reported. Because the usual data is not available, some of the dashboard areas appear blank or empty for such sessions, such as:

- Most of the data about the client and VM is unavailable.
- The User Experience metrics and charts are empty.
- The Processes tab is empty.
- Refresh icons are not clickable.
- Some of the action buttons, such as the **End task** button, are not displayed.
Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types

Horizon Cloud provides an environment in which you can have pods of varying types and deployed into various environments all connected to your single Horizon Cloud tenant environment. When the cloud-connected pods have onboarded to the cloud plane, they are listed on the administrative console's Capacity page. The Capacity page is your one-stop place from which you can oversee and manage your entire fleet of cloud-connected pods — add more pods to your tenant environment, edit characteristics of your pods, and remove pods. Besides using the Pods tab to operate on a pod as a whole entity, on the other Capacity page's tabs, you can configure sites (defined collections of cloud-connected pods) and configure settings for the pods' capacity-related resources such as stored credentials.

This topic has the following sections.

- Introducing the Capacity Page
- Pods — Pod-Level Information
- Pods — Available Pod-Level Actions
- Pods — Details Pages
- Pods — Displayed Health Statuses
- Sites
- Resources
Introducing the Capacity Page

The Capacity page is available from the console's Settings icon. The Capacity page has multiple tabs. One way to think about how to use these tabs is that they provide access to the CRUD operations for the cloud-connected pods, the sites, and the capacity-related resources — the typical create, read, update, delete (CRUD) operations.

Create operations

The Pods tab provides a New action for initiating the deployment of a new cloud-connected pod. The Sites tab provides a New action for defining a new site. The Resources tab provides a Manage action that opens a new window. From that new window, you can add new Microsoft Azure subscription information to store in Horizon Cloud.

Read operations

The Pods tab serves as an access point to drill down and examine the details of a specific pod. You select the name of a listed pod to open a page that displays details about the pod. On the Resources tab, you select the name of a listed resource to open a page that displays details about that resource. On the Sites tab, the Edit button is used to view the details of a listed site.

Update operations

The Pods tab provides an Edit action for changing the pod's editable characteristics. The specific characteristics you can edit for a pod depend on the pod's type, the pod's existing characteristics, and what sorts of changes are supported for that pod type and characteristics. Similarly, the Sites tab provides an Edit action for changing a site's editable characteristics. The Resources tab's Manage action is the entry point for changing a resource's editable characteristics.

Delete operations

The Pods tab provides a Remove action for removing the pod from your Horizon Cloud tenant's fleet of cloud-connected pods. The Sites tab provides a Delete action for removing a site that is defined on that tab. The Resources tab's Manage action is the entry point for deleting the stored capacity-related resource, such as the stored credentials of a Microsoft Azure subscription.

Pods — Pod-Level Information

The Pods tab gives you an overview of your Horizon Cloud tenant environment's fleet of cloud-connected pods, their status, and how they are doing in terms of utilization of their resources. From here, you can also initiate pod-level management actions — such as starting a new pod deployment, editing characteristics of a pod, or removing a pod from your tenant environment. Each type of pod has its unique information provided on the Pods tab.
### Table 4-1. Pod Tab's Per-Pod Information Columns

<table>
<thead>
<tr>
<th>Column</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Icon indicating the health status of the pod, such as online. For the meanings of the various statuses that might be displayed, see Pods — Displayed Health Statuses.</td>
</tr>
<tr>
<td>Pod</td>
<td>Displays the current name of the pod.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the pod's type, such as Microsoft Azure or Horizon.</td>
</tr>
<tr>
<td>Version</td>
<td>For a pod in Microsoft Azure, this column displays the software version from the pod's software manifest information. This number reflects the version of software binaries at which the pod is currently running. For a Horizon pod, this displays the software version of the Horizon Cloud Connector that connects the pod to Horizon Cloud.</td>
</tr>
<tr>
<td>State</td>
<td>This column displays the current state of the pod. The state's meaning depends on the pod's type, whether it is a pod in Microsoft Azure or a Horizon pod.</td>
</tr>
<tr>
<td><strong>pod in Microsoft Azure</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A pod in Microsoft Azure always displays managed state on the Capacity page, because they are always manageable using the Horizon Cloud control plane. You can manage all aspects of the pod using the console and leverage the console's Chapter 3 Introducing the Cloud Monitoring Service's Unified Visibility, Health Monitoring, and Help Desk Features Provided in Horizon Cloud.</td>
</tr>
<tr>
<td><strong>cloud-connected Horizon pod</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A cloud-connected Horizon pod can have either monitored or managed state. Monitored state is the default state of a cloud-connected Horizon pod after you first onboard it to Horizon Cloud. With a pod in monitored state, you can use those console features that provide for Chapter 3 Introducing the Cloud Monitoring Service's Unified Visibility, Health Monitoring, and Help Desk Features Provided in Horizon Cloud.</td>
</tr>
<tr>
<td></td>
<td>If the cloud-connected Horizon pod meets certain requirements, you can move that pod into managed state. A Horizon pod in managed state means that in addition to the console features you can use for monitored pods, you can also create Chapter 6 Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment (MCAs) that use resources from that managed pod and manage those MCAs using the console.</td>
</tr>
<tr>
<td>Location</td>
<td>Displays the geographic location that is currently associated with the pod. To change a pod's associated location, use the Capacity page's Edit action to associate the pod with a different location. See Change a Cloud-Connected Pod's Associated Location, Name, and Description in Your Horizon Cloud Tenant Environment.</td>
</tr>
<tr>
<td>Site</td>
<td>If you have configured your environment for the use of multi-cloud assignments brokered by Universal Broker, this column displays the name of the site that is currently associated with the pod. See Configuring Sites for Universal Broker.</td>
</tr>
</tbody>
</table>
Table 4-1. Pod Tab’s Per-Pod Information Columns (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Desktop &amp; App Utilization</strong></td>
<td>In a Horizon Cloud environment, the desktop and application utilization percentage is a measure of end-user activity in terms of active in-use end-user sessions in use divided by the maximum number of potential sessions. <strong>Note</strong> In this release, the system reports desktop and application utilization only for pods in Microsoft Azure. At the pod level, the Desktop &amp; App Utilization column displays the percentage calculated according to the following: 1 Summing all the active desktop and remote application sessions connect to the pod. 2 Summing all the potential desktop and remote application sessions the pod is configured to provide, based on its configured farm and VDI desktop assignment session maximums. 3 Dividing the first sum by the second sum and multiplying by 100 to get a percentage value. As an example, given a pod in Microsoft Azure with: • One desktop farm that is configured for only one RDSH VM and 10 concurrent sessions per VM (10 potential sessions from that farm). • One applications farm that is configured for two RDSH VMs and 20 concurrent sessions per VM (40 potential sessions from that farm). • One active end-user connection, to a remote application from the applications farm The percentage displayed for that pod in its Desktop &amp; App Utilization column would be 2%, because there are 50 potential sessions (10 potential from the desktop farm and 40 potential from the applications farm), and 1 active session, so the calculation is 1 / 50 = 2%.</td>
</tr>
<tr>
<td><strong>Capacity Used</strong></td>
<td>In your Horizon Cloud environment, capacity utilization is a measure of how much of the pod’s virtual CPU resources (vCPUs) are in use out of the total capacity potentially available for that pod’s use out of the underlying capacity infrastructure into which that pod is deployed. <strong>Note</strong> In this release, the system reports capacity utilization only for pods in Microsoft Azure. The capacity utilization for a pod in Microsoft Azure is based on the Total Regional vCPUs quota of the subscription as a whole. All pods in the same subscription report the same capacity utilization. As an example, for pods in Microsoft Azure, their vCPU capacity usage comes from your Microsoft Azure subscription’s Microsoft.Compute Total Regional vCPUs quota. In addition to the vCPUs used for imported VMs, sealed images, farm RDSH instances, and VDI desktop instances, each pod deployed in Microsoft Azure uses 4 vCPUs for its manager VM and 4 vCPUs for each of its Unified Access Gateway VMs out of your subscription’s total regional vCPUs quota.</td>
</tr>
</tbody>
</table>

Pods — Available Pod-Level Actions

The specifics of the pod-level management actions you can perform from the Capacity page depend on the pod's type for the pod involved in the action — an on-premises Horizon pod, a Horizon pod located in VMware Cloud on AWS, or a pod located in Microsoft Azure. You can initiate pod deployments for those pod types that have automated deployment wizards available in your environment.
### Action

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| **New > pod type** | Initiate deployment of a new cloud-connected pod. Use this action to deploy a pod after your initial one. The pod deployment process you use depends on the type of pod you want and what is supported for your use in the current Horizon Cloud service level. For details about these standard available pod deployment workflows,  
  - For the workflow steps of deploying a new pod into Microsoft Azure, see [Deploying Horizon Cloud Pods into Microsoft Azure from the Capacity Page](#).  
  - For the workflow steps of newly cloud-connecting a Horizon pod using the Horizon Cloud Connector, see [High-Level Workflow When You are Onboarding an Existing Manually Deployed Horizon Pod as Your First Pod to Your Horizon Cloud Tenant Environment](#). |
| **Edit**         | Select a pod and click **Edit** to change the pod's editable characteristics.                                                                 |
| **Remove**       | Select a pod and click **Remove** to remove the pod from your Horizon Cloud tenant.  
  **Tip** The outcome of the remove workflow varies with the pod type.  
  - For a pod deployed in Microsoft Azure, the remove workflow deletes the pod and all of its artifacts from your Microsoft Azure subscription.  
  - For a Horizon pod, the remove workflow disconnects the pod from the Horizon Cloud control plane, so that pod is no longer a cloud-connected pod. The pod's artifacts remain in the capacity environment in which they are deployed — in your on-premises infrastructure or in your VMware Cloud on AWS environment. For a Horizon pod, the remove workflow gives the same result as using the Horizon Cloud Connector **Unplug** action in the Horizon Cloud Connector user interface. |
| **More > Change State** | If a Horizon pod is in monitored state and meets certain requirements, you can change it to managed state for use in multi-cloud assignments.  
  **Note** This action is only available for Horizon pods. Pods deployed in Microsoft Azure are always in managed state and you cannot change the state of these pods.  
  Select a Horizon pod that is in monitored state and select **More > Change State**. For more information, see [Horizon Pods - Enabling a Cloud-Connected Pod for Multi-Cloud Assignments](#) and its subtopics. |

### Pods — Details Pages

When you click a pod's name on the Capacity page, the pod's details page is displayed. The pod's details page provides information and actions you can perform on that pod. The types of detailed characteristics you can see for a pod depend on the pod's type. The types of actions you can perform on the pod depend on the pod's type and the current state of the pod. Some of the actions duplicate the workflows you can perform on the pod from the Capacity page itself, such as editing the pod and removing the pod from your tenant environment.
<table>
<thead>
<tr>
<th>Type</th>
<th>Details</th>
</tr>
</thead>
</table>
| Cloud-connected Horizon pod, either an on-premises pod or one in VMware Cloud on AWS | The page has the following tabs: Summary and Audit Logs. For information about the Audit Logs tab, see Working with Audit Logs.
You use the action buttons on the pod's Summary tab to perform those actions that the service currently supports for use on Horizon pods.
- Use the Edit button to modify the pod's editable characteristics. For details, see Change a Cloud-Connected Pod's Associated Location, Name, and Description in Your Horizon Cloud Tenant Environment.
- Use the Disconnect button to remove the pod from your Horizon Cloud tenant environment. See Removing Cloud-Connected Horizon Pods from Use with Horizon Cloud.
- Use the Schedule Update button to schedule an automated update of the Horizon Cloud Connector virtual appliance, if an updated version is available. See Configure Automated Updates of the Horizon Cloud Connector Virtual Appliance.
- Use the Launch Horizon Console button to run Horizon Console for that pod’s Horizon Connection Server, as described in Launch Horizon Console as a Cloud Service.
- Use the More > Download Connector Logs button to collect log files of Horizon Cloud Connector activity. See Pods in Microsoft Azure - Create a VDI Multi-Cloud Assignment.
The number displayed in the Version No field reflects the version and build number of Horizon Cloud Connector that is currently running on the pod. |
| Pod in Microsoft Azure                                              | The page has the following tabs: Summary, System Activity, User Activity, and Audit Logs. For information about the Audit Logs tab, see Working with Audit Logs.
You can use the action buttons on the pod’s Summary tab to perform those actions that the service currently supports for use on pods in Microsoft Azure.
- Edit some of the pod’s properties. Not all of its properties are editable. The edit workflow is also used for changes to the pod’s configuration beyond changing simple properties. As an example, you use the edit workflow to add a RADIUS two-factor authentication configuration to the pod’s gateway settings or to add gateway settings to a pod that does not already have them. You also use the edit workflow to enable high availability for the pod and to add additional VM (tenant) subnets to the pod. For a list of links to the management tasks for pods in Microsoft Azure, see Managing Your Horizon Cloud Pods Deployed in Microsoft Azure.
- Delete the entire pod, or delete the pod’s gateway configuration.
- Upload an SSL certificate to the pod. For steps, see Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So That Connector Can Trust Connections to the Pod Manager VMs.
- Download logs, using the More > Download Logs choice.
- If an update of the VMware pod software is available, schedule an update using the Schedule Update action. See Updating Your Horizon Cloud Pod.
- If an issue happened during the system’s process of adding additional VM subnets to the pod, you can use the Redeploy failed networks action to trigger the system to try again. |
Table 4-2. Pod Details Page According to Type (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The number displayed in the <strong>Version No</strong> field reflects the version of software binaries at which the pod is currently running. This version is sometimes called the pod's manifest number or the pod's build number. When an updated version of the pod software is available for your pod, the screen displays a message which contains the manifest number that is available to apply to your pod. You can also edit the pod's subscription information from the pod's details page. See <a href="#">Change, Modify, and Update the Subscription Information Associated with Deployed Horizon Cloud Pods</a>. From the pod detail's page, you can also examine the level to which your pods are using your Microsoft Azure subscription limits. See <a href="#">Examine a Subscription's Current Usage of Your Microsoft Azure Limits Using the Horizon Cloud Administration Console</a>.</td>
</tr>
</tbody>
</table>

### Pods — Displayed Health Statuses

The cloud monitoring service retrieves information from each of your pods and uses that information to indicate pod health on the Capacity page and in the Dashboard page. The meanings of the health statuses that are displayed in the Capacity page's Status column are listed in the following sections. On the Capacity page, you can hover your cursor over the status icon to view underlying details for the reported status.

**Online**

The pod has no health issues. The pod's connector service has Online status and all the pod's services are operational.

**Ready**

The pod has no health issues. You might see the Ready status briefly on the Capacity page when a pod is in transition to Online, such as when a pod deployment or update process is finishing.

**Error**

The pod has some critical health issues that you should address. Critical issues will affect the pod operating properly.

**Warn**

The cloud monitoring system has retrieved the health status from the pod and some issues exist. The pod can operate normally because these issues are not critical to pod operations.

**Offline**
The cloud monitoring system detects the pod has no connection service running.

- For a pod in Microsoft Azure, this status typically means that the pod manager VM is not running. This situation is rare, and usually happens when you manually shut down the pod manager using the Microsoft Azure portal or the Microsoft Azure cloud is having an outage.

- For a Horizon pod, this status implies that there is no connectivity between the Horizon Cloud Connector and Horizon Cloud. Check if the Horizon Cloud Connector is operational and running.

**Unknown**

The cloud monitoring system cannot retrieve the health status from the pod. For a Horizon pod, this status typically means the API call to that Horizon pod cannot retrieve information, such as when the Horizon Cloud Connector instance or the Connection Server instances are having issues and cannot provide the needed data.

**Sites**

The Sites tab is displayed when your environment is configured to use the Universal Broker. See Working with Sites in a Universal Broker Environment and its subtopics for detailed information about sites in a Horizon Cloud environment.

**Resources**

Horizon Cloud needs specific types of information to work with the pods that live in each type of resource capacity. This information is stored in configuration sets in Horizon Cloud when you associate the resource capacity with your Horizon Cloud environment. The Resources tab provides:

- An overview of those stored configuration settings.

- A **Manage** action to manage those settings. As of today, this tab provides the ability to manage the stored Microsoft Azure subscription information that Horizon Cloud uses to run and manage the pods you have deployed in your Microsoft Azure cloud capacity. See [Horizon Cloud — Deleting, Editing, and Adding Microsoft Azure Subscription Information](#).

This chapter includes the following topics:

- **Launch Horizon Console as a Cloud Service**
- **Deploying Pods Using the Capacity Page**
- **Change a Cloud-Connected Pod’s Associated Location, Name, and Description in Your Horizon Cloud Tenant Environment**
- **Removing Cloud-Connected Horizon Pods from Use with Horizon Cloud**
Launch Horizon Console as a Cloud Service

You can administer a cloud-connected Horizon pod by running Horizon Console for that pod's Horizon Connection Server. When launched from Horizon Universal Console, Horizon Console runs as an integrated cloud service from the Horizon Control Plane, with support for single sign-on (SSO) authentication.

You can run Horizon Console for a specific Horizon pod's Connection Server from either the pod details page or the Dashboard page. Horizon Console opens in a new browser tab using the SSO credentials of your Horizon Universal Console login. No additional credentials are required.

You can use Horizon Console as a cloud service to access all the same pod administration features when running Horizon Console natively, except for the following:

- Help Desk features. To troubleshoot issues associated with your Horizon pod, use the Help Desk Features in Your Horizon Cloud Environment instead.
- JMP Server features. To define and manage desktop workspaces for users, configure multi-cloud assignments instead, as described in Chapter 6 Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment.

For detailed information about using Horizon Console, see the VMware Horizon Documentation.

**Note** If the Horizon pod does not meet the requirements for running Horizon Console as a cloud service, the native instance of Horizon Console opens instead without SSO authentication, if the pod's Connection Server is accessible to public networks. For example, if the pod is running Connection Server 7.11 or earlier or Horizon Cloud Connector 1.5 or earlier, a new browser tab opens the native Horizon Console page prompting you to log in to the pod's Connection Server. However, if the Connection Server is not publicly accessible (such as behind a firewall), the browser tab opens with a connection error. In such cases, you must run Horizon Console directly from the Connection Server endpoint.

**Prerequisites**

To run Horizon Console from the Horizon Control Plane, you must be logged in to Horizon Universal Console with the Super Administrator role.

In addition, verify that the Horizon pod is running the following components:

- Horizon Connection Server 7.12 or later
- Horizon Cloud Connector 1.6 or later

**Note** If the pod is running Horizon Cloud Connector 1.6, only the English-language version of Horizon Console is supported. If the pod is running Horizon Cloud Connector 1.7 or later, all language versions of Horizon Console are supported.
Procedure

- Run Horizon Console from the pod details page.
  - a In Horizon Universal Console, select Settings > Capacity.
  - b In the list of pods on the Capacity page, click the name of the Horizon pod that you want to administer.
  - c In the pod details page, click Launch Horizon Console.

- Run Horizon Console from the Dashboard page.
  - a In Horizon Universal Console, select Monitor > Dashboard.
  - b On the Overview tab of the Dashboard page, under the Issues or Session view, click the name of the Horizon pod that you want to administer.

What to do next

If you log out from Horizon Console as a cloud service, you are redirected to the login screen for Horizon Universal Console.

Deploying Pods Using the Capacity Page

When your Horizon Cloud customer account has its first cloud-connected pod and registered Active Directory domain, you can access the administrative console's Capacity page. Then you can use the Capacity page to start adding additional cloud-connected pods.

In the console, you open the Capacity page using Settings > Capacity. To add a pod, you click New > Pod, and then select the option for the pod's capacity type.

- Microsoft Azure
- On-Premises
- VMware Cloud on AWS

What happens next depends on your selected capacity type and the features that your Horizon Cloud customer account is licensed to use.

- If you select Microsoft Azure, an automated pod deployment wizard opens. You run the pod deployment wizard to deploy the pod's components into the Microsoft Azure cloud. For detailed steps, see Deploying Horizon Cloud Pods into Microsoft Azure from the Capacity Page.

- If you select On-Premises or VMware Cloud on AWS, an information box opens and describes the requirement to download and install the Horizon Cloud Connector. To connect these pod types requires you to deploy the Horizon Cloud Connector appliance into your pod's infrastructure environment and configure the connector to communicate with the pod's
Connection Server and with Horizon Cloud. For detailed steps for connecting a Horizon pod after you have downloaded the Horizon Cloud Connector, see the Connect Horizon Cloud with an Existing Manually Deployed Horizon Pod topic in the Horizon Cloud Deployment Guide.

Deploying Horizon Cloud Pods into Microsoft Azure from the Capacity Page

After your Horizon Cloud environment gets its first cloud-connected pod, you can deploy additional pods from the Capacity page. To deploy a pod into the Microsoft Azure cloud, you run the automated deployment wizard from the Capacity page.

**Caution** The IP addresses mentioned in these steps are examples. You should use the address ranges that meet your organization's needs. For each step that mentions an IP address range, substitute ones that are applicable for your organization.

The wizard has multiple steps. After specifying the information in a step, click **Next** to move to the next step.

**Prerequisites**

Before you start the pod deployment wizard, verify that you have the required items. The items you need to provide in the wizard vary according to the pod configuration options you want. See the list in Prerequisites for Running the Pod Deployment Wizard.

In addition to the items required by the configuration you want for an additional pod, your first cloud-connected pod must be completely deployed and the Active Directory domain-bind and domain-join steps completed before you can deploy additional pods. All cloud-connected pods within your customer account record share the same Active Directory information, and each cloud-connected pod must have line-of-sight to all of the cloud-configured Active Directory domains. For more information, see Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment.
Procedure

1. In the console, start the pod deployment wizard by navigating to **Settings > Capacity**, clicking **New > Pod**, and selecting the Microsoft Azure option.

   The Add Cloud Capacity wizard opens to its first step.

   ![Add Microsoft Azure Capacity](image)

2. On the wizard's first step, specify the subscription to use for this pod by selecting the name of a previously entered subscription or entering new subscription information.

   If you select an existing subscription, the step is populated with that subscription's information that was previously entered into the system.

   **Important** If you are entering new information, you must ensure the subscription information you enter meets the subscription requirements described in **Prerequisites for Running the Pod Deployment Wizard**, especially that the service principal has the role permissions it needs.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply Subscription</td>
<td>Select the name of a previously entered subscription or select Add New to enter new subscription information.</td>
</tr>
</tbody>
</table>
| Subscription Name             | When providing new subscription information, enter a friendly name so you can identify this subscription from other previously entered subscriptions.  
The name must start with a letter and contain only letters, dashes, and numbers.                                                   |
| Environment                   | Select the cloud environment associated with your subscription, for example:  
- Azure - Commercial, for the standard global Microsoft Azure cloud regions  
- Azure - China, for the Microsoft Azure in China cloud  
- Azure - US Government, for the Microsoft Azure US Government cloud                                                                 |
| Subscription ID               | Enter your cloud capacity subscription ID (in UUID form). This subscription ID must be valid for the environment you selected. For Microsoft Azure, you can obtain this UUID from your Microsoft Azure portal's Subscriptions area. |
| Directory ID                  | Enter your Microsoft Azure AD Directory ID (in UUID form). For Microsoft Azure, you can obtain this UUID from your Microsoft Azure Active Directory properties in the Microsoft Azure portal. |
| Application ID                | Enter the application ID (in UUID form) associated with the service principal you created in the Microsoft Azure portal. Creating an application registration and its associated service principal in your Microsoft Azure Active Directory is a prerequisite. |
| Application Key               | Enter the key value for the service principal's authentication key that you created in the Microsoft Azure portal. Creating this key is a prerequisite.                                                        |
| Use a Different Subscription for External Gateway | Enable this toggle when you want to deploy an external Unified Access Gateway configuration into its own subscription, separate from the pod's subscription. Using separate subscriptions for the external gateway gives your organization the flexibility to assign separate teams control over those subscriptions, depending on their area of expertise. It allows for more granular access control for which people in your organization can access the pod's assets in its subscription's resource groups and which people can access the gateway's assets. When this toggle is turned on, the fields for entering the gateway's subscription information are displayed. Specify the information in those fields as you did for the pod's subscription. |

3 Proceed to the next step by clicking Next.

When you click Next, in the case where you added a new subscription, the system verifies the validity of all of the specified values and whether they are appropriately related to each other, such as:

- Is the specified subscription ID valid in the selected environment.
- Are the specified directory ID, application ID, and application key valid in that subscription.
- Does the application's service principal for the specified application ID have either the Contributor role or a custom role configured for the role operations that the pod deployer requires?
Is the application's service principal for the specified application ID assigned a role that permits all of the operations that the deployment process requires for the type of deployment you are doing. For a description of the service principal and its role requirements, see the topic Create the Required Service Principal Needed by the Horizon Cloud Pod Deployer by Creating an Application Registration and Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions.

If you see an error message about checking values, at least one of the values is invalid either by not existing in your subscription or not having a valid relationship with another of the values. For example, if you specified a Directory ID that is in your subscription but you specified an Application ID value that is in a different directory, the error message will display.

More than one value might be invalid if that error message appears. If you see that error message, verify the subscription-related information that you collected and the configuration of the service principal.

4 In this wizard step, specify details such as the name of the pod, as well as networking information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>The wizard displays Site when your tenant environment is configured to use Universal Broker for your pods in Microsoft Azure and you are deploying additional pods. You associate the pod with a site. You can either select an existing site or with the Default-Site or specify the name of a new one. The Capacity page's Sites tab lists the sites that are already configured in your environment.</td>
</tr>
<tr>
<td>Pod Name</td>
<td>Enter a friendly name for this pod. This name is used in the administrative console to identify this pod from your other pods.</td>
</tr>
<tr>
<td>Note</td>
<td>This name must be unique among your existing pods in your Horizon Cloud customer account. The name cannot match the name of one of the pods listed in the Capacity page.</td>
</tr>
<tr>
<td>Location</td>
<td>Select an existing city name or click Add to specify a new city. The system groups your pods according to city name, and depicts them on the console's Dashboard page's Horizon Global Footprint map. When you click Add, start typing the name of a city. The system automatically displays world city names in its backend geography lookup table that match your entered characters, and you can choose a city from that list.</td>
</tr>
<tr>
<td>Note</td>
<td>You must select a city from the system's autocomplete list. Currently, due to a known issue, the location names are not localized.</td>
</tr>
<tr>
<td>Microsoft Azure Region</td>
<td>Select the physical geographic Microsoft Azure region into which you want the pod to be deployed. The available regions are determined by the previously selected Microsoft Azure environment. Consider choosing the region based on its proximity to the end users you intend to serve with this pod. Nearer proximity would provide lower latency. Important Not all Microsoft Azure regions support GPU-enabled virtual machines. If you want to use the pod for GPU-capable desktops or remote applications, ensure that the Microsoft Azure region you select for the pod provides for those NV-series VM types that you want to use and which are supported in this Horizon Cloud release. See the Microsoft documentation at <a href="https://azure.microsoft.com/en-us/regions/services/">https://azure.microsoft.com/en-us/regions/services/</a> for details.</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Optional: Enter a description for this pod.</td>
</tr>
</tbody>
</table>
| **Azure Resource Tags** | Optional: Create custom tags to be applied to Azure resource groups. Azure resource tags are only applied to the resource groups, and are not inherited by the resources in the groups.  
To create the first tag, enter information in the Name and Value fields. To create an additional tag, click + and then enter information in the Name and Value fields that appear below the existing ones.  
- You can create a maximum of 10 tags.  
- The tag name is limited to 512 characters, and the tag value is limited to 256 characters. For storage accounts, the tag name is limited to 128 characters, and the tag value is limited to 256 characters.  
- Tag names cannot contain the following characters: < > % & \ ? /  
- Tag names cannot contain these case-insensitive strings: ‘azure’, ‘windows’, ‘microsoft’  
- Tag names and tag values can only contain ASCII characters. Blank spaces and characters outside the standard 128-character ASCII set (also known as high ASCII or extended ASCII characters) are not allowed. |
| **High Availability** | This toggle determines whether the deployed pod has two pod manager VMs. In the deployed pod, one pod manager VM is the active one and the other is ready to handle failover if the active one goes offline, which provides high availability for the pod. For details, see *High Availability and Your Horizon Cloud Pod in Microsoft Azure*.  
If you switch off this toggle, the pod is deployed with a single pod manager VM. If that pod manager VM goes offline, there is no second one ready to handle the failover.  
**Note** Even when this toggle is switched off, the pod still deploys with the pod architecture that has the memory-optimized, Gen 5, Microsoft Azure Database for PostgreSQL server and a Microsoft Azure load balancer in front of the pod manager VM. When you see this toggle displayed in the pod deployment wizard, its presence indicates that the pod deployer will deploy a pod using the pod architecture that has those items. A pod deployed with this toggle turned on will have a second pod manager VM, while a pod deployed with this toggle turned off will have a single pod manager VM. |
| **Virtual Network** | Select a virtual network from the list.  
Only virtual networks (V Nets) that exist in the region selected in the *Microsoft Azure Region* field are shown here. You must have already created the VNet you want to use in that region in your Microsoft Azure subscription. |
| **Use Existing Subnet** | Enable this toggle if you have created subnets in advance to meet the pod's subnet requirements. When this toggle is set to Yes, the wizard’s fields for specifying subnets change to drop-down selection menus.  
**Important** The wizard does not support using an existing subnet for one of the required subnets and also entering CIDR addresses for the other required subnets. When this toggle is set to Yes, you must select from existing subnets for all the pod's required subnets. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Subnet</td>
<td>When <em>Use Existing Subnet</em> is enabled, this menu lists the subnets available on the VNet selected for <strong>Virtual Network</strong>. Select the existing subnet that you want to use for the pod's management subnet.</td>
</tr>
<tr>
<td><strong>Management Subnet (CIDR)</strong></td>
<td><em>Important</em> Select a subnet that has the Microsoft.SQL service configured as a service endpoint for that subnet. This service endpoint supports the required communication between the pod manager VMs and the pod's Azure Postgres database over the management subnet.</td>
</tr>
<tr>
<td></td>
<td>Select an empty subnet, one that has no other resources attached to it. If the subnet is not empty, unexpected results might occur during the deployment process or pod operations.</td>
</tr>
<tr>
<td></td>
<td>When <em>Use Existing Subnet</em> is switched off, enter a subnet address range (in CIDR notation) for the deployer to create a subnet to which the pod and Unified Access Gateway instances will get connected, such as 192.168.8.0/27. For the management subnet, a CIDR of at least /27 is required.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> When you do not select the wizard option to use existing subnets, the subnet must not already exist in your Microsoft Azure environment. If it already exists, you will get an error when you try to proceed to the next wizard step.</td>
</tr>
<tr>
<td>VM Subnet - Primary</td>
<td>This field relates to the subnet used for those VMs that the pod provisions to provide your end-user desktops and applications. Such VMs include the golden image VMs, the farms' RDSH-capable VMs, and the VDI desktop VMs.</td>
</tr>
<tr>
<td>VM Subnet (CIDR) - Primary</td>
<td>When <em>Use Existing Subnet</em> is enabled, this menu lists the subnets available on the VNet selected for <strong>Virtual Network</strong>. Select the existing subnet that you want used for those VMs.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> Select an empty subnet, one that has no other resources attached to it. If the subnet is not empty, unexpected results might occur during the deployment process or pod operations.</td>
</tr>
<tr>
<td></td>
<td>When <em>Use Existing Subnet</em> is switched off, enter a subnet address range (in CIDR notation) for the deployer to create this subnet as the pod is deployed, such as 192.168.12.0/22. For the desktop subnet, a CIDR of at least /27 is required, and a CIDR of /22 is recommended.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> Ensure the range that you enter is large enough to allow for accommodating the number of VMs you anticipate you will want this pod to provision to provide your farms' RDSH-capable VMs and the VDI desktop VMs for your end users. This desktop subnet cannot be extended after the pod is deployed.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> When you do not select the wizard option to use existing subnets, the subnet must not already exist in your Microsoft Azure environment. If it already exists, you will get an error when you try to proceed to the next wizard step.</td>
</tr>
</tbody>
</table>
### Option | Description
--- | ---
**NTP Servers** | Enter the list of NTP servers you want to use for time synchronization, separated by commas. An NTP server you enter here can be a public NTP server or your own NTP server that you set up for providing time synchronization. The NTP servers you specify here must be reachable from the virtual network you selected in the Virtual Network field for the pod to use. In this field, you can specify each NTP server either by its numeric IP address or its domain name. When you provide a domain name in this field instead of a numeric IP address, you must ensure that the DNS configured for your virtual network can resolve the specified name. Examples of public NTP server domain names are time.windows.com, us.pool.ntp.org, time.google.com.

**Use Proxy** | If you require a proxy for outbound Internet connectivity, enable this toggle and complete the associated displayed fields. The pod deployer requires outbound access to the Internet to securely download software into the Microsoft Azure cloud environment and connect back to the Horizon Cloud cloud control plane. To enable the pod to use your proxy configuration, you must provide the following information after enabling the toggle.

- **Proxy** (required): Type the hostname or IP address for your proxy server.
- **Port** (required): Type the port number that is specified in your proxy server configuration.

If your proxy server configuration requires a user name and password for authentication, provide those credentials also.

![Use Proxy](image)

5 Proceed to the next step by clicking **Next**.

The following screenshot is an example of the next step when it is initially displayed. Some controls are displayed only when you selected at the first wizard step to use a different subscription for the external Unified Access Gateway gateway configuration.
6 Specify the information for at least one gateway configuration, and optionally any RADIUS two-factor authentication.

Complete the steps in the following topics:

- Specify the Horizon Cloud Pod's Gateway Configuration
Specify Two-Factor Authentication Capability for the Pod

**Note** In this step, you can choose whether to have the gateway resource groups inherit the same custom tags that you specified for the pod or specify different ones. Both gateway types will use the same set of specified tags.

7 Click **Validate & Proceed**.

When you click **Validate & Proceed**, the system verifies the validity and appropriateness of your specified values, such as:

- Are the subnets valid and non-overlapping with other networks in the selected region within your subscription.
- Are there enough virtual machine (VM) and cores in your subscription's quota to build out the pod.
- Is the certificate in the correct PEM format.

If you see an error message about overlapping networks, verify whether you have existing subnets using the same values already in your subscription.

If everything validates OK, the summary page displays.

8 Review the summarized information and click **Submit**

The system starts deploying the pod into your Microsoft Azure environment.

**Results**

Deploying the pod can take up to an hour. Until the pod is successfully deployed, a progress icon is displayed for that pod. You might need to refresh the screen in your browser to see the updating progress.

**Important** When deploying additional pods in Microsoft Azure China cloud, the process can take longer than an hour to complete. The process is subject to geographic network issues that can cause slow download speeds as the binaries are downloaded from the cloud control plane.

**What to do next**

If you specified RADIUS two-factor authentication for the pod's gateway configurations, you must complete the following tasks.

- If you configured an external gateway with RADIUS settings and that RADIUS server is not reachable within the same VNet as used by the pod, or within the peered VNet topology if you deployed the external gateway into its own VNet, verify, configure that RADIUS server to allow client connections from the IP address of the external gateway's load balancer. In an external gateway configuration, the Unified Access Gateway instances attempt contact with the RADIUS server using that load balancer address. To allow the connections, ensure the load balancer resource's IP address that is in that external gateway's resource group is specified as a client in your RADIUS server configuration.
If you configured an internal gateway, or an external gateway and your RADIUS server is reachable within the same VNet as used by the pod, configure the RADIUS server to allow connections from the appropriate NICs that were created in the gateway’s resource group in Microsoft Azure that must communicate with the RADIUS server. Your network administrator determines the RADIUS server’s network visibility to the pod’s Azure Virtual Network and subnets. Your RADIUS server must allow client connections from the IP addresses of those gateway NICs that correspond to the subnet for which your network administrator has given network visibility to the RADIUS server. The gateway’s resource group in Microsoft Azure has four NICs that correspond to that subnet, two that are currently active for the two Unified Access Gateway instances and two that are idle and will become the active ones after the pod goes through an update. To support connectivity between the gateway and the RADIUS server both for ongoing pod operations and after each pod update, ensure the IP addresses of those four NICs are specified as clients in the RADIUS server configuration.

If you specified having a Unified Access Gateway configuration, ensure you set up the appropriate CNAME records in your DNS server according to the type of configuration you specified.

- For an external Unified Access Gateway configuration, map the FQDN that you entered in the deployment wizard to the pod's Microsoft Azure public load balancer's auto-generated FQDN.
- For an internal Unified Access Gateway configuration, map the FQDN that you entered in the deployment wizard to the pod's Microsoft Azure internal load balancer's private IP address.

See Obtain the Pod Gateway’s Load Balancer Information to Map in your DNS Server for the steps to locate the load balancer information in the pod's details page.
Prerequisites for Running the Pod Deployment Wizard

Before you run the pod deployment wizard, verify that your environment satisfies these prerequisites. You must have the following items so that you can provide the requested values in the pod deployment wizard and proceed through the wizard.

**Important** Before launching the pod deployment wizard and starting to deploy your pod, in addition to the requirements below, you must be aware of the following key points:

- Starting with the July 2020 service release, in brand new environments, new pods are required to deploy with at least one gateway configuration. If your customer account was created prior to the July 2020 release, but you have not yet deployed your first pod, deployment of that first pod will require configuring at least one gateway configuration at the time of pod deployment.

- Successful pod deployment requires that none of the Microsoft Azure Policies that you or your IT team have set in your Microsoft Azure environment block, deny, or restrict creation of the pod's components. Also you must verify that your Microsoft Azure Policies Built-in Policy definitions do not block, deny, or restrict creation of the pod's components. As an example, you and your IT team must verify that none of your Microsoft Azure Policies block, deny, or restrict creation of components on Azure storage account. For information about Azure Policies, see the Azure Policy documentation.

- The pod deployer requires that your Azure storage account allow for the deployer to use the Azure StorageV1 and StorageV2 account types. Ensure that your Microsoft Azure Policies do not restrict or deny the creation of content requiring the Azure StorageV1 and StorageV2 account types.

- As part of the pod and gateway deployment processes, unless you specify custom resource tags in the deployment wizard, Horizon Cloud creates resource groups (RGs) in your Microsoft Azure subscription that do not have tags on them, including the initial resource group that is created for the temporary jump box that orchestrates those deployment processes. As of the October 8, 2020 cloud plane refresh, the deployment wizard has a feature in which you can specify custom resource tags that you want applied to the deployer-created resource groups. If you do not specify custom resource tags and your Microsoft Azure subscription has any type of resource tag requirement, pod deployment will fail if you try to deploy a pod into that subscription, or it will fail at the time of pod updates or adding a gateway configuration to a pod. If you are not planning to use the deployment wizard’s custom resource tags feature, you must verify that your Microsoft Azure Policies allows creation of the pod's untagged resource groups in the target subscription. For the list of RGs that the deployer creates, see the Administration Guide’s Resource Groups Created For a Pod Deployed In Microsoft Azure topic.

- All cloud-connected pods must have line-of-sight to the same set of Active Directory domains at the time you deploy those pods.
**Prerequisites for All Deployments**

- When you add another pod, you can use the same subscription that you used before for your previous pods, or you can use a different subscription if required by your organization. If you plan to use a different subscriptions, you must perform the steps described in the Deployment Guide to obtain the subscription ID, directory ID, application ID, and application key. You must ensure the subscription you use meets the requirements described in that guide, especially that the service principal has the appropriate role permissions granted at the relevant levels in your subscription. You can navigate to the getting started document online from the Horizon Cloud Documentation page.

- When your tenant is configured to use Universal Broker for your pods in Microsoft Azure, when running the pod deployment wizard to add a new pod, you must specify a site. You can either select an existing site or specify a new one.

- Verify that you have a VNet in the region in which you want to deploy the pod and that the VNet meets the requirements as described in Configure the Required Virtual Network in Microsoft Azure.

**Important**  Not all Microsoft Azure regions support GPU-enabled virtual machines. If you want to use the pod for GPU-capable desktops or remote applications, ensure that the Microsoft Azure region you select for the pod provides for those NV-series VM types that you want to use and which are supported in this Horizon Cloud release. See the Microsoft documentation at [https://azure.microsoft.com/en-us/regions/services/](https://azure.microsoft.com/en-us/regions/services/) for details.

- Verify that your VNet is configured to point to a DNS that can resolve external addresses. The pod deployer must be able to reach external addresses in the Horizon Cloud control plane to securely download the pod software into your Microsoft Azure environment.

- Verify that the pod deployer's DNS, ports, and protocols requirements are met, as described in DNS Requirements for a Horizon Cloud Pod in Microsoft Azure and Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later.

- If you require use of a proxy for outbound Internet access, verify you have the networking information for your proxy configuration and the authentication credentials it requires, if any. The pod deployment process requires outbound Internet access.

- Verify that you have the information for at least one NTP server that you want the pod to use for time synchronization. The NTP server can be a public NTP server or your own NTP server that you set up for this purpose. The NTP server you specify must be reachable from the virtual network you configured. When you plan to use an NTP server using its domain name instead of a numeric IP address, also ensure that the DNS configured for the virtual network can resolve the NTP server's name.
If you do not want the deployer to automatically create the subnets it needs, verify that the required subnets have been created in advance and exist on the VNet. For the steps to create the required subnets in advance, see In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure and When Using Existing Subnets for a Horizon Cloud Pod in Microsoft Azure.

**Caution**  The subnets you manually create on your VNet in advance for the pod deployment must remain empty. Do not reuse existing subnets that already have items that are using IP addresses on those subnets. If an IP address is already in use on the subnets, issues such as the pod failing to deploy and other downstream IP-conflict issues have a high likelihood of occurring. Do not put any resources on these subnets or otherwise use any of the IP addresses. This caution notice includes pods deployed from Horizon Cloud — do not reuse subnets on which you already have a deployed pod.

**Important**  When deploying additional pods after your first one, you cannot reuse an existing subnet which is already in use by an existing pod.

If you are going to have the deployer create the required subnets, verify that you know the address ranges you are going to enter into the wizard for the management subnet, desktop subnet, and DMZ subnet. The DMZ subnet is required when you want the external Unified Access Gateway configuration. Also verify that those ranges do not overlap. You enter the address ranges using CIDR notation (classless inter-domain routing notation). The wizard will display an error if the entered subnet ranges overlap. For the management subnet range, a CIDR of at least /27 is required. For the DMZ subnet range, a CIDR of at least /28 is required. If you want to keep the management and DMZ subnet ranges co-located, you can specify the DMZ subnet range similar to the management subnet with an IP specified. For example, if the management subnet is 192.168.8.0/27, a matching DMZ subnet would be 192.168.8.32/27.

**Important**  The CIDRs you enter in the wizard's fields must be defined so that each combination of prefix and bit mask results in an IP address range having the prefix as the starting IP address. Microsoft Azure requires that the CIDR prefix be the start of the range. For example, a correct CIDR of 192.168.182.48/28 would result in an IP range of 192.168.182.48 to 192.168.182.63, and the prefix is the same as the starting IP address (192.168.182.48). However, an incorrect CIDR of 192.168.182.60/28 would result in an IP range of 192.168.182.48 to 192.168.182.63, where the starting IP address is not the same as the prefix of 192.168.182.60. Ensure that your CIDRs result in IP address ranges where the starting IP address matches the CIDR prefix.

If you are going to have the deployer create the required subnets, verify that subnets with those address ranges do not already exist on the VNet. In this scenario, the deployer itself will automatically create the subnets using the address ranges you provide in the wizard. If the wizard detects subnets with those ranges already exist, the wizard will display an error about overlapping addresses and will not proceed further. If your VNet is peered, also verify that the CIDR address spaces that you plan to enter in the wizard are already contained in the VNet's address space.
Prerequisites for the Unified Access Gateway Configurations

If you are planning to have the pod use a Unified Access Gateway configuration, you must provide:

- The fully qualified domain name (FQDN) which your end users will use to access the service. Starting with the new pod manifest made available in the July 2020 quarterly service release, when deploying both of the gateway configurations on a pod, you are required to specify the same FQDN for both gateway configurations. After the pod is deployed with both the external and internal gateway configuration, you must configure the incoming end-user client traffic to route to the appropriate load balancer. The goal is to set up the routing so that client traffic from the Internet is routed to the external gateway's Microsoft Azure Public Load Balancer and client traffic from your intranet is routed to the internal gateway's Microsoft Azure Internal Load Balancer. Because both gateways will have the same FQDN, you configure Split DNS (Split Domain Name System) to resolve the gateway address either to the external gateway or internal gateway depending on the origin network of the end-user client’s DNS query. Then the same FQDN used in the end-user client can route to the external gateway when the client is on the Internet and route to the internal gateway when the client is on your internal network.

**Important** This FQDN cannot contain underscores. In this release, connections to the Unified Access Gateway instances will fail when the FQDN contains underscores.

- A signed SSL server certificate (in PEM format) based on that FQDN. The Unified Access Gateway capabilities require SSL for client connections, as described in the Unified Access Gateway product documentation. The certificate must be signed by a trusted Certificate Authority (CA). The single PEM file must contain the full entire certificate chain with the private key. For example, the single PEM file must contain the SSL server certificate, any necessary intermediate CA certificates, the root CA certificate, and private key. OpenSSL is a tool you can use to create the PEM file.

**Important** All certificates in the certificate chain must have valid time frames. The Unified Access Gateway VMs require that all of the certificates in the chain, including any intermediate certificates, have valid time frames. If any certificate in the chain is expired, unexpected failures can occur later as the certificate is uploaded to the Unified Access Gateway configuration.

- If you are deploying with an external Unified Access Gateway configuration, you must specify a DMZ (demilitarized zone) subnet. You can provide for this DMZ subnet by one of two ways:
  - Creating the DMZ subnet in advance on the VNet. With this method, you also have to create the management and desktop tenant subnets in advance. See the steps in In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure.
  - Having the deployer automatically create the DMZ subnet during deployment. With this method, you must have the address range you are going to enter into the wizard for the DMZ subnet and verify that the range does not overlap with the ranges for the
management and desktop tenant subnets. You enter the address ranges using CIDR notation (classless inter-domain routing notation). The wizard will display an error if the entered subnet ranges overlap. For the DMZ subnet range, a CIDR of at least /28 is required. If you want to keep the management and DMZ subnet ranges co-located, you can specify the DMZ subnet range the same as the management subnet with an IP specified. For example, if the management subnet is 192.168.8.0/27, a matching DMZ subnet would be 192.168.8.32/27. Also see the important note in Prerequisites for All Deployments about ensuring the IP address range has a combination of prefix and bit mask that results in the range having the prefix as the starting IP address.

- If you are deploying with an external Unified Access Gateway configuration and you want to prevent having a public IP address for the configuration's load balancer, you must specify an IP address that you have mapped in your DNS settings to the FQDN which your end users will use for PCoIP connections in their Horizon clients.

For more information about the PEM file considerations required by Unified Access Gateway, see Convert a Certificate File to the PEM Format Required for Pod Deployment.

Prerequisites When Deploying With an External Unified Access Gateway Configuration Using its Own VNet or Subscription Separate from the Pod's VNet or Subscription

Along with the above prerequisites when deploying with a Unified Access Gateway configuration, these prerequisites are specific to the use case of deploying the external gateway in its own VNet or own subscription. Using its own subscription is a special case of using its own VNet, because the separate subscription must have its own VNet, because V Nets are scoped to a subscription.

- The VNet for the gateway must be peered with the pod's VNet.
- Verify that either the required subnets have been created in advance and exist on the VNet, or that the CIDR address spaces that you plan to enter in the wizard are already contained in the VNet's address space. Because the V Nets are peered, the deployer will not be able to expand the VNet automatically if you enter into the wizard CIDR address spaces that are not already contained in the VNet's address space. If that happens, the deployment process will fail.

Tip The best practice is to create the subnets in advance. For the steps to create the required subnets in advance, see In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure and When Using Existing Subnets for a Horizon Cloud Pod in Microsoft Azure.

- If you are using a separate subscription for the external gateway, verify that you have the subscription information, as described in Subscription-Related Information for the Horizon Cloud Pod Deployment Wizard.
- If you are using a separate subscription for the external gateway and are planning to deploy the gateway into a named resource group that you create instead of having the deployer
auto-create the resource group, verify that you have created that resource group in that subscription. You will select that resource group by name in the wizard. Also verify that you have granted the required access to that resource group for the deployer to operate in it, as described in Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions.

Prerequisites When Deploying With a Two-Factor Authentication Configuration

If you are planning to use the two-factor authentication capability, or use it with an on-premises two-factor authentication server, verify that you have the following information used in your authentication server's configuration, so that you can provide it in the appropriate fields in the pod deployment wizard. If you have both a primary and secondary server, obtain the information for each of them.

- IP address or DNS name of the authentication server
- The shared secret that is used for encryption and decryption in the authentication server's protocol messages
- Authentication port numbers, typically the 1812 UDP port.
- Authentication protocol type. The authentication types include PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, version 1 and 2).

Note Check your RADIUS vendor's documentation for the authentication protocol that your RADIUS vendor recommends and follow their indicated protocol type. The pod’s capability to support two-factor authentication with RADIUS is provided by the Unified Access Gateway instances, and Unified Access Gateway supports PAP, CHAP, MSCHAP1, and MSCHAP2. PAP is generally less secure than MSCHAP2. PAP is also a simpler protocol than MSCHAP2. As a result, even though most RADIUS vendors are compatible with the simpler PAP protocol, some RADIUS vendors are not as compatible with the more secure MSCHAP2.

Specify the Horizon Cloud Pod's Gateway Configuration

In this step of the wizard, specify the information required to deploy the pod with a gateway configured. Unified Access Gateway provides the gateway environment for a pod deployed into Microsoft Azure. When deploying the new pod, you can choose to have either an external or internal gateway configuration — or have both types on the same pod. By default, when this wizard step displays, the external gateway configuration is selected.

External gateway configuration

The external gateway configuration gives the ability to provide access to desktops and applications for end users located outside of your corporate network. When the pod has this external gateway configuration, the pod includes an Azure Load Balancer resource and Unified Access Gateway instances to provide this access. In this case, the instances have three NICs each: one NIC on the management subnet, one NIC on the desktop subnet, and one NIC on the DMZ subnet. In the deployment wizard, you have the option to specify the
load balancing type as either private or public, depending on whether you want a private IP or public IP address for the load balancer. If you switch off this public IP toggle in the wizard, then you must specify the IP address that you have mapped in your DNS server to the FQDN that your end users’ Horizon clients will use for PCoIP connections to the gateway.

For an external gateway configuration, you also have the option to deploy the configuration into a VNet that is separate from the pod’s VNet. The VNets must be peered. This type of configuration gives the ability to deploy the pod into more complex network topologies in Microsoft Azure, such as a hub-spoke network topology.

**Note** If you enabled the toggle for having the external gateway using its own subscription in the first wizard step, you must deploy the external gateway into its own VNet, the VNet that is associated with that subscription. If you enabled that toggle, you can optionally select an existing resource group in that subscription for the external gateway’s resources. You must have prepared that resource group in advance so that you can select it in this wizard step.

**Internal gateway configuration**

The internal gateway configuration gives the ability for end users located inside your corporate network to have trusted HTML Access (Blast) connections to their desktops and applications. If the pod is not configured with this internal gateway configuration, end users inside your corporate network see the standard browser untrusted certificate error when they use their browsers to make HTML Access (Blast) connections to their desktops and applications. When the pod has this internal gateway configuration, the pod includes an Azure Load Balancer resource and Unified Access Gateway instances to provide this access. In this case, the instances have two NICs each: one NIC on the management subnet and one NIC on the desktop subnet. By default, this gateway’s load balancing type is private.

The following screenshot is an example of the step when it is initially displayed. Some controls are displayed only when you selected at the first wizard step to use a different subscription for the external gateway configuration.
Add Microsoft Azure Capacity

| Gateway Settings |  
|------------------|---
| **External Gateway** |  
| Enable External Gateway? | OFF |
| FQDN:* |  
| DNS Addresses: |  
| Routes: |  
| VM Model:* | Standard_A4_v2 (4 CPUs, 8 GB RAM) |
| Certificate:* | Upload |
| Load Balancer |  
| Enable Public IP? | OFF |
| Networking |  
| Use a Different Virtual Network: | OFF |
| Virtual Network:* |  
| Use Existing Subnet: |  
| Management Subnet (CIDR):* |  
| Back End Subnet (CIDR): |  
| DMZ Subnet (CIDR):* |  
| 2 Factor Authentication Settings |  
| Enable 2 Factor Authentication? | OFF |
| Deployment |  
| Use Existing Resource Group? | OFF |
| Internal Gateway |  
| Enable Internal Gateway? | OFF |
Prerequisites

Verify that you have met the prerequisites described in Prerequisites for Running the Pod Deployment Wizard.

**Important** To complete this step, you must have the required fully qualified domain name (FQDN) which your end users will use to access the service and have a signed SSL certificate (in PEM format) based on that FQDN. The certificate must be signed by a trusted CA. A single PEM file must contain the entire certificate chain and the private key: SSL certificate intermediate certificates, root CA certificate, private key. For details, see Convert a Certificate File to the PEM Format Required for Pod Deployment.

Verify that all certificates in the certificate chain have valid time frames. If any certificate in the chain is expired, unexpected failures can occur later in the pod onboarding process.

This FQDN cannot contain underscores. In this release, connections to the Unified Access Gateway instances will fail when the FQDN contains underscores.

Procedure

1. If you want the external gateway configuration, complete the fields in the External Gateway section.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable External Gateway?</strong></td>
<td>Controls whether the pod has an external gateway configuration. The external configuration allows access to desktops and applications for users located outside of your corporate network. The pod includes a Microsoft Azure load balancer resource and Unified Access Gateway instances to provide this access. Note Leaving the default enabled setting is recommended. When this toggle is switched off, clients must either connect through Workspace ONE Access integrated with the pod or directly to the pod managers' load balancer, or they connect through an internal gateway configuration. In the case of clients connecting through Workspace ONE Access integrated with the pod or directly, some post-deployment steps are required. In this case, after the pod is deployed, follow the steps in Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs.</td>
</tr>
<tr>
<td><strong>FQDN</strong></td>
<td>Enter the required fully qualified domain name (FQDN), such as ourOrg.example.com, which your end users will use to access the service. You must own that domain name and have a certificate in PEM format that can validate that FQDN. <strong>Important</strong> This FQDN cannot contain underscores. In this release, connections to the Unified Access Gateway instances will fail when the FQDN contains underscores.</td>
</tr>
</tbody>
</table>
Option | Description
---|---
**DNS Addresses** | Optionally enter addresses for additional DNS servers that Unified Access Gateway can use for name resolution, separated by commas. When configuring this external Unified Access Gateway configuration to use two-factor authentication with your on-premises RADIUS server, you would specify the address of a DNS server that can resolve the name of your on-premises RADIUS server. As described in the Prerequisites for All Deployments, a DNS server must be set up internally in your subscription and configured to provide external name resolution. The Unified Access Gateway instances use that DNS server by default. If you specify addresses in this field, the deployed Unified Access Gateway instances use the addresses in addition to the prerequisite DNS server that you configured in your subscription's virtual network.

**Routes** | Optionally specify custom routes to additional gateways that you want the deployed Unified Access Gateway instances to use to resolve network routing for the end user access. The specified routes are used to allow Unified Access Gateway to resolve network routing such as to RADIUS servers for two-factor authentication. When configuring this pod to use two-factor authentication with an on-premises RADIUS server, you must enter the correct route the Unified Access Gateway instances can use to reach the RADIUS server. For example, if your on-premises RADIUS server uses 10.10.60.0/24 as its IP address, you would enter 10.10.60.0/24 and your default route gateway address as a custom route. You obtain your default route gateway address from the Express Route or VPN configuration you are using for this environment. Specify the custom routes as a comma-separated list in the form ipv4-network-address/bits ipv4-gateway-address, for example: 192.168.1.0/24 192.168.0.1, 192.168.2.0/24 192.168.0.2.

**VM Model** | Select a model to use for the Unified Access Gateway instances. You must ensure that the Microsoft Azure subscription you specified for this pod can provide the capacity for two VMs of the selected model.

**Certificate** | Upload the certificate in PEM format that Unified Access Gateway will use to allow clients to trust connections to the Unified Access Gateway instances running in Microsoft Azure. The certificate must be based on the FQDN you entered and be signed by a trusted CA. The PEM file must contain the entire certificate chain and the private key: SSL certificate intermediate certificates, root CA certificate, private key.

Specify the settings for this gateway's Microsoft Load Balancer.

Option | Description
---|---
**Enable Public IP?** | Controls whether this gateway’s load balancing type is configured as private or public. If switched on, the deployed Microsoft Azure load balancer resource is configured with a public IP address. If switched off, the Microsoft Azure load balancer resource is configured with a private IP address.

**Important** In this release, you cannot later change the external gateway’s load balancing type from public to private, or from private to public. The only way to make that change would be to delete the gateway configuration entirely from the deployed pod and then edit the pod to add it back with the opposite setting.

If you switch off this toggle, the field Public IP for Horizon FQDN appears.

**Public IP for Horizon FQDN** | When you have chosen not to configure the deployed Microsoft Azure load balancer with a public IP, you must provide the IP address that you are mapping in your DNS to the FQDN that your end users’ Horizon clients will use for PCoIP connections to the gateway. The deployer will configure this IP address in the Unified Access Gateway configuration settings.

Specify the external gateway’s networking settings.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a Different Virtual Network</td>
<td>This toggle controls whether the external gateway will be deployed into its own VNet, separate from the pod’s VNet. The following rows describe the different cases.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When you specified to use a different subscription for the external gateway in the first step of the wizard, this toggle is enabled by default. You must choose a VNet for the gateway in that situation.</td>
</tr>
<tr>
<td>Use a Different Virtual Network — Switched off</td>
<td>When the toggle is switched off, the external gateway will be deployed into the pod’s VNet. In this case, you must specify the DMZ subnet.</td>
</tr>
<tr>
<td>DMZ Subnet</td>
<td><strong>DMZ Subnet</strong> - When <strong>Use Existing Subnet</strong> is enabled in the Pod Setup wizard step, <strong>DMZ Subnet</strong> lists the subnets available on the VNet selected for <strong>Virtual Network</strong>. Select the existing subnet that you want to use for the pod’s DMZ subnet.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>Select an empty subnet, one that has no other resources attached to it. If the subnet is not empty, unexpected results might occur during the deployment process or pod operations.</td>
</tr>
<tr>
<td>DMZ Subnet (CIDR)</td>
<td><strong>DMZ Subnet (CIDR)</strong> - When <strong>Use Existing Subnet</strong> is switched off in the preceding wizard step, enter the subnet (in CIDR notation) for the DMZ (demilitarized zone) network that will be configured to connect the Unified Access Gateway instances to the gateway’s Microsoft Azure public load balancer.</td>
</tr>
<tr>
<td>Use a Different Virtual Network — Enabled</td>
<td>When the toggle is enabled, the external gateway will be deployed into its own VNet. In this case, you must select the VNet to use and then specify the three required subnets. Enable the <strong>Use Existing Subnet</strong> toggle to select from subnets that you have created in advance on the specified VNet. Otherwise, specify the subnets in CIDR notation.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>Select empty subnets, ones that have no other resources attached to them. If the subnets are not empty, unexpected results might occur during the deployment process or pod operations.</td>
</tr>
<tr>
<td></td>
<td>In this case, the gateway’s VNet and pod’s VNet are peered. The best practice is to have the subnets created in advance, and not use the CIDR entries here. See Prerequisites When Deploying With an External Unified Access Gateway Configuration Using its Own VNet or Subscription Separate from the Pod’s VNet or Subscription.</td>
</tr>
<tr>
<td></td>
<td><strong>Management subnet</strong> - Specify the subnet to use for the gateway’s management subnet. A CIDR of at least /27 is required. This subnet must have the Microsoft.SQL service configured as a service endpoint.</td>
</tr>
<tr>
<td></td>
<td><strong>Back-end subnet</strong> - Specify the subnet to use for the gateway’s back end subnet. A CIDR of at least /27 is required.</td>
</tr>
<tr>
<td></td>
<td><strong>Front-end subnet</strong> - Specify the subnet for the front-end subnet that will be configured to connect the Unified Access Gateway instances to the gateway’s Microsoft Azure public load balancer.</td>
</tr>
</tbody>
</table>

2. (Optional) In the **External Gateway** section, optionally configure two-factor authentication for the external gateway.

Complete the steps in **Specify Two-Factor Authentication Capability for the Pod**.
3  (Optional) In the **Deployment** section, use the toggle to optionally select an existing resource group into which you want the deployer to deploy the resources for the external gateway configuration.

This toggle displays when you have specified to use a different subscription for the external gateway in the first step of the wizard. When you enable the toggle, a field appears in which you can search for and select the resource group.

4  In the **Internal Gateway** section, if you want the internal gateway configuration, switch on the **Enable Internal Gateway?** toggle and complete the fields that appear.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Internal Gateway?</td>
<td>Controls whether the pod has an internal gateway configuration. The internal configuration provides trusted access to desktops and applications for HTML Access (Blast) connections for users located inside of your corporate network. The pod includes an Azure load balancer resource and Unified Access Gateway instances to provide this access. By default, this gateway’s load balancing type is private. The load balancer is configured with a private IP address.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Enter the required fully qualified domain name (FQDN), such as <code>ourOrg.example.com</code>, which your end users will use to access the service. You must own that domain name and have a certificate in PEM format that can validate that FQDN. If you specified an FQDN for the external gateway, you must enter the same FQDN here. <strong>Important</strong> This FQDN cannot contain underscores. In this release, connections to the Unified Access Gateway instances will fail when the FQDN contains underscores.</td>
</tr>
<tr>
<td>DNS Addresses</td>
<td>Optionally enter addresses for additional DNS servers that Unified Access Gateway can use for name resolution, separated by commas. When configuring this internal gateway configuration to use two-factor authentication with your on-premises RADIUS server, you would specify the address of a DNS server that can resolve the name of your on-premises RADIUS server. As described in the <strong>Prerequisites for All Deployments</strong>, a DNS server must be set up internally in your subscription and configured to provide name resolution. The Unified Access Gateway instances use that DNS server by default. If you specify addresses in this field, the deployed Unified Access Gateway instances use the addresses in addition to the prerequisite DNS server that you configured in your subscription’s virtual network.</td>
</tr>
<tr>
<td>Routes</td>
<td>Optionally specify custom routes to additional gateways that you want the deployed Unified Access Gateway instances to use to resolve network routing for the end user access. The specified routes are used to allow Unified Access Gateway instances to resolve network routing such as to RADIUS servers for two-factor authentication. When configuring this pod to use two-factor authentication with an on-premises RADIUS server, you must enter the correct route the Unified Access Gateway instances can use to reach the RADIUS server. For example, if your on-premises RADIUS server uses <code>10.10.60.20</code> as its IP address, you would enter <code>10.10.60.0/24</code> and your default route gateway address as a custom route. You obtain your default route gateway address from the Express Route or VPN configuration you are using for this environment. Specify the custom routes as a comma-separated list in the form <code>ipv4-network-address/bits ipv4-gateway-address</code>, for example: <code>192.168.1.0/24 192.168.0.1, 192.168.2.0/24 192.168.0.2</code>.</td>
</tr>
</tbody>
</table>
### VM Model
Select a model to use for the Unified Access Gateway instances. You must ensure that the Microsoft Azure subscription you specified for this pod can provide the capacity for two VMs of the selected model.

### Certificate
Upload the certificate in PEM format that Unified Access Gateway will use to allow clients to trust connections to the Unified Access Gateway instances running in Microsoft Azure. The certificate must be based on the FQDN you entered and be signed by a trusted CA. The PEM file must contain the entire certificate chain and the private key: SSL certificate, intermediate certificates, root CA certificate, private key.

5. (Optional) In the **Internal Gateway** section, optionally configure two-factor authentication for the internal Unified Access Gateway.

   Complete the steps in Specify Two-Factor Authentication Capability for the Pod.

6. (Optional) In the **Azure Resource Tags** section, optionally add custom tags to the resource groups that contain all the internal and external Unified Access Gateway instances that you have configured for the pod.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherit Pod Tags</td>
<td>Switch on this toggle to add the pod’s resource tags to the resource groups containing all the Unified Access Gateway instances that you have configured. Each resource group receives the resource tags that you defined in the Pod Setup wizard step. Switch off this toggle to define new resource tags for the Unified Access Gateway instances.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Azure Resource Tags| This setting becomes visible when you switch off the **Inherit Pod Tags** toggle. Use this setting to add new resource tags to the resource groups containing the Unified Access Gateway instances that you have configured. To create the first tag, enter information in the Name and Value fields. To create an additional tag, click + and then enter information in the Name and Value fields that appear below the existing ones.  
|                  | - You can create a maximum of 10 tags.  
|                  | - The tag name is limited to 512 characters, and the tag value is limited to 256 characters. For storage accounts, the tag name is limited to 128 characters, and the tag value is limited to 256 characters.  
|                  | - Tag names cannot contain the following characters:  
|                  |   `< > % & \ ? /`  
|                  | - Tag names cannot contain these case-insensitive strings:  
|                  |   ’azure’, ’windows’, ’microsoft’  
|                  | - Tag names and tag values can only contain ASCII characters. Blank spaces and characters outside the standard 128-character ASCII set (also known as high ASCII or extended ASCII characters) are not allowed. |

### Results
When you have provided the required information associated with your selected options, you can click **Validate & Proceed** to continue to the wizard’s final step. Complete the final steps in Deploying Horizon Cloud Pods into Microsoft Azure from the Capacity Page.
Specify Two-Factor Authentication Capability for the Pod

In the pod deployment wizard step for specifying its Unified Access Gateway configurations, you can also specify use of two-factor authentication for your end users' access to their desktops and applications through those gateway configurations. You can specify these two-factor authentication details after providing the Unified Access Gateway configuration details.

Prerequisites

For the external or internal Unified Access Gateway configuration for which you are entering the two-factor authentication details, verify that you have completed the fields for the Unified Access Gateway configuration in the wizard as described in Specify the Horizon Cloud Pod's Gateway Configuration. When configuring two-factor authentication to an on-premises authentication server, you also provide information in the following fields so that the Unified Access Gateway instances can resolve routing to that on-premises server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Addresses</td>
<td>Specify one or more addresses of DNS servers that can resolve the name of your on-premises authentication server.</td>
</tr>
<tr>
<td>Routes</td>
<td>Specify one or more custom routes that allow the pod's Unified Access Gateway instances to resolve network routing to your on-premises authentication server. For example, if you have an on-premises RADIUS server that uses 10.10.60.20 as its IP address, you would use 10.10.60.0/24 and your default route gateway address as a custom route. You obtain your default route gateway address from the Express Route or VPN configuration you are using for this environment. Specify the custom routes as a comma-separated list in the form ipv4-network-address/bits ipv4-gateway-address, for example: 192.168.1.0/24 192.168.0.1, 192.168.2.0/24 192.168.0.2.</td>
</tr>
</tbody>
</table>

Verify that you have the following information used in your authentication server's configuration, so that you can provide it in the appropriate fields in the pod deployment wizard. If you have both a primary and secondary server, obtain the information for each of them.

- IP address or DNS name of the authentication server
- The shared secret that is used for encryption and decryption in the authentication server's protocol messages
- Authentication port numbers, typically the 1812 UDP port.
- Authentication protocol type. The authentication types include PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, version 1 and 2).

**Note** Check your RADIUS vendor's documentation for the authentication protocol that your RADIUS vendor recommends and follow their indicated protocol type. The pod's capability to support two-factor authentication with RADIUS is provided by the Unified Access Gateway instances, and Unified Access Gateway supports PAP, CHAP, MSCHAP1, and MSCHAP2. PAP is generally less secure than MSCHAP2. PAP is also a simpler protocol than MSCHAP2. As a result, even though most RADIUS vendors are compatible with the simpler PAP protocol, some RADIUS vendors are not as compatible with the more secure MSCHAP2.
Procedure

1. Switch on the **Enable 2 Factor Authentication** toggle.

   When the toggle is enabled, the wizard displays the additional configuration fields. Use the scroll bar to access all of the fields.

   The following screenshot is an example of what is displayed after you switch on the toggle in the **External UAG** section.

2. Select your two-factor authentication method in the drop-down list.

   In this release, RADIUS authentication is supported.

3. In the **Name** field, enter an identifying name for this configuration.

4. In the **Properties** section, specify details related to the end users' interaction with the login screen they will use to authenticate for access.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>You can leave this field blank. Even though this field is visible in the wizard, it only sets an internal name in Unified Access Gateway. This name is not used by Horizon clients.</td>
</tr>
<tr>
<td>Display Hint</td>
<td>Optionally enter a text string that will be displayed to the end users in the message on the end-user client login screen when it prompts the user for their RADIUS user name and passcode. The specified hint appears to the end user as Enter your DisplayHint user name and passcode, where DisplayHint is the text you specify in this field. This hint can help guide users to enter the correct RADIUS passcode. As an example, specifying a phrase like Example Company user name and domain password below for would result in a prompt to the end user that says Enter your Example Company user name and domain password below for user name and passcode.</td>
</tr>
<tr>
<td>Name ID Suffix</td>
<td>This setting is used in SAML scenarios, where your pod is configured to use TrueSSO for single sign-on. Optionally provide a string which the system will append to the SAML assertion user name that is sent to the broker. For example, if the user name is entered as user1 on the login screen and a name ID suffix of @example.com was specified here, the system sends a SAML assertion user name of <a href="mailto:user1@example.com">user1@example.com</a> to the broker.</td>
</tr>
</tbody>
</table>
5 In the Primary Server section, specify details about the authentication server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name / IP Address</td>
<td>Enter the DNS name or the IP address of the authentication server.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the secret for communicating with the authentication server. The value must be identical to the server-configured value.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Specify the UDP port configured on the authentication server for sending or receiving authentication traffic. The default is 1812.</td>
</tr>
<tr>
<td>Accounting Port</td>
<td>Optionally specify the UDP port configured on the authentication server for sending or receiving accounting traffic. The default is 1813.</td>
</tr>
<tr>
<td>Mechanism</td>
<td>Select the authentication protocol that is supported by the specified authentication server and which you want the deployed pod to use.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>Specify the number of seconds that the pod should wait for a response from the authentication server. After this number of seconds, a retry is sent if the server does not respond.</td>
</tr>
<tr>
<td>Max Number of Retries</td>
<td>Specify the maximum number of times the pod should retry failed requests to the authentication server.</td>
</tr>
<tr>
<td>Realm Prefix</td>
<td>Optionally provide a string which the system will place at the beginning of the user name when the name is sent to the authentication server. The user account location is called the realm. For example, if the user name is entered as user1 on the login screen and a realm prefix of DOMAIN-A\ was specified here, the system sends DOMAIN-A\user1 to the authentication server. If you do not specify a realm prefix, only the entered user name is sent.</td>
</tr>
<tr>
<td>Realm Suffix</td>
<td>Optionally provide a string which the system will append to the user name when the name is sent to the authentication server. For example, if the user name is entered as user1 on the login screen and a realm suffix of @example.com was specified here, the system sends <a href="mailto:user1@example.com">user1@example.com</a> to the authentication server.</td>
</tr>
</tbody>
</table>

6 (Optional) In the Secondary Server section, optionally specify details about an auxiliary authentication server.

You can configure a secondary authentication server to provide for high availability. Enable the Auxiliary Server toggle and complete the fields as described in Step Primary Server section.
In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure

If you are using a peered VNet, a best practice is to create the required subnets in advance of deploying the pod, to ensure that you have accounted for the address spaces your subnets need in the VNet prior to running the deployment wizard. Even when your VNet is not peered, instead of having the pod deployment process create the required subnets, you can create them in advance on your VNet.

**Important** Starting with the September 2019 release's pod manifest version, both for pods newly deployed at that manifest version or later and for pods updated to that version or later versions, the pod's management subnet must also support network communication with the pod's Microsoft Azure Database for PostgreSQL service resource. Before deploying a new pod or upgrading an existing pod, the pod management subnet that you create must have the Microsoft.Sql service listed as a service endpoint. The deployment or update process will check if the subnet has the endpoint and not proceed if the endpoint is not enabled on the subnet. For details, see [When Using Existing Subnets for a Horizon Cloud Pod in Microsoft Azure](#).

When you create the subnets in advance, you must ensure their address ranges, in classless interdomain routing (CIDR) notation, adhere to the pod deployment wizard's minimum requirements:

- For the management subnet, a CIDR of /27 or more is required. This subnet is for IP addresses used by the VMs involved in management activities of the pod itself.
- For the primary VM subnet — also known as the desktop or tenant subnet — a CIDR of /27 or more is required. For production environments, a CIDR of /24 to /21 is recommended (256 addresses to 2048 addresses). This subnet is for IP addresses used for the RDSH server VMs and VDI desktop VMs on that subnet. The pod’s manager VM uses an IP address from this
subnet. If the pod will have an internal Unified Access Gateway configuration, those Unified Access Gateway VMs also use IP addresses from this subnet. If the pod will have an external gateway configuration that is deployed using the pod's VNet, that external gateway's Unified Access Gateway VMs also use IP addresses from this subnet.

**Important** The VMs for your VDI desktops, the RDS-capable images, and every RDSH VM in the pod's farms consume these IP addresses. Because this primary VM subnet cannot be extended after the pod is deployed, ensure you set this range large enough to accommodate the number of desktops you anticipate you might want this pod to provide. For example, if you anticipate this pod should provide over 1000 desktops in the future, ensure this range provides for more than that number of IP addresses. Starting in the July 2020 release, a new feature allows you to later edit the pod and add additional VM subnets for use by your farm VMs and VDI desktop VMs. That new feature gives you the flexibility to add VM subnets over time to accommodate growth in your farms and VDI desktop assignments. Because the system will default to using this primary VM subnet unless you expressly specify those additional subnets in the definitions of your farms and VDI desktop assignments, it is a best practice to ensure the range for this primary VM subnet to be large enough to accommodate your anticipated number of farm VMs and desktops.

- If you are going to have an external Unified Access Gateway configuration deployed into the pod's VNet, you need a DMZ subnet, with a CIDR of /28 or more. This subnet is for IP addresses used by the Unified Access Gateway VMs' NICs to communicate with this external gateway configuration's load balancer. If you want to keep the management and DMZ subnet ranges co-located, you could specify the DMZ subnet range similar to the management subnet with an IP specified. For example, if the management subnet is 192.168.8.0/27, a matching DMZ subnet would be 192.168.8.32/27.

- If you are going to have the external Unified Access Gateway configuration deployed into its own VNet, separate from the pod's, that VNet needs three subnets:
  - A management subnet, of a CIDR of /27 more is required. This subnet is for IP addresses used by the VMs involved in management activities of the external gateway overall, such as the gateway connector VM.
  - A back-end subnet, of a CIDR of /27 more is required. This subnet is for IP addresses used by the Unified Access Gateway VMs' NICs to communicate with the pod-provisioned farm and desktop VMs over the peered VNet with the pod's VNet.
A front-end (DMZ) subnet, of a CIDR of /28 or more. This subnet is for IP addresses used by the Unified Access Gateway VMs' NICs to communicate with the external gateway's load balancer. If you want to keep the management and front-end subnet ranges co-located in this VNet, you could specify the DMZ subnet range similar to the management subnet with an IP specified. For example, if the management subnet is 192.168.8.0/27, a matching front-end subnet would be 192.168.8.32/27.

**Important** For each CIDR, ensure that each combination of prefix and bit mask results in an IP address range having the prefix as the starting IP address. Microsoft Azure requires that the CIDR prefix be the start of the range. For example, a correct CIDR of 192.168.182.48/28 would result in an IP range of 192.168.182.48 to 192.168.182.63, and the prefix is the same as the starting IP address (192.168.182.48). However, an incorrect CIDR of 192.168.182.60/28 would result in an IP range of 192.168.182.48 to 192.168.182.63, where the starting IP address is not the same as the prefix of 192.168.182.60. Ensure that your CIDRs result in IP address ranges where the starting IP address matches the CIDR prefix.

**Prerequisites**

Ensure your Microsoft region has the VNet that you plan to use for your pod. For details about setting up the VNet, see the *Horizon Cloud Deployment Guide*.

Ensure the address ranges you plan to use for the subnets do not overlap. The pod deployment wizard will display an error if the subnet ranges overlap.

**Procedure**

1. In the Microsoft Azure portal, navigate to the VNet for which you need to create the described subnets.
2. Click **Subnets**.
3. Click **+ Subnet**.
   The *Add subnet* screen appears.
4. Provide the information for the required fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Specify a name for the subnet.</td>
</tr>
<tr>
<td><strong>Address range (CIDR block)</strong></td>
<td>Type a CIDR for the subnet.</td>
</tr>
</tbody>
</table>

5. If this subnet is going to be the management subnet, in the **Service endpoints** section, select the Microsoft.Sql service.
6. Click **OK**.
   - The subnet is added to the VNet.
7. Repeat steps 3 through 5 to add the remaining required subnets.
8 If you are going to deploy the external gateway in its own VNet, repeat the steps for that VNet's subnets.

Results

**Caution** The subnets you manually create on your VNet in advance for the pod deployment must remain empty. Do not reuse existing subnets that already have items that are using IP addresses on those subnets. If an IP address is already in use on the subnets, issues such as the pod failing to deploy and other downstream IP-conflict issues have a high likelihood of occurring. Do not put any resources on these subnets or otherwise use any of the IP addresses. This caution notice includes pods deployed from Horizon Cloud — do not reuse subnets on which you already have a deployed pod.

What to do next

For any management subnets you created, ensure the Microsoft.Sql service is enabled as a service endpoint. See [When Using Existing Subnets for a Horizon Cloud Pod in Microsoft Azure](#). This service must be enabled on the pod's management subnet, and if you are deploying the external gateway in its own VNet, the service must be enabled on that gateway's management subnet also.

**When Using Existing Subnets for a Horizon Cloud Pod in Microsoft Azure**

Starting with the September 2019 release, both for pods newly deployed using that release's manifest version or later versions, and for pods updated to that release's manifest version or later versions, a pod's management subnet must also support network communication with the Microsoft Azure Database for PostgreSQL service endpoint. Before deploying a new pod or upgrading an existing pod, the pod management subnet that you create must have the Microsoft.Sql service enabled as a service endpoint. The deployment or update process will check if the subnet has the endpoint and not proceed if the endpoint is not enabled on the management subnet. In addition to enabling that service endpoint, if you have firewall or network security group (NSG) rules on your management subnet, you must configure it to allow traffic for the Microsoft Azure Database for PostgreSQL service before deploying a new pod or upgrading an existing pod.

**Important** The December 2019 release debuted the feature to deploy the pod's external Unified Access Gateway configuration into its own VNet, separate from the pod's VNet. When using that feature, the management subnet in the external gateway's VNet must also adhere to this requirement to have the Microsoft.Sql service enabled as a service endpoint on that subnet.

The September 2019 release introduced use of the Microsoft Azure Database for PostgreSQL service as a required element of a Horizon Cloud pod in Microsoft Azure. As described in the Microsoft documentation, Microsoft Azure Database for PostgreSQL is a fully managed database-as-a-service offering. In a pod deployment or update, a Microsoft Azure Database for PostgreSQL server resource is deployed in the pod's resource group, using the Single Server type of deployment. The deployment and update processes also automatically add a VNet rule...
to the pod's VNet. This VNet rule restricts the Microsoft Azure Database for PostgreSQL server's traffic to the pod's management subnet. Communication between the pod and that Microsoft Azure Database for PostgreSQL server use the management subnet, which places some requirements on the pod's management subnet.

**On the Management Subnet, Enable the Microsoft.Sql Service as a Service Endpoint**

The VNet rule to restrict traffic for the deployed Microsoft Azure Database for PostgreSQL server to the management subnet requires the subnet to have the Microsoft.Sql service endpoint enabled. In the scenario where you have the pod deployer create the subnets, the deployer ensures the pod's management subnet has the Microsoft.Sql service endpoint enabled on the management subnet that it creates. However, when you create the management subnet yourself, you must ensure that management subnet meet these requirements before you deploy a new pod or update an existing pod. The following screenshot is an example to illustrate where you enable the Microsoft.Sql service as a service endpoint on a subnet using the Microsoft Azure portal. After clicking on the subnet in the portal, in the **Service endpoints** section, use the Services drop-down list to select Microsoft.Sql, and then save.
You can use the Microsoft Azure portal to navigate to the management subnet and select Microsoft.Sql in the Services drop-down.

**Ensure Your Firewalls or NSGs Allow for Pod Communication to the Microsoft Azure Database for PostgreSQL Service**

As listed in DNS Requirements for a Horizon Cloud Pod in Microsoft Azure, on the management subnet, you must configure your network rules for the management subnet to allow communication from the pod to the Microsoft Azure Database for PostgreSQL service. You must ensure your management subnets meets this requirement before you deploy a new pod or update an existing pod.

If your firewalls or NSGs support using service tags to specify access, allow pod communication with one of the following:

- Global Azure SQL service tag: Sql
- Region-specific SQL service tag for the Azure region where the pod is deployed: Sql.region, such as Sql.WestUS.

If your firewalls or NSGs do not support using service tags to specify access, you can use the host name of the database server resource that is created in the pod's resource group. The server resource's name follows the pattern *.postgres.database.azure.com.

For information about service tags in security groups, see the Microsoft Azure documentation topic at Service tags.

**Change a Cloud-Connected Pod's Associated Location, Name, and Description in Your Horizon Cloud Tenant Environment**

To change the geographic location, name, or description that the administrative console displays for one of your tenant's cloud-connected pods, use the Capacity page's Edit action.

The locations that the console displays are based on world city names. The system uses the cities' geographic coordinates to place icons representing your pods on the interactive map on the The Horizon Cloud Administration Console's Dashboard Page - Overview Tab for a Horizon Cloud Tenant. When you want to change a pod's associated geographic location to one that is not listed in the location-related drop-down list, you start typing the name of a city in the relevant entry field.

**Note** You must select a city from the system's autocomplete list. Currently, due to a known issue, the location names are not localized.

**Procedure**

1. In the console, navigate to the Capacity page by clicking **Settings > Capacity**.
2. Start the Edit Pod workflow by selecting the pod, and clicking **Edit**.
In the Edit Pod window, follow the guidance below depending on what type of cloud-connected pod you selected.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon pod</td>
<td>Use the fields and controls in the wizard’s Pod Setup step to make your updates. If you want to change the pod’s associated geographic location to one that is not listed in the Pod Location drop-down list, select New and click the drop-down list to get an entry box in which to start typing the location name you want. Click Next and then Save to save your changes to the system.</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>Use the fields and controls in the Pod Details step to make your updates and save your changes to the system. If you want to change the pod’s associated geographic location to one that is not listed in the Location drop-down list, click Edit, type the name of the location you want into the City Name field, and save it into the field.</td>
</tr>
</tbody>
</table>

Save your changes and exit out of the wizard, clicking Next as needed until you see the appropriate buttons to save and exit out of the wizard.

Removing Cloud-Connected Horizon Pods from Use with Horizon Cloud

The business reasons for cloud-connecting a Horizon pod to Horizon Cloud range from the simple use case of using a subscription license with that pod to leveraging all the cloud-hosted services that are supported for use with cloud-connected Horizon pods. If you no longer have a need for those use cases, you can remove, or disconnect, the cloud-connected pod from use with Horizon Cloud by using the Remove button on the console’s Capacity page. When disconnected from Horizon Cloud, that pod is no longer cloud-connected and you can no longer use a subscription license or use cloud-hosted services with that pod.

**Tip** In addition to the Remove action on the Capacity page, the pod’s details page has a Disconnect action that gives the same result.

Prerequisites

Remove the pod from any assignments in which that pod is involved. See Edit a Multi-Cloud Assignment in Your Horizon Cloud Tenant Environment.

If an on-premises Horizon pod is offline or unavailable when you complete these steps and the system completes its activities to disconnect the pod, the system cannot communicate with the pod's Connection Server to clear out the appropriate cloud-management-related properties in the Horizon global database. This property informs the Horizon Connection Server that the pod is in-use with Horizon Cloud. In this situation, after performing the steps here, you must also manually edit the Horizon global database to clear out the cloud-management-related properties.

Procedure

1. On the Capacity page, select the pod that you want to remove from use with Horizon Cloud.
2 Click **Remove**.

A notification message appears in the following cases:

- If the pod is included in one or more assignments, a message appears stating that you cannot disconnect the pod. You must first disassociate the pod from any assignments before trying to remove it.

- If the pod is offline or unavailable, a message alerts you that the pod will still retain its cloud-managed property in the Horizon global database after the disconnection process. You can specify whether to proceed with or cancel the process.

**Results**

If you proceed with the disconnection process, the pod is disconnected from Horizon Cloud, and the pod's name disappears from the pages in the administrative console.

**What to do next**

If you saw a notification message that the pod was offline or unavailable during the disconnection process, manually edit the Horizon global database to clear out the pod's cloud-managed properties. See **Clear the Cloud-Managed Properties from a Horizon Pod that was Offline During the Process to Disconnect it from Horizon Cloud**.

**Clear the Cloud-Managed Properties from a Horizon Pod that was Offline During the Process to Disconnect it from Horizon Cloud**

If you use the **Remove** or **Disconnect** button in the Horizon Cloud administrative console to remove a cloud-connected pod from use with Horizon Cloud, and the pod was offline or unavailable, you can still proceed to disconnect the pod from Horizon Cloud. In this case though, you must subsequently remove the pod's cloud-managed properties from the Horizon global database, because the system could not automatically remove those properties when Horizon Cloud could not communicate with the pod. If left in place, the cloud-managed properties prevent you from renaming the pod or removing it from a pod federation.

**Prerequisites**

Disconnect the on-premises pod from Horizon Cloud. See **Removing Cloud-Connected Horizon Pods from Use with Horizon Cloud**.

**Procedure**

1 Log in to the pod’s Connection Server with domain administrator privileges.

2 On the Connection Server, select **File > Windows Administrative Tools > ADSI Edit**.

3 Configure a connection to the Horizon global database.

   a In the console, right-click **ADSI Edit** and then click **Connect to**.

   b In the Name text box, enter **Horizon 7 Global Database**.
c Select **Select or type a Distinguished Name or Naming Context**. In the text box, enter the following name information:

```
dc=vdiglobal,dc=vmware,dc=int
```

d Select **Select or type a domain or server**. In the text box, enter the following server information:

```
localhost:22389
```

e Click **OK**.

The connection to the Horizon global database is established.

4 Expand the properties tree by navigating to **Horizon 7 Global LDAP Database [localhost:22389] > DC=vdiglobal,dc=vmware,dc=int**.

5 Clear the cloud-managed property from the pod.

a Under **DC=vdiglobal,dc=vmware,dc=int**, navigate to **OU=Properties** and then **OU=Pod**.

b Locate the target pod in the **OU=Pod** list, right-click it, and select **Properties**.

The pod appears in the list with its Horizon Administrator or Horizon Console name.

c Set the value of the **paе-CloudManaged** attribute to **0**.

Setting the value to 0 clears the cloud-managed property from the pod.

6 Clear the cloud-managed property from global entitlements.

a Under **DC=vdiglobal,dc=vmware,dc=int**, navigate to **OU=Entitlements**.

b Locate the global entitlement in the **OU=Entitlements** list. Right-click the global entitlement and select **Properties**.

The global entitlement appears in the list with its Horizon Administrator or Horizon Console name.

c Set the value of the **paе-CloudManaged** attribute to **0**.

Setting the value to 0 clears the cloud-managed property from the global entitlement.
Typical Administrative and Maintenance Tasks You Perform on the Horizon Cloud Connector After the Horizon Pod is Paired with Horizon Cloud

The Horizon Cloud Connector configuration portal gives you access to perform a number of administrative and maintenance tasks on the Horizon Cloud Connector virtual appliance after it is successfully paired with the Horizon pod's Connection Server and the pod is connected to Horizon Cloud. Some of these tasks are performed using the configuration portal while some tasks require accessing the virtual appliance's operating system and updating configuration files on the appliance.

These types of tasks include:

- Configuring a CA-signed certificate for the Horizon Cloud Connector virtual appliance. See the topic Configure a CA-Signed Certificate for the Horizon Cloud Connector Virtual Appliance.
- Setting a password expiry policy for the virtual appliance's root user. See the topic Set a Password Expiry Policy for the Horizon Cloud Connector Root User.
- Configuring settings that support automated updates to the virtual appliance. See the topic Automated Updates of the Horizon Cloud Connector Virtual Appliance.

**Note** Configuration of the virtual appliance for automated updates requires enablement of that feature in your Horizon Cloud customer account by the VMware Horizon Cloud Operations team. That feature is not enabled by default. To request use of that feature, open a service request or contact your VMware representative.

- Updating the static IP address of the virtual appliance. See the topic Update the Static IP for the Horizon Cloud Connector Virtual Appliance.
- Enabling and disabling SSH access to the virtual appliance. See Enable or Deactivate SSH on the Horizon Cloud Connector Appliance Using the Configuration Portal.
- Managing proxy settings and no-proxy hosts for the virtual appliance. See Modifying Proxy Settings for Horizon Cloud Connector 1.5 or Earlier.
- Synchronizing the virtual appliance's clock with an NTP server. See Synchronize the Horizon Cloud Connector Virtual Appliance with an NTP Server.
- Examining the health status of the Horizon Cloud Connector components.
If you want to reconfigure the Connection Server details for this same pod, in the configuration portal, click **Reconfigure** and follow the steps to complete the wizard.

**Important** If the credentials change for the Active Directory domain account that was used in the configuration portal when the Horizon Cloud Connector was paired with the pod, you must use the **Reconfigure** action to change the stored Active Directory domain account details.

If you want to remove the connection between this Connection Server instance and the control plane, click **Unplug**.

For those tasks that can be performed using the Horizon Cloud Connector configuration portal, you log in to the portal with My VMware credentials valid for your tenant environment and perform the tasks from there. Point your browser to one of the following:

- The Horizon Cloud Connector appliance's IP address, `https://IP-address/`
- If you created a forward and reverse lookup record in your DNS server that maps a fully-qualified domain name (FQDN) to the IP address, that FQDN

**Note** If your Horizon Cloud tenant environment has a registered Active Directory domain, the system requires you to log in with valid Active Directory domain credentials after the My VMware login.

This chapter includes the following topics:

- Configure a CA-Signed Certificate for the Horizon Cloud Connector Virtual Appliance
- Update the Static IP for the Horizon Cloud Connector Virtual Appliance
- Set a Password Expiry Policy for the Horizon Cloud Connector Root User
- Enable or Deactivate SSH on the Horizon Cloud Connector Appliance Using the Configuration Portal
- Modify DNS Settings for Horizon Cloud Connector
- Modifying Proxy Settings for Horizon Cloud Connector 1.6 or Later
- Modifying Proxy Settings for Horizon Cloud Connector 1.5 or Earlier
- Synchronize the Horizon Cloud Connector Virtual Appliance with an NTP Server
- Manually Activate Horizon Cloud Services for Horizon Cloud Connector 1.8 or Later
- Monitoring the Horizon Subscription License
- Manually Update the Horizon Cloud Connector Virtual Appliance
- Configure Automated Updates of the Horizon Cloud Connector Virtual Appliance
- Troubleshoot the Horizon Cloud Connector Virtual Appliance Update
- Collecting Log Files for Horizon Cloud Connector
- Horizon Cloud Connector Known Considerations
Configure a CA-Signed Certificate for the Horizon Cloud Connector Virtual Appliance

For enhanced security, you can configure a custom CA-signed certificate for the Horizon Cloud Connector virtual appliance.

Prerequisites

- Verify that the full certificate chain is available in the PEM format.
- Verify that the private key is available in the PEM format.
- Verify that the FQDN and Subject Alt Name is included in the issued certificate.

Procedure

1. Open an SSH session to your deployed Horizon Cloud Connector virtual appliance.
2. Copy the CA-signed certificate in the directory /root/server.crt.
3. Copy the CA-signed key in the directory /root/server.key.
4. Back up the existing certificate.
   - (Horizon Cloud Connector version 1.4 or later) Use the following command:
     ```bash
     cp /opt/container-data/certs/hze-nginx/server.crt /opt/container-data/certs/hze-nginx/server.crt.orig
     ```
   - (Horizon Cloud Connector version 1.3 or earlier) Use the following command:
     ```bash
     cp /etc/nginx/ssl/server.crt /etc/nginx/ssl/server.crt.orig
     ```
5. Back up the existing key.
   - (Horizon Cloud Connector version 1.4 or later) Use the following command:
     ```bash
     cp /opt/container-data/certs/hze-nginx/server.key /opt/container-data/certs/hze-nginx/server.key.orig
     ```
   - (Horizon Cloud Connector version 1.3 or earlier) Use the following command:
     ```bash
     cp /etc/nginx/ssl/server.key /etc/nginx/ssl/server.key.orig
     ```
6. Copy the existing nginx.conf file.
   - (Horizon Cloud Connector version 1.4 or later) Use the following command:
     ```bash
     cp /opt/container-data/conf/hze-nginx/nginx.conf /opt/container-data/conf/hze-nginx/nginx.conf.orig
     ```
   - (Horizon Cloud Connector version 1.3 or earlier) Use the following command:
     ```bash
     cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.orig
     ```
7 Copy the CA certificate in the appropriate directory for your virtual appliance version.
   - (Horizon Cloud Connector version 1.4 or later) Use the following command:
     ```bash
     cp /root/server.crt /opt/container-data/certs/hze-nginx/server.crt
     ```
   - (Horizon Cloud Connector version 1.3 or earlier) Use the following command:
     ```bash
     cp /root/server.crt /etc/nginx/ssl/server.crt
     ```

8 Copy the CA certificate key file in the appropriate directory for your virtual appliance version.
   - (Horizon Cloud Connector version 1.4 or later) Use the following command:
     ```bash
     cp /root/server.key /opt/container-data/certs/hze-nginx/server.key
     ```
   - (Horizon Cloud Connector version 1.3 or earlier) Use the following command:
     ```bash
     cp /root/server.key /etc/nginx/ssl/server.key
     ```

9 Verify the owner and permissions for the certificate and key file.
   - (Horizon Cloud Connector version 1.4 or later) Use the following commands:
     ```bash
     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 version 1.3 or earlier) Use the following commands:
     ```bash
     chown -R root:root /etc/nginx/ssl
     chmod -R 600 /etc/nginx/ssl
     ```

10 Verify that the issued FQDN in the certificate matches the server name directive in the server listen 443 block in the nginx configuration file.
   - (Horizon Cloud Connector version 1.4 or later) The nginx configuration file is located at `/opt/container-data/conf/hze-nginx/nginx.conf`.
   - (Horizon Cloud Connector version 1.3 or earlier) The nginx configuration file is located at `/etc/nginx/nginx.conf`.

11 Verify and restart nginx.
   - (Horizon Cloud Connector version 1.4 or later) Use the following commands:
     ```bash
     docker exec -i hze-nginx sudo nginx -t
     systemctl restart hze-nginx
     ```
   - (Horizon Cloud Connector version 1.3 or earlier) Use the following commands:
     ```bash
     nginx -t
     systemctl restart nginx
     ```
12 (Horizon Cloud Connector version 1.4 or later) Update the SSL thumbprints in the welcome screen.

Use the following commands:

```
docker exec -i hze-core sudo /opt/vmware/bin/configure-welcome-screen.py
/usr/bin/killall --quiet vami_login
```

13 Test the new certificate by reloading the Horizon Cloud Connector user interface URL in a Web browser.

14 (Optional) If the certificate works correctly, remove the backed-up files.

- (Horizon Cloud Connector version 1.4 or later) Use the following commands:

```
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 version 1.3 or earlier) use the following commands:

```
rm /etc/nginx/ssl/server.crt.orig
rm /etc/nginx/ssl/server.key.orig
rm /etc/nginx/nginx.conf.orig
```

15 Remove the copied CA certificates and key files in the root directory.

Use the following commands:

```
rm /root/server.crt
rm /root/server.key
```

**Update the Static IP for the Horizon Cloud Connector Virtual Appliance**

Information about the static IP for the Horizon Cloud Connector virtual appliance is saved in a container file in the deployed virtual appliance. If you update the static IP address for the Horizon Cloud Connector virtual appliance, you must also perform some additional steps. You must manually reconfigure the container settings file and then send the new static IP information to all desktops associated with the paired Horizon pod.

**Where the static IP is stored**

The static IP address of the deployed Horizon Cloud Connector virtual appliance is saved in the `~/opt/container-data/cc-settings/ip.conf` file and is shared with containers running inside the appliance.
For example, the static IP information might appear in the file as follows.

```
cc.address=10.117.163.20
```

**Where the proxy settings are stored**

The proxy settings of the Horizon Cloud Connector virtual appliance are stored in the `-/opt/container-data/cc-settings/proxy.conf` and are shared with containers running inside the appliance.

For example, the proxy information might appear in the file as follows.

```
proxyHost=null
proxyPort=0
proxySsl=false
proxyUsername=null
proxyPassword=
noProxyFor=null
```

**Prerequisites**

Configure a new static IP address for the Horizon Cloud Connector virtual appliance, and join the appliance to Active Directory.

**Procedure**

1. Edit the `cc.address` line in the `-/opt/container-data/cc-settings/ip.conf` file, as shown in the following example.

   ```
   cc.address=[new static IP address]
   ```

2. To send the new static IP address to all running Horizon desktops, run the following command.

   ```
docker exec csms /bin/bash -c "cd /usr/local/csms; ./scripts/address_changed.sh"
```

**Set a Password Expiry Policy for the Horizon Cloud Connector Root User**

When deploying the Horizon Cloud Connector OVA into your vSphere environment, the deployment process requires you to set the password for the root user. By default, this
password does not expire. However, based on the user's security policy, you might need to periodically update the root password by setting an expiry policy for the root user.

**Note** You must enter all commands as the root user after you log in to the Horizon Cloud Connector virtual appliance. If the user sets a custom password expiry policy, it is your responsibility as an administrator to periodically log in and update the password before it expires. The Horizon Cloud Connector virtual appliance does not notify administrators about password expiry.

**Procedure**

1. To set an expiry policy for the password for the root user, enter the following command:

   ```bash
   chage -M <Max days before password change> -W <Number of days of warning before password expires> root
   ```

   For example, if you want the password to expire after 365 days from the date of password change with a 30-day warning period before the password expires, enter the following command:

   ```bash
   chage -M 365 -W 30 root
   ```

2. To list the current password expiry policy of the root user, enter the following command:

   ```bash
   chage -l root
   ```

**Enable or Deactivate SSH on the Horizon Cloud Connector Appliance Using the Configuration Portal**

After the Horizon Cloud Connector appliance is successfully paired with a Horizon pod, you can use the browser-based Horizon Cloud Connector configuration portal's **Enable SSH on Cloud Connector** toggle to activate or deactivate the SSH setting on the appliance. Starting with version 1.5 of the appliance, SSH is turned off in the appliance's operating system by default. These steps apply to Horizon Cloud Connector version 1.5 or later.

**Prerequisites**

Verify that the following items are in place.

- The appliance is successfully paired with the Horizon pod. The configuration portal screen with the toggle is accessible only when the Horizon Cloud Connector appliance is successfully paired with the Horizon pod. Prior to pairing the connector with the pod, you can use your vSphere environment to launch the appliance console and log in to use the command line to activate or deactivate SSH on the appliance. See the topic **Enable SSH Access to the Horizon Cloud Connector Prior to Pairing it with Horizon Connection Server**.
You have the My VMware credentials that have administrator access to your Horizon Cloud tenant environment. Those credentials are needed to log in to the Horizon Cloud Connector configuration portal.

If your Active Directory domain is registered with your Horizon Cloud tenant environment, you need the credentials of an Active Directory account that is in a group with the Horizon Cloud Super Administrator role. When an Active Directory domain is registered with your Horizon Cloud tenant, a second login screen appears after you enter the My VMware credentials and you must subsequently enter Active Directory account credentials to access the configuration portal. For details about how your Active Directory domain gets registered with your Horizon Cloud tenant and the Super Administrators role, see Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment and Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment.

You have the URL address to display the configuration portal in your browser. To display the configuration portal's login screen, point your browser to one of the following:

- The Horizon Cloud Connector appliance's IP address, https://IP-address/
- If you created a forward and reverse lookup record in your DNS server that maps a fully-qualified domain name (FQDN) to the IP address, that FQDN

Procedure

1. In your browser, load the Horizon Cloud Connector configuration portal's URL and log in with My VMware credentials valid for your tenant environment, as described in the prerequisites. When your Active Directory domain is registered with that tenant environment, the system displays a second login screen. Enter the credentials for an Active Directory account that has the Super Administrators role, as described in the prerequisites.

   The configuration portal opens to the screen that displays the action buttons for administrative tasks on the connector.

2. Use the Enable SSH on Cloud Connector toggle to activate or deactivate SSH on the Horizon Cloud Connector appliance.

   The setting of the toggle that you see displayed in the portal is the current status of SSH in the appliance.

Modify DNS Settings for Horizon Cloud Connector

If the configuration of your DNS server changes, you must modify the network setup of the Horizon Cloud Connector appliance to include the updated DNS server.

For more information about modifying DNS settings on appliances such as Horizon Cloud Connector that run on the Photon OS, see the Adding a DNS Server document.
Procedure

◆ If you deployed Horizon Cloud Connector using a static IP address:
  a. On the appliance, open the /etc/systemd/network/10-eth0.network file for editing.
  b. Under the Network section of the file, add the new DNS server as an entry.
  c. Restart the appliance.

◆ If you deployed Horizon Cloud Connector using a dynamic IP address:
  a. On the appliance, open the /etc/resolv.conf file for editing.
  b. Add the new DNS server as an entry in the file.
  c. Restart the appliance.

Modifying Proxy Settings for Horizon Cloud Connector 1.6 or Later

You can configure HTTP proxy settings during deployment of the Horizon Cloud Connector OVF template. If you want to modify these proxy settings after deployment, you must use the configure-webproxy.py command. The configure-webproxy.py command is located in the /opt/vmware/bin directory of the deployed Horizon Cloud Connector appliance.

**Note** Observe the following guidelines with respect to proxy settings and appliance updates:

- If you manually update Horizon Cloud Connector 1.6 or later to a newer version, you must reconfigure your proxy settings. Your original proxy configuration does not carry over with the manual appliance update.

- If Horizon Cloud Connector 1.6 or later is automatically updated to a newer version, your proxy settings carry over with the automatic update. You do not need to reconfigure the proxy settings.

- To view the existing proxy settings for the Horizon Cloud Connector virtual appliance, run the following command.

  ```
  cat /opt/container-data/cc-settings/proxy.conf
  ```

**Syntax for Using configure-webproxy.py**

Use the following syntax to create a script with configure-webproxy.py:

```python
configure-webproxy.py [argument1 [value1]] [argument2 [value2]] ...
```

To display the command usage and list of available arguments, run configure-webproxy.py -h or configure-webproxy.py --help.
Arguments for configure-webproxy.py

All arguments are optional for the configure-webproxy.py script.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--proxyHost</td>
<td>Host name or IP address of the HTTP proxy server</td>
</tr>
<tr>
<td>--proxyPort</td>
<td>Port number for the proxy connection</td>
</tr>
<tr>
<td>--noProxyFor</td>
<td>Hosts or network range configured to bypass the HTTP proxy. Use spaces to separate multiple values.</td>
</tr>
<tr>
<td>--proxySsl</td>
<td>Specifies whether to use SSL for the proxy connection. Allowed values are true or false.</td>
</tr>
<tr>
<td>--proxyUsername</td>
<td>User name for the HTTP proxy</td>
</tr>
<tr>
<td>--proxyPassword</td>
<td>Password for the HTTP proxy</td>
</tr>
<tr>
<td>--implicitNonProxyHosts</td>
<td>Specifies whether to add the paired pod's Connection Server and vCenter Server implicitly to the list of hosts that bypass the HTTP proxy. Allowed values are true or false. The default is true. If your environment requires internal requests to the Connection Server and vCenter Server to route through the proxy, set this argument to false. In this case, only the hosts specified explicitly by --noProxyFor bypass the proxy.</td>
</tr>
</tbody>
</table>

Example Script

```
configure-webproxy.py --proxyHost PROXYEXAMPLE --proxyPort 80 --proxySsl=false
--noProxyFor ".AD-DOMAIN.EXAMPLE.COM 10.109.*"
```

This example script configures the following proxy settings:

- PROXYEXAMPLE is the proxy server.
- The proxy connection uses port 80.
- The proxy connection does not use SSL.
- Hosts that fall under .AD-DOMAIN.EXAMPLE.COM and 10.109.* bypass the proxy.
- Also, the paired pod's Connection Server and vCenter Server implicitly bypass the proxy by default.

Modifying Proxy Settings for Horizon Cloud Connector 1.5 or Earlier

You can configure HTTP proxy settings during deployment of the Horizon Cloud Connector OVF template. If you want to change the proxy settings after deployment or configure no-proxy hosts, you must modify certain configuration files. Due to a known limitation, Horizon Cloud Connector 1.5 or earlier does not honor the no-proxy host configuration specified during
deployment. To configure no-proxy hosts, you must modify a certain configuration file after deployment.

**Important** Due to a known limitation, if you plan to use Universal Broker with Horizon Cloud Connector 1.5, and your environment requires using proxy settings, you must configure those proxy settings when you deploy the OVF template. Universal Broker does not recognize any proxy settings configured after deployment. Since you can only configure no-proxy hosts after deployment, this limitation means that the use of no-proxy hosts with Universal Broker is not supported by Horizon Cloud Connector 1.5.

### Configuring No-Proxy Hosts for Horizon Cloud Connector 1.5 or Earlier

During deployment of the Horizon Cloud Connector OVF template, the deployment wizard provides prompts for configuring no-proxy hosts. However, due to a known issue, Horizon Cloud Connector 1.5 or earlier does not honor the no-proxy host configuration specified during deployment. Instead, you must modify a certain configuration file after deployment to set up no-proxy hosts.

To ensure that only outbound requests to the Internet route through the HTTP proxy, configure no-proxy hosts that bypass the proxy server when receiving internal requests from the appliance. At the minimum, configure the Connection Server and vCenter Server instances of the paired pod to be no-proxy hosts.

**Note** If you update Horizon Cloud Connector 1.5 or earlier to a newer version, you must reconfigure your no-proxy hosts. Your original no-proxy host configuration does not carry over with the appliance update.

For detailed information about configuring no-proxy hosts after deployment of the virtual appliance, see VMware Knowledge Base (KB) article 76663: Proxy Configuration issues and remediation for Horizon Cloud Connector.

### Modifying the Proxy Settings for Horizon Cloud Connector 1.5 or 1.4

Use the following steps to modify HTTP proxy settings for Horizon Cloud Connector 1.5 or 1.4 after deploying the appliance.

1. Open a Secure Shell (SSH) session to your deployed Horizon Cloud Connector virtual appliance.

2. Change the proxy details as needed in the following files:
   - `/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  Restart the necessary services.

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

Modifying the Proxy Settings for Horizon Cloud Connector 1.3 or Earlier

Use the following steps to modify HTTP proxy settings for Horizon Cloud Connector 1.3 or earlier after deploying the appliance.

1  Open a Secure Shell (SSH) session to your deployed Horizon Cloud Connector virtual appliance.

2  Change the proxy details as needed in the following files:
   - `/opt/vmware/var/lib/tomcat8/properties/hydra.properties`
   - `/opt/vmware/var/lib/tomcat8/properties/sn.config`

3  Restart the necessary services.

```
systemctl restart tomcat8
ersystemctl restart cccService
```

Synchronize the Horizon Cloud Connector Virtual Appliance with an NTP Server

To ensure that the Horizon Cloud Connector virtual appliance authenticates correctly with Horizon Cloud and the required Connection Server instances, you must synchronize the virtual appliance's clock with a Network Time Protocol (NTP) server. Synchronize the clock on the Horizon Cloud Connector virtual appliance with the clock on the physical ESXi host on which the virtual appliance resides, after first ensuring that the host itself is properly synchronized with an NTP server.
Procedure

◆ (Preferred method) Synchronize the Horizon Cloud Connector virtual appliance with the physical ESXi host on which the virtual appliance resides.

a. Verify that the ESXi host’s clock is properly synchronized with an NTP server.
   For more information, see the VMware vSphere Documentation.

b. Use vSphere Client to open the Edit Settings window of the Horizon Cloud Connector virtual appliance and enable the Synchronize Time with Host option.
   For detailed instructions, see the VMware vSphere Documentation.

   **Note** In Horizon Cloud Connector 1.5 and later, Synchronize Time with Host is enabled by default.

◆ (Alternative method) If you are unable to synchronize the Horizon Cloud Connector virtual appliance with the physical ESXi host, you can synchronize the virtual appliance directly with an NTP server.

   **Note** The preferred method of time synchronization is to synchronize the virtual appliance with the physical ESXi host. Use the following steps only if you are unable to perform the preferred method.

a. Open an SSH connection to the Horizon Cloud Connector virtual appliance, and log in as the root user.

b. Using a text editor such as vi, open the timesyncd.conf file for editing.

   ```bash
   vi /etc/systemd/timesyncd.conf
   ```

c. Edit the [Time] section so that it resembles the following example. Replace ntpAddress with the domain name of the NTP server that you want to use.

   ```
   [Time]
   #FallbackNTP=time1.google.com time2.google.com time3.google.com time4.google.com
   NTP=ntpAddress
   ```

   Save your changes to the timesyncd.conf file and exit the text editor.

d. Restart the virtual appliance’s network service.

   ```bash
   systemctl restart systemd-networkd
   ```

e. Restart the virtual appliance’s timesync service.

   ```bash
   systemctl restart systemd-timesyncd
   ```

f. Verify that the clock on the virtual appliance is now synchronized with the specified NTP server.
Manually Activate Horizon Cloud Services for Horizon Cloud Connector 1.8 or Later

If you deployed Horizon Cloud Connector 1.8 or later and selected the Basic Feature profile in the deployment wizard, only the Horizon subscription license service is activated. If you want to activate additional Horizon Cloud Services for your cloud-connected Horizon pod, you can do so by running commands in a Secure Shell session on the Horizon Cloud Connector appliance.

You can optionally activate one or more of the following cloud-hosted services:

Cloud Monitoring Service

The Cloud Monitoring Service (CMS) allows you to monitor capacity, usage, and health within and across your fleet of cloud-connected pods. To activate the CMS, you must first activate the Connection Server Monitoring Service which supports the CMS capabilities for a particular Horizon pod.

For more information about the CMS, see Chapter 3 Introducing the Cloud Monitoring Service’s Unified Visibility, Health Monitoring, and Help Desk Features Provided in Horizon Cloud.

Cloud Broker Client Service

The Cloud Broker Client Service supports the use of Universal Broker with your Horizon pod. You must activate the Cloud Broker Client Service if you want to use Universal Broker and configure multi-cloud assignments based on resources in your Horizon pod.

For more information about Universal Broker and multi-cloud assignments, see the subtopics under Chapter 6 Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment.

Image Locality Service

The Image Locality Service supports the use of the Horizon Image Management Service with your Horizon pod. You must activate the Image Locality Service if you want to use the Horizon Image Management Service to track and manage system images from your Horizon pod.
For more information about the Horizon Image Management Service, see the topics under Managing Horizon Images from the Cloud.

**Important** Observe the following guidelines:

- Do not perform these activation steps if you deployed Horizon Cloud Connector 1.7 or earlier, or if you deployed version 1.8 or later of the appliance with the **Full Feature** profile. In either of these cases, all supported Horizon Cloud services are already activated and running.

- Use these steps only to activate services if you selected the **Basic Feature** profile during the appliance deployment.

- Once you have activated a service, do not attempt to deactivate it manually. Deactivating a service can produce unexpected results.

**Procedure**

1. Navigate to the deployed Horizon Cloud Connector appliance in your pod's vSphere environment and configure the resource capacity required by the additional service or services that you want to activate.

<table>
<thead>
<tr>
<th>Additional Service to Activate</th>
<th>Minimum Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Server Monitoring Service</td>
<td>Total of 7 vCPUs, 8 GB memory (RAM), 40 GB datastore</td>
</tr>
<tr>
<td>Cloud Broker Client Service</td>
<td>Total of 6 vCPUs, 8 GB memory (RAM), 40 GB datastore</td>
</tr>
<tr>
<td>Image Locality Service</td>
<td>Total of 6 vCPUs, 7.5 GB memory (RAM), 40 GB datastore</td>
</tr>
<tr>
<td>Two or more of the above services</td>
<td>Total of 8 vCPUs, 8 GB memory (RAM), 40 GB datastore</td>
</tr>
</tbody>
</table>

2. Activate and start each service that you want to use.

   a. Open a Secure Shell (SSH) session on the Horizon Cloud Connector appliance, and log in as the root user.

   b. Run the commands corresponding to each service that you want to activate.

<table>
<thead>
<tr>
<th>Service</th>
<th>Command</th>
</tr>
</thead>
</table>
   | Connection Server Monitoring Service (required for the Cloud Monitoring Service) | systemctl enable csms  
   systemctl restart csms |
   | Cloud Broker Client Service | systemctl enable cbcs  
systemctl restart cbcs |
   | Image Locality Service | systemctl enable ils  
systemctl restart ils |

3. If you activated the Connection Server Monitoring Service, go to **Settings > General Settings** and verify that the **Cloud Monitoring Service** toggle is switched on.
Monitoring the Horizon Subscription License

Horizon subscription licenses rely on an operational communication chain between the Horizon pod deployment, Horizon Cloud Connector, and the Horizon Cloud license service. The license service syncs with the Horizon pod every 24 hours. You can use the Horizon Cloud Administration Console to monitor the status of your subscription licenses and troubleshoot any sync problems that might arise.

If one of the links in the license communication chain becomes nonoperational, the license sync fails and the Horizon pod enters a sync grace period of 25 days. During this period, the subscription license remains valid and the pod stays operational to allow time for you to investigate and remediate the cause of the sync failure. If the failure persists until the end of the sync grace period, services to the pod are disrupted and the pod becomes nonoperational. End users will not be able to connect to remote desktops and applications on the pod when the sync grace period expires.

To notify you in the event of a sync failure, alert messages appear in several different areas of the console, as described in the following sections.

Subscription License Status on the Dashboard Page

The Dashboard page reports sync errors for subscription licenses, as follows:

- The interactive Global Footprint map indicates that a pod is experiencing license sync failures when you hover over the pod icon on the map.
- The Issues tab lists any errors associated with a subscription license sync. Click the Read more link in the issue item to go directly to VMware Knowledge Base (KB) article 79509. This KB article provides detailed guidelines on troubleshooting common errors that can cause the license sync to fail.

The following screenshot shows an example of the Dashboard page reporting the status of a license sync failure.
Subscription License Health Status on the Capacity Page

You can view the status of a pod's subscription license on the pod's details page under **Settings > Capacity**.

1. On the pod's details page, view the health status of the Horizon subscription license under **Health > Other Components**. The following example shows the health status for a license that is experiencing sync problems.

![Other Components](image)

2. To view more details about a license sync failure, click the health status text. The console jumps to the Audit Logs page for the pod, with a filter automatically set to display the logs for license sync events over the past 30 days. The logs report the number of days that the license has been unavailable and the probable cause of the sync failure.

   The following example shows the log reports for a license that has failed to sync due to the offline condition of the Horizon pod.

![Audit Logs](image)

3. Perform the necessary actions to resolve the error causing the license sync to fail.

   For detailed guidelines on troubleshooting common errors, see **VMware Knowledge Base (KB) article 79509**.
Subscription License Alert Banner

After the first four days of the sync grace period have elapsed, an alert banner is displayed prominently at the top of the console window. As stated in the banner, you must resolve the license sync error before the sync grace period expires to avoid a service disruption.

The alert banner is color-coded according to the urgency level of the time remaining in the sync grace period.

<table>
<thead>
<tr>
<th>Alert Banner Color</th>
<th>Time Remaining in Sync Grace Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>21 to 15 days</td>
</tr>
<tr>
<td>Orange</td>
<td>14 to 8 days</td>
</tr>
<tr>
<td>Red</td>
<td>7 to 1 day(s) <strong>When the sync grace period expires, the red banner displays a message stating that there are 0 days left and services are now disrupted.</strong></td>
</tr>
</tbody>
</table>

The following screenshot shows an example of how the alert banner appears for a license sync failure with a remaining sync grace period of 21 days.

You can perform the following actions from the alert banner:

- If more than one pod is experiencing subscription license sync failures, scroll buttons appear at the left edge of the alert banner, as shown in the following example screenshot. Click the scroll buttons to view the alerts for all affected licenses.

- Click the **View** button in the banner to jump directly to the details page for the affected pod. If more than one pod is affected with the same sync grace period, the **View** button becomes a drop-down menu allowing you to select a pod. For information on the reports and actions available to you on the pod’s details page, see the preceding section in this topic.

Manually Update the Horizon Cloud Connector Virtual Appliance

To obtain the latest Horizon Cloud features for your cloud-connected Horizon pods, update those pods’ Horizon Cloud Connector virtual appliance to the latest version applicable to Horizon Cloud.

This documentation topic describes the steps to manually update the virtual appliance within the vSphere environment in which it is deployed. If your Horizon Cloud tenant account is configured for automated updates of the Horizon Cloud Connector, the appliance is automatically updated from the cloud plane when the VMware Operations team makes a new version available to your tenant account. For details, see Configure Automated Updates of the Horizon Cloud Connector Virtual Appliance.
An existing version can be updated to one or two later versions. That is, version ‘n’ can be updated to either ‘n+1’ or ‘n+2’.

**Note** Proxy SSL configuration is not supported during an update of the Horizon Cloud Connector virtual appliance.

**Prerequisites**

- Download the most recent version of the Horizon Cloud Connector virtual appliance that is supported for the current Horizon Cloud release. For the version supported for this Horizon Cloud release, see the Release Notes at the Horizon Cloud documentation page.

- Verify that the new Horizon Cloud Connector virtual appliance and the existing Horizon Cloud Connector virtual appliance that needs the update are in the same network so that the new virtual appliance can establish an SSH communication with the existing virtual appliance.

- Verify that the virtual appliance is powered on. It would be unusual if the appliance was powered off, because the Horizon Cloud Connector must maintain a connection with the cloud control plane to ensure that your Horizon subscription license remains active for the cloud-connected pod.

- (Horizon pods on premises or in VMware Cloud on AWS) Use vSphere Web Client to take a snapshot of the existing Horizon Cloud Connector virtual appliance.

- (Horizon pods in Azure VMware Solution) Use one of the following methods to take a snapshot of the existing Horizon Cloud Connector virtual appliance.

  - For instructions on how to use the Azure portal or PowerShell to take a snapshot of the appliance, see [https://docs.microsoft.com/en-us/azure/virtual-machines/windows/snapshot-copy-managed-disk](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/snapshot-copy-managed-disk).


- Obtain the static IP address, DNS address, gateway address, and subnet mask for the Horizon Cloud Connector virtual appliance.

- Verify that you have the My VMware account credentials that are valid to log in to your Horizon Cloud tenant account. As described in the onboarding information in the Deployment Guide, you use a My VMware account to log in to the Horizon Cloud Connector onboarding and management portal. If the pod's associated Active Directory domain is already registered in your Horizon Cloud tenant to which the connector is paired, a second login screen will appear after you log in with your My VMware credentials. This second login screen requests the Active Directory credentials of an administrator that has the Super Administrators role in your Horizon Cloud tenant environment. If you see that second login screen, you will need the credentials for an Active Directory account in that domain that has access permissions. For a description of this login process, see Log In to the Horizon Cloud Administration Console to Perform Management Tasks on Your Horizon Cloud Environment.
(Horizon pods on premises or in VMware Cloud on AWS) Add the FQDN of the vCenter Server to the /etc/hosts file on the Horizon Cloud Connector virtual appliance. This FQDN is needed for these manual update steps to work.

After editing the /etc/hosts file, you must restart the hze-core and csms services. Use the following commands:

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

**Important** Version 1.0 of the connector appliance is no longer supported. If you are updating from version 1.0, you must log in to the appliance's operating system and run the `chage -E -1 -M -1 tomcat8` command in the Horizon Cloud Connector virtual appliance after you have taken its snapshot.

```
root@example.com [ ~ ]# chage -E -1 -M -1 tomcat8
```

This command is required only when updating from Horizon Cloud Connector version 1.0, and not for updating from later versions.

**Procedure**

1. In a Web browser, to log in to the Horizon Cloud Connector onboarding and management portal, enter either the Horizon Cloud Connector virtual appliance IP address or, if you mapped that IP to an FQDN in your DNS, enter that FQDN in the browser.

   Use your My VMware account credentials to log in. This step logs you in to your Horizon Cloud tenant account, as described in the onboarding process in the Deployment Guide. A successful login verifies that the existing Horizon Cloud connection was successfully configured with the cloud-connected pod's Connection Server. If your Horizon Cloud tenant has a registered Active Directory domain, a second login screen will appear. If that happens, enter the appropriate Active Directory credentials, as described in Log In to the Horizon Cloud Administration Console to Perform Management Tasks on Your Horizon Cloud Environment.

2. Deploy the latest version of the Horizon Cloud Connector virtual appliance as described in steps 1 through 8 of Connect Horizon Cloud Service with an Existing Horizon Pod to Use Horizon Subscription Licenses or Cloud-Hosted Services or Both.

   **Note** If the previous instance of the Horizon Cloud Connector virtual appliance used an HTTP proxy, reconfigure the proxy settings by following the prompts in the deployment wizard. Proxy settings are not transferred from the previous virtual appliance to the new virtual appliance during a manual update.
3 Log in to the onboarding portal for the Horizon Cloud Connector appliance that you just deployed in step 2 using its IP address in your browser.

Log in with your My VMware credentials as described in step 1 above. If your Horizon Cloud tenant account has a registered Active Directory domain, the Active Directory login window appears and you must log in with the appropriate Active Directory credentials.

4 Connect the latest version of the Horizon Cloud Connector appliance that you just deployed with the appropriate Connection Server instance.

The previous version of the Horizon Cloud Connector is connected to the cloud-connected pod’s Connection Server instance. In the Connect to Horizon Connection Server box, enter the FQDN of the Connection Server, and click Connect.

5 If the display requests verification of the thumbprint certificate, click the check box to verify the thumbprint certificate for the Connection Server.

**Note**  This verification is skipped if the Connection Server has a valid Root CA certificate.

6 Enter the domain name, user name, and password for the Connection Server and click Connect.

**Note**  For better auditing of Horizon Cloud Connector actions, use a unique user name and password for the Connection Server.

7 When updating to Horizon Cloud Connector version 1.5, enable the Enable SSH on Cloud Connector toggle.

Enabling SSH provides for the new connector appliance to communicate over SSH with the existing one for the update process. When the update is complete, you can switch off this toggle.

8 Click Upgrade in the dialog box.

9 In the Old Cloud Connector address text box, enter the IP address of the earlier Horizon Cloud Connector virtual appliance and then click Connect.

10 Click the check box to verify the thumbprint for the SSH connection.

11 Click Upgrade.

The new Horizon Cloud Connector is now managing the cloud connection between the Horizon pod and Horizon Cloud.

**What to do next**

If the previous instance of the Horizon Cloud Connector virtual appliance used custom CA-signed certificates, configure a new CA-signed certificate for the updated virtual appliance. Certificates are not transferred from the previous virtual appliance to the new virtual appliance during a manual update. For more information, see Configure a CA-Signed Certificate for the Horizon Cloud Connector Virtual Appliance.
Remove the old version of the appliance from your pod's environment.

For future updates, if you want to enable automated updates of the Horizon Cloud Connector virtual appliance, instead of using these manual steps, see the information in Configure Automated Updates of the Horizon Cloud Connector Virtual Appliance.

Configure Automated Updates of the Horizon Cloud Connector Virtual Appliance

You can have your pod configured to perform an automated update of the Horizon Cloud Connector virtual appliance. This configuration allows the Horizon Cloud operations team to run maintenance actions on the virtual appliance from the cloud control plane, as needed for successful service operations.

**Note** The following limitations apply to automated updates:

- To participate in automated updates, your existing Horizon Cloud Connector appliance must be running with a minimum version of 1.5.0.0.
- The automated update feature is not supported for Horizon pods deployed in the Azure VMware Solution (AVS) environment. To update your Horizon pod in AVS, see Manually Update the Horizon Cloud Connector Virtual Appliance.

**Attention** The ability to configure the automated update feature is deactivated by default for Horizon Cloud Connector 1.6 or earlier and will only be available to you if your Horizon Cloud tenant account is configured to allow it. To gain access to the automated update feature, you must specifically request it by contacting your VMware representative or VMware support to activate it on your tenant account.

Requirements for Automated Updates

To support automated updates of the Horizon Cloud Connector appliance that is paired with a pod, prepare your system environment by performing the following tasks:

1. Contact your VMware representative or VMware support to activate the automated update feature for your Horizon Cloud tenant account.

2. Enable the pod to accept automated updates.

   By default, the automated updates are not sent to your pods, even if the feature is activated in your tenant account. To enable a pod to receive automated updates, contact your VMware representative or VMware support. You must make a specific request for each pod that you want to receive automated updates.

3. Verify that your system environment meets the following requirements:

   - Existing Horizon Cloud Connector appliance is deployed with a static IP address.
Existing Horizon Cloud Connector appliance is running with a minimum version of 1.5.0.0.

**Important** To activate automated updates for Horizon Cloud Connector 1.5 if your tenant account is located in any regional control plane instance besides USA, you must restart the hze-core service using the command `systemctl restart hze-core`. If you do not start the hze-core service, automated updates will fail. For more information about troubleshooting automated updates for Horizon Cloud Connector 1.5, see VMware Knowledge Base (KB) article 78184.

**Note** Automated updates for Horizon Cloud Connector 1.5 in VMware Cloud on AWS are not supported with vCenter Server version 7.0.0.

- At least 50 GB of datastore capacity is available for deploying the appliance update.
- ESXi host is accessible from the Horizon Cloud Connector appliance.
- You have configured vCenter Server and network settings in the Horizon Cloud Connector configuration portal. For detailed instructions, see the next section in this topic.
- An unassigned static IP address is available for temporary use during the appliance update. This temporary address must be distinct from the static IP address used by your current version of the Horizon Cloud Connector appliance.

### Configuring vCenter Server and Network Settings

The automated update feature deploys new versions of the Horizon Cloud Connector appliance to your vCenter Server. To prepare your system environment for these deployments, first gather an unassigned static IP address and the network settings that you want to use for the updated appliance. Then perform the following steps.

**Remember** As stated at the start of this topic, the ability to configure the automated update feature is deactivated by default for Horizon Cloud Connector 1.6 or earlier and will only be available to you if and only if your Horizon Cloud tenant account is configured to allow it. You will not see any of these elements in the user interface if you have not specifically requested it by contacting your VMware representative or VMware support to activate it on your tenant account.

1. Log in to the Horizon Cloud Connector configuration portal.
2. To open the configuration screen for vCenter Server details, do one of the following:
   - (Horizon Cloud Connector 1.7 or later) Click the **Configure vCenter Server and Network Details** button.
   - (Horizon Cloud Connector 1.6 or earlier) Click the **Configure Automatic Cloud Connector Updates** button.
3. In the **Horizon Cloud Connector vCenter Server Details** screen, enter the FQDN of the vCenter Server, and click **Get Certificate**. After the certificate information appears, select I have verified the above certificate and would like to continue.
4. Under **Horizon Cloud Connector vCenter Server Credentials**, enter the user name and password for vCenter Server.

5. Under **Additional Static IP Details for Cloud Connector upgrade**, configure the required settings.

   **Note** The gateway, subnet, and DNS server settings used by the current appliance version do not transfer to the new appliance version during the update process. To use specific gateway, subnet, and DNS server settings for the new appliance version, you must configure these settings under **Additional Static IP Details for Cloud Connector upgrade**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static IP</td>
<td>The temporary, unassigned static IP address that you determined earlier. This address must be distinct from the static IP address used by the current version of the appliance. During the update process, the new version of the appliance uses the temporary static IP address to gain network access temporarily while the current version of the appliance remains operational.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Gateway configuration that you want to use for the new version of the appliance.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask that you want to use for the new version of the appliance.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>DNS server that you want to use for the new version of the appliance.</td>
</tr>
</tbody>
</table>

Important: Configure at most one DNS server for the new appliance version. If you configure multiple DNS servers, the appliance update will fail.

6. Click **Save**.

**End-to-End Flow of the Automated Update Process**

The automated update process for Horizon Cloud Connector is modeled after a software industry technique known as blue-green deployment.

The existing to-be-updated Horizon Cloud Connector instance is known as the blue appliance. The new version of Horizon Cloud Connector is known as the green appliance.

To view the current version number of the blue appliance, select **Settings > Capacity >** and click the **Pods** tab if needed. The version number appears next to the paired pod’s name in the list.
After you configure the vCenter Server and network settings in the Horizon Cloud Connector onboarding user interface, the end-to-end update process consists of the following steps:

1. When VMware releases an updated version of Horizon Cloud Connector that is compatible with the blue appliance, one of the following occurs:
   - If your system environment meets all the requirements for supporting the automated update, a notification message appears when you click the version number of the pod in the Capacity page.

In addition, the **Schedule Update** button becomes available on the pod details page. (To display the pod details page, select **Settings > Capacity >**, click the **Pods** tab if needed, and click the name of the pod in the list.) A notification banner on the page indicates the version number of the update that is available.
If these conditions are met, you can proceed to step 3 of the update process.

- If your system environment does not meet all the requirements for automated updates, the **Clear Update Errors** button appears instead on the pod details page. An alert banner also notifies you that an error is preventing the update.

2. If there are any error conditions preventing the update, you must resolve them. Click the **Clear Update Errors** button or the link in the alert banner to open the **Resolve Pod Update Errors** dialog box. Using the message in this dialog box as guidance, perform the necessary actions or update the necessary configurations to clear the described error condition. Then validate that the error has been resolved by selecting the check box next to the error description and clicking **Continue**.

The following screenshot shows an example of the **Resolve Pod Update Errors** dialog box after an error has been resolved.

It can take up to 30 minutes for the configuration changes to take effect and for the administration console to reflect these changes. When the error is cleared, the **Clear Update Errors** button changes to **Schedule Update**.

3. You must schedule the update to ensure that it is performed. On the pod details page, click **Schedule Update**. Then set a day and time for the Horizon Cloud service to update the blue appliance to the green appliance.
You determine the convenient time for the update to take place. Typically, the update process, including the deployment of the green appliance and the migration from the blue to the green appliance, takes up to 90 minutes. As a best practice, schedule the update at a time when the environment is least busy. After the update is scheduled, the console displays the time remaining until the scheduled update in a top banner. You can reschedule the time for the update at any time prior to the scheduled time, if required by your organization's needs.

The following screenshot shows an example of a banner indicating the scheduled update.

![Scheduled Update Banner](image)

**Important**  When you schedule the update, you are prompted for a date and time. This time is local to your browser time zone.

4. At your scheduled day and time, the service deploys the green appliance to the vCenter Server using the temporary IP address that you configured earlier in the [Horizon Cloud Connector vCenter Server Details](#) screen. This deployment stage typically takes around 25 minutes to complete. However, the exact duration can vary depending on the capacity and characteristics of your system infrastructure.

**Note**  During the update process—which includes the stages of deployment, migration, and IP address reassignment—you cannot perform administrative tasks on the pod paired with the blue appliance that is undergoing the update. In addition, all action buttons in the Horizon Cloud Connector configuration portal will be in a deactivated state. However, the blue appliance remains fully operational during the update and the pod remains connected to the cloud control plane and the subscription license service.

5. After the green appliance is completely deployed, the service migrates the configuration from the blue appliance to the green appliance. The migration stage typically takes around 10 minutes to complete.
6 When the migration is complete, the temporary IP address is unassigned from the green appliance and the permanent IP address of your Horizon Cloud Connector instance is reassigned from the blue appliance to the green appliance.

**Note** The reassignment results in a short period of downtime lasting less than a minute, during which the pod momentarily loses its connection to the control plane and Horizon Cloud services. During this time, end users might momentarily lose their connection sessions to remote desktops and applications on the pod.

Once the IP address reassignment is complete:

- The green appliance becomes fully operational and the pod's connection to the control plane and the subscription license service is restored.
- The green appliance takes a name composed of the blue appliance's name with the new version number appended as the suffix.
- The blue appliance remains in the datastore and is powered off.

7 To verify that the update has completed successfully, do the following:

- Select **Settings > Capacity >** and click the **Pods** tab if needed. The version number of the updated appliance appears next to the pod's name in the list.

- Log in to the Horizon Cloud Connector configuration portal of the green appliance and verify the health of the Horizon Cloud Connector components.

### Error Conditions That Prevent Automated Updates

Examples of common error messages include:

- Check to ensure Cloud Connector is online
- Cloud Connector is not deployed with static IP
- Unable to contact vCenter for upgrade. Please re-enter vCenter credentials in the Cloud Connector setup
There is not enough disk space to perform upgrade. Minimum required disk space is 50 GB.

Make the necessary configuration changes to fix the specified error so that you can proceed to schedule the automated update.

Troubleshoot the Horizon Cloud Connector Virtual Appliance Update

The earlier version of the Horizon Cloud Connector virtual appliance is disabled only at the end of the update process. If there is any update issue, you can roll back the update to the earlier version of the Horizon Cloud Connector virtual appliance.

**Note** When you perform any troubleshooting task, do not unplug the latest deployed version of the Horizon Cloud Connector appliance.

**Procedure**

1. If the update fails and the earlier version of the Horizon Cloud Connector virtual appliance is still accessible, you can continue to use this version of the virtual appliance. After you check the log files and verify the configuration information of the new Horizon Cloud Connector virtual appliance, you can perform the update task again.

2. If the update fails and the earlier version of the Horizon Cloud Connector virtual appliance is not accessible, perform these steps:
   a. Power off the new Horizon Cloud Connector virtual appliance.
   b. Revert the existing Horizon Cloud Connector virtual appliance to the virtual appliance snapshot taken prior to the update. Verify that the Horizon Cloud Connector virtual appliance is accessible from the Web browser and displays the paired status.
   c. Perform the update task to deploy the latest version of the Horizon Cloud Connector appliance again. If the issue persists, contact VMware Support.

**Collecting Log Files for Horizon Cloud Connector**

You can use the Horizon Cloud Administration Console or the Horizon Cloud Connector configuration portal to download the log files for a Horizon Cloud Connector virtual appliance. If you cannot access these automated methods for collecting logs, you can collect the logs manually by establishing an SSH connection to the appliance and running a command-line script.
Using the Horizon Cloud Connector Configuration Portal to Download the Appliance Logs

If you have deployed Horizon Cloud Connector 1.7 or later, you can use the appliance's configuration portal to download the log files for the virtual appliance in .zip format. This log collection capability is available before, during, and after you pair the Horizon pod with Horizon Cloud.

1. Using a browser, navigate to the URL of the Horizon Cloud Connector appliance.
2. In the login screen, enter your My VMware account credentials and click Login. If needed, click Accept to continue past the Terms of Service message.
3. Click Download Log in any of the configuration portal screens. Specify a location for the .zip logs package and save the logs package.

Using Horizon Cloud Administration Console to Download the Horizon Cloud Connector Logs

After you successfully pair a Horizon pod with Horizon Cloud and register Horizon Cloud with the Active Directory domain for that pod, you can use Horizon Cloud Administration Console to download the Horizon Cloud Connector logs in .zip format.

1. In the console, navigate to the details page for the pod. Select Settings > Capacity. Click the Pods tab if needed and then click the name of the pod in the list. If needed, click the Summary tab to display the pod's details page.
2. Select More > Download Connector Logs. Specify a location for the .zip logs package and save the logs package.

Collecting the Horizon Cloud Connector Logs Using the Command Line

If you have deployed Horizon Cloud Connector 1.7 or later and cannot access the Download Log button in the Horizon Cloud Connector configuration portal or the Download Connector Logs action in Horizon Cloud Administration Console, you can still collect the appliance's log files manually by running a command-line script.

1. Open an SSH connection to the Horizon Cloud Connector appliance.
2. In the command-line terminal, run the following script:

   ```bash
   /opt/vmware/bin/configure-adapter.py --archiveLogs
   ```

   The script bundles the logs and archives them as a .tgz package in the /home/logs directory. You can find the filename of the .tgz archive listed near the end of the script's output.
For example, the following excerpt shows the output of a script that has saved the Horizon Cloud Connector logs to the cc_logs_20200424_154638.tgz archive in /home/logs.

```
/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!
```

Horizon Cloud Connector Known Considerations

Keep these considerations in mind when you are using Horizon Cloud Connector.

- You must deploy the Horizon Cloud Connector virtual appliance into your pod's vSphere environment using vSphere Client or vSphere Web Client. Do not deploy the appliance directly into the ESXi host.

- Use of IPv6 with the Horizon Cloud Connector virtual appliance is not supported.

- Proxy SSL configuration is not supported during the deployment of the Horizon Cloud Connector virtual appliance.

- Due to a known limitation, any no-proxy host configuration that you specify when deploying the OVF template is not honored by Horizon Cloud Connector 1.5 or earlier. To configure a no-proxy host configuration, you must change a configuration file in the appliance after it is deployed. For details, see VMware Knowledge Base article 76663. This limitation does not apply to Horizon Cloud Connector 1.6 or later.

- If you plan to use the pod with Universal Broker and Horizon Cloud Connector 1.5, and your environment requires using proxy settings, you must configure those proxy settings when you deploy the OVF template. Due to a known limitation, Universal Broker will not honor any modifications made to proxy settings after deployment. Since you can only configure no-proxy hosts after deployment, this limitation means that the use of no-proxy hosts with Universal Broker is not supported by Horizon Cloud Connector 1.5. This limitation does not apply when you use Universal Broker with Horizon Cloud Connector 1.6 or later.

- Information about the static IP and proxy settings for the deployed Horizon Cloud Connector virtual appliance is saved in certain container files. When you want to change those settings on the virtual appliance, you must connect to the virtual appliance and edit those container files. If you change the static IP address for the deployed virtual appliance in your vSphere environment, you must edit the appropriate container file in the virtual appliance's operating system and run a command to ensure that the new IP address is shared with all the pod's components that depend upon the virtual appliance. See Update the Static IP for the Horizon Cloud Connector Virtual Appliance.

- Before deleting the Horizon Cloud Connector virtual appliance from your vCenter environment, point your browser to the Horizon Cloud Connector appliance's IP address and use the Unplug action to remove the connection between the pod and Horizon Cloud.
Using a separate vdmadmin account for the Horizon Cloud Connector paired with the Horizon pod is a best practice. Using a separate vdmadmin account avoids configurations being overridden between cloud and on-premises management. Using separate accounts also provides easier auditing for the cloud-based operations.

The connection between the Horizon Cloud Connector and Horizon Cloud uses outbound Internet port 443. For all the connector's required DNS, ports, and protocols, see DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod.

You set the password for the root user of the Horizon Cloud Connector virtual appliance during deployment. By default, this password does not expire. However, based on your organization's security policy, you might want to periodically update that root password by setting an expiry policy for that root user. For steps, see Set a Password Expiry Policy for the Horizon Cloud Connector Root User.

If your Connection Server is using self-signed certificates and you then replace those self-signed certificates after pairing the pod with Horizon Cloud, you must log in to the Horizon Cloud Connector interface and use the Reconfigure workflow to perform the certificate validation steps again with the new self-signed certificate. When you log in to the Horizon Cloud Connector interface, you can click Reconfigure and complete the wizard steps to verify communication using the new self-signed certificate from the Connection Server.

Similarly, upgrading your Connection Server might result in changes to self-signed certificates. To ensure validation of the new certificates, perform the Reconfigure workflow for the Horizon Cloud Connector after upgrading your Connection Server.

If you added an entry to the /etc/hosts file to resolve the IP address of the Connection Server, you must restart the hze-core and csms services. Use the following commands:

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

To ensure that the Horizon Cloud Connector virtual appliance authenticates correctly with Horizon Cloud and the required Connection Server instances, you must synchronize the virtual appliance's clock with an NTP server. For more information, see Synchronize the Horizon Cloud Connector Virtual Appliance with an NTP Server.

If you encounter connectivity issues with the Horizon Cloud Connector configuration portal, see the troubleshooting information in VMware Knowledge Base (KB) article VMware Knowledge Base (KB) article 79859.
Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment

You can use the cloud-management capabilities of Horizon Cloud to give your end users access to virtual resources, such as virtual desktops, session-based desktops, and remote applications. The resources can reside in an on-premises pod or in a pod on a public cloud. In some cases, you must select and set up a brokering method before you can configure assignments from a certain type of pod.

Setting Up a Brokering Method

A Horizon Cloud tenant environment can have the following brokering configurations. For details about the brokering types, and when and how they are configured, see Introduction to Universal Broker and Single-Pod Broker.

- Universal Broker type — relevant for both Horizon pods and Horizon Cloud pods deployed into Microsoft Azure.
- Single-pod broker — relevant only for Horizon Cloud pods deployed into Microsoft Azure.

End-User Assignments You Can Configure Using Resources from Pods Deployed into Microsoft Azure

When Universal Broker is configured as the brokering method for your tenant's pods in Microsoft Azure, you can configure the following types of assignments:

- A multi-cloud assignment consisting of VDI desktops from either one or more Horizon pods, or one or more pods in Microsoft Azure. For more information, see Pods in Microsoft Azure - Create a VDI Multi-Cloud Assignment.
- A session desktop assignment consisting of session-based desktops from Microsoft Remote Desktop Services (RDS) hosts within a single pod in Microsoft Azure. For more information, see Create an RDSH Session Desktop Assignment.
A remote applications assignment consisting of applications provisioned by RDS hosts within pods in Microsoft Azure. For more information, see Remote Applications - Create a Remote Application Assignment for Remote Applications Provisioned By Horizon Cloud Pods in Microsoft Azure.

An App Volumes applications assignment consisting of App Volumes applications hosted on VDI desktops within pods in Microsoft Azure, For more information, see Create an App Volumes Assignment.

When single-pod broker is selected as the brokering method for your tenant's pods in Microsoft Azure, you can configure the following types of assignments:

- A VDI desktop assignment consisting of virtual desktops from a single pod in Microsoft Azure. For more information, see Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure and Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure.

- A session desktop assignment consisting of session-based desktops from Microsoft Remote Desktop Services (RDS) hosts within a single pod in Microsoft Azure. For more information, see Create an RDSH Session Desktop Assignment.

- A remote applications assignment consisting of applications provisioned by RDS hosts within pods in Microsoft Azure. For more information, see Remote Applications - Create a Remote Application Assignment for Remote Applications Provisioned By Horizon Cloud Pods in Microsoft Azure.

- An App Volumes applications assignment consisting of App Volumes applications hosted on VDI desktops within pods in Microsoft Azure, For more information, see Create an App Volumes Assignment.

End-User Assignments You Can Configure Using Resources from Cloud-Connected Horizon Pods

In addition to the Horizon Cloud features for unified visibility, health monitoring, and help desk services for cloud-connected Horizon pods deployed on premises or in VMware Cloud on AWS, you can create multi-cloud assignments. A multi-cloud assignment uses Universal Broker to allocate pod resources such as virtual desktops to your end users.

For overview information about configuring multi-cloud assignments based on resources from your Horizon Cloud tenant's cloud-connected Horizon pods, see High-Level Steps for Setting Up Horizon Cloud Multi-Cloud Assignments (MCA) for Your Horizon Cloud Tenant.

This chapter includes the following topics:

- Introduction to Universal Broker and Single-Pod Broker
- System Requirements for Universal Broker
- Setting Up a Brokering Method
High-Level Steps for Setting Up Horizon Cloud Multi-Cloud Assignments (MCA) for Your Horizon Cloud Tenant

Working with Sites in a Universal Broker Environment

Horizon Pods - Enabling a Cloud-Connected Pod for Multi-Cloud Assignments

Creating and Managing Multi-Cloud Assignments in Your Horizon Cloud Tenant Environment

Introduction to Universal Broker and Single-Pod Broker

The cloud control plane provides two distinct brokering methods for delivering remote resources from your cloud-connected pods to end users: Universal Broker and single-pod broker (available for pods in Microsoft Azure only). You collect the remote resources together in an entity known as an end-user assignment. The tenant-wide brokering method that you select and enable for each pod type determines the types of end-user assignments you can create.

Important Be sure to review the following information in this documentation topic carefully before you proceed to Select a Brokering Method for End-User Assignments. Since your brokering selection becomes a tenant-wide setting that cannot be changed, it is important for you to understand how each brokering method applies to your use cases involving specific pod types and assignment types before you make a permanent selection.

Considerations When Selecting a Brokering Method

Keep the following points in mind as you consider the brokering method to select for end-user assignments from your cloud-connected pods.

- In a hybrid environment that contains both Horizon pods deployed on premises or in VMware Cloud on AWS and pods deployed in Microsoft Azure, each pod type can have its own tenant-wide brokering method.

- Once you select a brokering method, that brokering method becomes a permanent, irreversible, and tenant-wide setting for the specified pod type. For example, if you select Universal Broker for your Horizon pods, Universal Broker becomes the brokering method for all Horizon pods across your tenant account and cannot be changed.

- If you select Universal Broker as the brokering method for both your Horizon pods and pods in Microsoft Azure, each end-user assignment you create must consist of VDI desktops from only one pod type. For example, you can create an assignment consisting of desktops that span multiple Horizon pods or an assignment consisting of desktops that span multiple pods in Microsoft Azure. However, you cannot create an assignment consisting of desktops that span a mix of Horizon pods and pods in Microsoft Azure.

- The brokering options available to you depend on a combination of factors, including the pod type, date of pod deployment, and whether a brokering method has been previously selected for another pod type. For more details, see the following table.
## Overview of Universal Broker

Universal Broker, the latest cloud-based brokering technology from VMware, is available for the following types of cloud-connected pods:

- Horizon pods hosted on premises or in VMware Cloud on AWS
- Pods deployed in Microsoft Azure at the July 2020 release's manifest or later. The pod manifest that was released in July 2020 is 2298.0.

**Note** Universal Broker is available only if you have deployed all your pods in Microsoft Azure at the July 2020 release's manifest or later. If you deployed any of your pods in Microsoft Azure prior to the July 2020 release, Universal Broker is not an available brokering option and single-pod brokering is used as the default.

When you select Universal Broker as the tenant-wide brokering method for a particular pod type, you can create the following types of end-user assignments:

- A multi-cloud assignment consisting of VDI desktops from either one or more Horizon pods, or one or more pods in Microsoft Azure.
- A session desktop assignment consisting of session-based desktops from Microsoft Remote Desktop Services (RDS) hosts within a single pod in Microsoft Azure.

<table>
<thead>
<tr>
<th>State of Your Tenant Account at the Time of the July 2020 Release</th>
<th>Brokering Options Available for Horizon Pods (On-Premises or in VMware Cloud on AWS)</th>
<th>Brokering Options Available for Pods in Microsoft Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td>New tenant with no pods deployed yet</td>
<td>Universal Broker</td>
<td>Universal Broker or single-pod broker</td>
</tr>
<tr>
<td>All of the following:</td>
<td>Universal Broker</td>
<td>Universal Broker or single-pod broker</td>
</tr>
<tr>
<td>- One or more Horizon pods deployed, all in monitored state</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- No brokering selection has been made for Horizon pods yet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- No pods deployed in Microsoft Azure yet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All of the following:</td>
<td>Universal Broker is already selected</td>
<td>Universal Broker is automatically selected</td>
</tr>
<tr>
<td>- One or more Horizon pods deployed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Universal Broker selected and configured for Horizon pods</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- No pods deployed in Microsoft Azure yet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>One or more pods deployed in Microsoft Azure already</td>
<td>Universal Broker</td>
<td>Single-pod broker is automatically selected</td>
</tr>
<tr>
<td>Integrated with VMware Workspace ONE Access</td>
<td>Universal Broker</td>
<td>Single-pod broker is automatically selected</td>
</tr>
</tbody>
</table>
- An application assignment consisting of applications provisioned by RDS hosts within pods in Microsoft Azure
- An App Volumes applications assignment consisting of App Volumes applications hosted on VDI desktops within pods in Microsoft Azure

For detailed information about how the system components of the Universal Broker solution work together to allocate remote resources to end users, see **System Architecture and Components of Universal Broker**.

Universal Broker offers the following key features:

- **Single connection FQDN for all remote resources**

  End users can access multi-cloud assignments in your environment by connecting to a fully qualified domain name (FQDN), which you define in the Universal Broker configuration settings. Through the single Universal Broker FQDN, users can access assignments from any participating Horizon pod in any site in your environment. No internal networking between your pods is required.
- **Global pod connectivity and awareness for optimal performance**
  
  Universal Broker maintains direct connectivity with every pod participating in multi-cloud assignments and stays aware of the availability status of each pod. As a result, Universal Broker can manage connection requests and deliver virtual resources to end users directly from these pods. There is no need for global server load balancing (GSLB) or any interpod network communication which can result in reduced performance and latency issues.

- **Smart brokering**
  
  By maintaining an awareness of your geographical sites and pod topology, Universal Broker can deliver desktops from multi-cloud assignments to end users along the shortest network route.

---

**Note**  This release of Universal Broker has some known feature limitations. If your use case requires the implementation of a feature that Universal Broker does not support, such as integration with VMware Workspace ONE Access, you must use single-pod broker instead. For more information, see [Known Limitations of Universal Broker](#).

---

**Overview of Single-Pod Broker**

Also known as legacy or classic brokering, single-pod broker is available only for pods in Microsoft Azure in the following cases:

- **When all your pods in Microsoft Azure were deployed at the July 2020 release's manifest or later**

  In this case, you must explicitly select **Single-Pod Broker** in the Broker selection page to use this classic brokering method for all the pods in Microsoft Azure deployed across your tenant account.

- **When at least one of your pods in Microsoft Azure was deployed prior to the July 2020 release**

  In this case, you do not have the option of selecting a brokering method. Single-pod broker is used by default as the implicit brokering method for all the pods in Microsoft Azure deployed across your tenant account.
With single-pod brokering, you can create the following types of end-user assignments:

- A VDI desktop assignment consisting of virtual desktops from a single pod in Microsoft Azure
- A session desktop assignment consisting of session-based desktops from Microsoft Remote Desktop Services (RDS) hosts within a single pod in Microsoft Azure
- A remote applications assignment consisting of applications provisioned by RDS hosts within pods in Microsoft Azure
- An App Volumes applications assignment consisting of App Volumes applications hosted on VDI desktops within pods in Microsoft Azure

Single-pod broker supports a wider range of Horizon features than Universal Broker does. For example, single-pod broker supports features associated with VMware Workspace ONE Access integration, such as True SSO.

System Architecture and Components of Universal Broker

Universal Broker represents the latest cloud-based brokering technology from VMware and is the preferred brokering method for end-user assignments in new deployments. Universal Broker includes several system components that run within participating pods and in the cloud.

For an overview of the key features of Universal Broker, see Introduction to Universal Broker and Single-Pod Broker.

The system architecture of the Universal Broker solution varies slightly based on whether the brokered resources reside on Horizon pods or on pods in Microsoft Azure.

System Architecture of Universal Broker for Horizon Pods

The following components comprise the Universal Broker solution for cloud-based brokering of multi-cloud assignments from Horizon pods.

- The Universal Broker service is a multi-tenant cloud service that runs within the Universal Broker cloud, which is connected to Horizon Cloud. Each customer connects to the Universal Broker service using a unique, dedicated FQDN that is configured as described in Configure Universal Broker.
- The Universal Broker client runs within the Horizon Cloud Connector for each of your cloud-connected Horizon pods. The client is part of the OVA file for Cloud Connector 1.5 or later and is automatically installed when you pair the Cloud Connector with your pod.
- The Universal Broker plugin runs within the Connection Server for every cloud-connected pod that participates in multi-cloud assignments. You must download and install the plugin on each Connection Server instance within a participating pod, as described in Horizon Pods - Install the Universal Broker Plugin on the Connection Server.

The following diagram illustrates how Universal Broker works with the components in your Horizon pod environment to allocate virtual desktops from multi-cloud assignments to your end users.
1. From Horizon Client, the end user requests a virtual desktop by connecting to the Universal Broker service through the brokering FQDN. The service uses the XML-API protocol to authenticate the Horizon Client user and manage the connection session.

2. After determining that Pod 1 in Site 1 is the best available source for the desktop, the Universal Broker service sends a message to the Universal Broker client, which runs on the Horizon Cloud Connector paired with Pod 1.

3. The Universal Broker client forwards the message to the Universal Broker plugin, which runs on one of the Connection Server instances within Pod 1.
4 The Universal Broker plugin identifies the best available desktop to allocate to the end user.

5 The Universal Broker service returns a response to Horizon Client which includes the unique FQDN of Pod 1 (typically the FQDN of the Pod 1 load balancer). Horizon Client establishes a connection with the load balancer to request a protocol session with the desktop.

6 After passing through the local load balancer, the request goes to the Unified Access Gateway for Pod 1. The Unified Access Gateway validates that the request is trusted and prepares the Blast Secure Gateway, PCoIP Secure Gateway, and tunnel server.

7 The Horizon Client user receives the specified desktop and establishes a session based on the configured secondary protocol (Blast Extreme, PCoIP, or RDP).

For more information about the ports used for Universal Broker communications, see Horizon Pods - Port and Protocol Requirements for Universal Broker.

**System Architecture of Universal Broker for Pods in Microsoft Azure**

The following components comprise the Universal Broker solution for cloud-based brokering of VDI and RDSH assignments from pods in Microsoft Azure.

- The Universal Broker service is a multi-tenant cloud service that runs within the Universal Broker cloud, which is connected to Horizon Cloud. Each customer connects to the Universal Broker service using a unique, dedicated FQDN that is configured as described in Configure Universal Broker.

- The Universal Broker client runs within each participating pod in Microsoft Azure.
1 From Horizon Client, the end user requests a virtual resource by connecting to the Universal Broker service through the brokering FQDN. The service uses the XML-API protocol to authenticate the Horizon Client user and manage the connection session.

2 After determining that Pod 1 in Site 1 has the best available resource for the user's request, the Universal Broker service sends a message to the Universal Broker client running within Pod 1.

3 The Universal Broker client forwards the message to the active pod manager within Pod 1.

4 The active pod manager identifies the best available resource to allocate to the end user.
5 The Universal Broker service returns a response to Horizon Client which includes the unique FQDN of Pod 1 (typically the FQDN of the Microsoft Azure load balancer for Pod 1). Horizon Client establishes a connection with the load balancer to request a protocol session with the resource.

6 After passing through the Microsoft Azure load balancer, the request goes to the Unified Access Gateway for Pod 1. The Unified Access Gateway validates that the request is trusted and prepares the Blast Secure Gateway, PCoIP Secure Gateway, and tunnel server.

7 The Horizon Client user receives the specified resource and establishes a session based on the configured secondary protocol (Blast Extreme, PCoIP, or RDP).

For more information about the ports used for Universal Broker communications, see the "Ports and Protocols Required by Universal Broker" section in Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release’s Manifest or Later.

**Known Limitations of Universal Broker**

This release of Universal Broker supports a certain subset of Horizon features.

**Virtual Resources**

For the brokering of virtual desktops, this release of Universal Broker only supports Windows operating systems. Linux-based desktops are not supported.

This release does not support administrator-created shortcuts to desktops and applications.

**Horizon HTML Access and Horizon Client for Chrome**

End users can make requests for resources to the Universal Broker service by running Horizon HTML Access in a supported web browser or by running Horizon Client for Chrome 5.4 or later. If the brokering service redirects the request to a Unified Access Gateway instance that uses a self-signed certificate, the client application displays an error message indicating that the certificate authority is invalid.

This behavior is according to design. To connect to the requested resource, the user can accept the self-signed certificate by following the prompts in the certificate error message.

**Authentication Methods**

This release of Universal Broker supports client user authentication through Windows user name and password, in UPN and NETBIOS formats.

Two-factor authentication through Radius (for all cloud-connected pods) or RSA (for Horizon pods only) is also supported.

The following user authentication and access methods are not supported:

- Smart card
- Certificate
- SAML
Log in as the current user
Anonymous access

**VMware Workspace ONE Access**
This release of Universal Broker does not support integration with VMware Workspace ONE Access. Features associated with Workspace ONE Access integration, such as True SSO, are not supported.

**Remote Desktop Features**
The following features are not supported in this release of Universal Broker:
- URL content redirection
- Session collaboration

**Other Features**
The following features are also not supported in this release of Universal Broker:
- Kiosk mode
- Smart policies that require the identification of a user's location (for example, policies that pertain specifically to internal or external users)
- Timing profile (for troubleshooting user sessions)
- OPSWAT-based endpoint compliance checks

**System Requirements for Universal Broker**
To support the use of Universal Broker for the brokering of resources from your cloud-connected pods, your system environment must meet certain requirements.

**Requirements for Horizon Pods that are Connected to Horizon Cloud by Horizon Cloud Connector**
To support the use of Universal Broker for Horizon pods that are connected to the cloud service by Horizon Cloud Connector, your system environment must meet the following requirements.
- Each participating Horizon pod must be:
  - Running Horizon Connection Server version 7.11 or later, with a valid license and the Universal Broker plugin installed, as described in [Horizon Pods - Install the Universal Broker Plugin on the Connection Server](#)
  - Running Unified Access Gateway 3.8 or later. Unified Access Gateway is required for both internal and external network access. Direct connect mode is not supported.
  - Configured according to the [VMware Horizon 7 Documentation](#). See the "Configuring Horizon 7 for the First Time" topic in the [Horizon 7 Installation](#) document.
Cloud-connected to Horizon Cloud using Horizon Cloud Connector version 1.6 or later

**Note** If your Horizon pod is cloud-connected using Horizon Cloud Connector 1.8 or later, Universal Broker is supported if you deployed Horizon Cloud Connector with the Full Feature profile or if you deployed with the Basic Feature profile and then manually activated the Cloud Broker Client Service. For more information, see [Manually Activate Horizon Cloud Services for Horizon Cloud Connector 1.8 or Later](#).

- Configured with split DNS zones for the FQDN of the pod's load balancer, to route internal and external network traffic from Universal Broker to their respective internal and external DNS servers
- Configured with the required ports and protocols as described in [Horizon Pods - Port and Protocol Requirements for Universal Broker](#)
- Desktop pools must be configured on the participating pods and based on virtual machines running the Windows operating system. In addition, the pool configuration settings must meet the requirements of Universal Broker, as described in [Horizon Pods - Prepare an Existing Desktop Pool for Use in a Multi-Cloud Assignment](#).

### Requirements for Pods in Microsoft Azure

To support the use of Universal Broker, each participating pod in Microsoft Azure must be:

- Deployed new in Microsoft Azure at the July 2020 release's manifest (2298.0) or later

**Note** Universal Broker is available only if you have deployed **all** your pods in Microsoft Azure at the July 2020 release's manifest or later. If you deployed any of your pods in Microsoft Azure prior to the July 2020 release, Universal Broker is not an available brokering option for these pods.

- Configured with either an internal or external Unified Access Gateway instance. Unified Access Gateway is required for both internal and external network access. Direct connect mode is not supported.
- Configured with split DNS zones for the FQDN of the pod's load balancer, to route internal and external network traffic from Universal Broker to their respective internal and external DNS servers
- Configured such that the required DNS names for your regional Universal Broker instance are resolvable and reachable. See the "Pod Deployment and Operations DNS Requirements" table in [DNS Requirements for a Horizon Cloud Pod in Microsoft Azure](#).
- Configured with the required ports and protocols, as described in the "Ports and Protocols Required by Universal Broker" section in [Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later](#)
- In a healthy state. On the Capacity page, a healthy pod shows a green dot under the Status column, indicating that the pod is online and ready.
Client Requirements

To access remote resources brokered by Universal Broker, an end user must be running one of the following client applications:

- Horizon Client 5.4 or later for their operating system. Windows users can run Horizon Client for Windows 5.3 or later.

End users can also connect to the Universal Broker service through a web browser using Horizon HTML Access.

*Note*  Horizon HTML Access works for both versions 19.4 and 20.1 of the Universal Broker plugin for Horizon pods. Note that when using Horizon HTML Access, unless the SSL certificate configured on the load balancer of your Unified Access Gateway setup has a common name that precisely matches that load balancer’s name and is signed by a well-known Certificate Authority (CA), when the user launches a brokered desktop, their browser displays the standard browser ‘unsafe’ message. (For information about the relationship between a certificate’s common name and the hostname of where the certificate is installed, see [https://support.dnsimple.com/articles/what-is-common-name/](https://support.dnsimple.com/articles/what-is-common-name/).)

For more information about client releases, see the VMware Horizon Clients documentation page. You must provide your end users with the connection FQDN for Universal Broker. For instructions on how to configure the connection FQDN, see Configure Universal Broker.

Horizon Pods - Port and Protocol Requirements for Universal Broker

To establish ongoing communications between its brokering components and the system components in participating Horizon pods deployed on premises or in VMware Cloud on AWS, Universal Broker has specific port and protocol requirements. These requirements are described in the following table.

The Universal Broker client on the Horizon Cloud Connector establishes a persistent WebSocket connection with the Universal Broker service through port 443. The Universal Broker client receives connection requests from the service through a randomly selected port.

The Universal Broker client then forwards the request through a different randomly selected port to the Universal Broker plugin on the Connection Server. The Universal Broker plugin listens for these incoming requests through the port that was specified during the installation of the plugin.

For more information about the system architecture and traffic flow of Universal Broker, see System Architecture and Components of Universal Broker.
### Setting Up a Brokering Method

The process of setting up a brokering method for end-user assignments can vary in complexity, depending on the brokering method you select and the type of pod that you are configuring.

### Setting Up Single-Pod Broker for Pods in Microsoft Azure

This scenario requires little to no manual configuration. In some cases, you must select single-pod broker as your brokering method as described in Select a Brokering Method for End-User Assignments.
Setting Up Universal Broker for Pods in Microsoft Azure

**Note** Universal Broker is only supported if all of your pods deployed in Microsoft Azure are at pod manifest 2298.0 or later. To support the successful setup of Universal Broker, all your pods in Microsoft Azure must be online and in a healthy, ready state.

First, select Universal Broker as your brokering method as described in Select a Brokering Method for End-User Assignments. Then set up the Universal Broker service as described in Configure Universal Broker.

Setting Up Universal Broker for Horizon Pods Deployed on Premises or in VMware Cloud on AWS

This configuration involves several steps, which are described in detail in the following topics:

1. **Horizon Pods - Install the Universal Broker Plugin on the Connection Server**
2. **Horizon Pods - Configure Unified Access Gateway for Use with Universal Broker**
3. **Select a Brokering Method for End-User Assignments**
4. **Configure Universal Broker**

**Horizon Pods - Install the Universal Broker Plugin on the Connection Server**

Before a Horizon pod can participate in multi-cloud assignments brokered by Universal Broker, you must install the required plugin on each Connection Server instance in that pod. The Universal Broker plugin supports communication between the brokering service and the Connection Server instances within a pod.

When installing the Universal Broker plugin, observe the following considerations:

- You must download and install the version of the Universal Broker plugin that is compatible with your Connection Server version. To download the correct version of the plugin:
  a. Log in to my.vmware.com with your My VMware credentials and navigate to View & Download Products > Products A - Z > VMware Horizon Service > View Download Components.
  b. Locate the Horizon Cloud Connector product downloads group and click Go To Downloads. The Universal Broker plugin installer is on the Horizon Cloud Connector downloads page.
To access and download the correct version of the plugin for your Connection Server version, select the appropriate version of Horizon Cloud Connector on the downloads page.

**Note** The Horizon Cloud Connector version listed in the following table indicates the location of the Universal Broker plugin installer and does not necessarily match the version of Horizon Cloud Connector that you have paired with your Connection Server. For example, you might be running Connection Server 7.11 paired with Horizon Cloud Connector 1.7. However, you still must select Horizon Cloud Connector 1.6 on the downloads page to access the installer for version 19.4 of the plugin which is compatible with Connection Server 7.11.

<table>
<thead>
<tr>
<th>If your Connection Server version is:</th>
<th>Select this Horizon Cloud Connector version:</th>
<th>Then download this Universal Broker plugin version:</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.11</td>
<td>1.6</td>
<td>19.4</td>
</tr>
<tr>
<td>7.12</td>
<td>1.7</td>
<td>20.1</td>
</tr>
</tbody>
</table>

- If a pod has multiple Connection Server instances, you must install the Universal Broker plugin on each Connection Server instance.
- You must install the same version of the plugin on all Connection Server instances within participating pods. For example, if you upgrade the plugin to a later version on one Connection Server instance, you must upgrade the plugin to that same version on every other Connection Server instance within the pod.
- If you add a new Connection Server instance to a participating pod, you must install the plugin on the new Connection Server instance.
- Any existing plugin installation is lost during a Connection Server upgrade. If you upgrade your Horizon deployment, you must reinstall the plugin immediately after upgrading each Connection Server instance to the later version. For example, if you upgrade your Connection Server instances to version 7.12, you must then install version 20.1 of the plugin on those Connection Server instances.
- During the plugin installation, the Connection Server service is restarted and all administration console sessions on the Connection Server are logged off.
- In this release of Universal Broker, the plugin only supports IPv4.
- When working with the LDAP configuration in a Connection Server instance that has the Universal Broker plugin installed, observe the following guidelines:
  - In addition to making a backup copy of the LDAP configuration, take a virtual-machine snapshot of the current Connection Server instance. If you use the backup to restore the LDAP configuration to an earlier state, you can use the snapshot to populate the restored LDAP configuration with the information required by the Universal Broker plugin to function.
When restoring the LDAP configuration to an earlier state, only use LDAP backups made after the plugin was installed on the Connection Server.

If you restore the LDAP configuration to a state earlier than the Universal Broker plugin installation, certain information required by the plugin will be missing in the restored LDAP configuration. Therefore, the plugin will not function.

After downloading the correct version of the Universal Broker plugin for your Connection Server version, use the following procedures to install the plugin on the Connection Server instances within your pod.

To install the Universal Broker plugin silently on a bulk deployment of Connection Server instances, use the following command. Replace X.X.X with the version number and yyyyyyyyy with the build number of the plugin installer that you downloaded. Replace <portNumber> with the TCP port that the plugin uses to listen for and accept incoming requests from the Universal Broker client.

```
horizon-universal-broker-plugin-X.X.X-yyyyyyyy-x64.exe /s /v"LISTENPORT=<portNumber> /qn"
```

To install the Universal Broker plugin on an individual Connection Server instance, perform the numbered steps outlined later in this topic.

**Prerequisites**

Verify that:

- Each Connection Server instance on the pod is running version 7.11 or later, and you have downloaded the compatible version of the Universal Broker plugin for your Connection Server version.
- You have both Horizon administrator and local administrator privileges on the Connection Server. The plugin installer only runs when initiated by an administrator with both of these privileges.

**Procedure**

1. If needed, place the downloaded plugin installer file on the Connection Server.
2. Run the .exe installer file.
3. At the Welcome screen of the installer wizard, click Next.
4. Accept the End-User License Agreement, and click Next.
At the Configuration screen, specify the required port information.

- Enter the TCP port number that the Universal Broker plugin will use to listen for and accept incoming requests from the Universal Broker client.

  **Note** The installer validates that the specified port is available. If the port already has a process running on it, a warning message appears and the installation is stopped. To resume the installation, you must specify an available TCP port.

- Select **Configure Windows firewall exception automatically** if you want the installer to configure the firewall exception required to allow incoming connections through the specified port. Deselect this option if you want to configure the firewall exception manually.

  **Note** The Windows firewall exception is mandatory for Universal Broker, whether you instruct the installer to configure it or you configure it yourself.

- Click **Next**.

Follow the prompts in the remaining screens of the wizard to finish installing the Universal Broker plugin on the Connection Server.

**What to do next**

**Important** If, at a later time, you want to uninstall the Universal Broker plugin or the Connection Server instance, follow this order of uninstallation:

1. First, uninstall the Universal Broker plugin.
2. Next, uninstall Connection Server.

If you uninstall Connection Server first, a system error results and you will not be able to uninstall the Universal Broker plugin.

**Note** If you want to change the port that the Universal Broker plugin uses to listen for incoming requests from the Universal Broker client, do the following:

1. In the LDAP configuration for the Connection Server, change the value of the pae-RCXServerPort property to the new port number.
2. Restart the Connection Server.
3. If needed, update the corresponding Windows firewall exception to allow incoming traffic through the new port.

The new port configuration takes effect after the Connection Server and the Universal Broker plugin complete their restart sequences.
Horizon Pods - Configure Unified Access Gateway for Use with Universal Broker

To use Universal Broker with your cloud-connected Horizon pods, you must first replace the security server in each pod with a Unified Access Gateway appliance. Then you must configure the required JSON Web Token settings in each Unified Access Gateway instance to support the tunnel server and protocol redirection required by Universal Broker.

If you want to use two-factor authentication for Universal Broker, you must also configure the appropriate RADIUS or RSA SecurID service on each Unified Access Gateway instance.

Prerequisites

- Install a dedicated Unified Access Gateway appliance for each cloud-connected Horizon pod participating in multi-cloud assignments. Ensure that you install version 3.8 or later of Unified Access Gateway. Configure each Unified Access Gateway instance as the proxy server for connection requests to its paired Connection Server.

For more information, see the Unified Access Gateway documentation and the VMware Horizon 7 documentation.

**Note** Ensure that each Unified Access Gateway instance is paired with only one pod.

- To validate the pairing of each Unified Access Gateway instance with its respective Connection Server, connect directly to the Unified Access Gateway and verify that you can access virtual desktops.

Procedure

1. Log in to the Unified Access Gateway administration console.
2. In the **Configure Manually** section, click **Select**.
3. Under **Advanced Settings**, click the gearbox for **JWT Settings**.
4. To create a JWT configuration set, click **Add**.
5. Specify the required settings in the JWT Settings dialog box.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for the configuration set.</td>
</tr>
<tr>
<td>Issuer</td>
<td>Enter the cluster name of the Horizon pod, as displayed in Horizon Console.</td>
</tr>
</tbody>
</table>
### Setting | Description
--- | ---
Dynamic Public key URL | Enter https://<Horizon pod FQDN>/broker/publicKey/protocolredirection, where <Horizon pod FQDN> is replaced with the pod's unique FQDN (fully qualified domain name). The FQDN is typically defined as follows:
- If the pod has multiple Unified Access Gateway instances, specify the address of the local load balancer as the FQDN.
- If the pod has only one Unified Access Gateway instance, specify the address of that instance's paired Connection Server as the FQDN.

Public key URL thumbprints | To use a public key URL for authentication, enter the SHA1 thumbprint of the Horizon pod's certificate.

   **Note** You can configure either Public key URL thumbprints or Trusted Certificates for authentication. You do not need to configure both options.

Trusted Certificates | To use a certificate other than the Horizon pod's certificate for authentication, click the (+) icon and add the trusted certificate.

   **Note** You can configure either Trusted Certificates or Public key URL thumbprints for authentication. You do not need to configure both options.

Public key refresh interval | For best results, enter 900. This value sets the refresh interval to 900 seconds, or 15 minutes.

Static public keys | Leave this option set to its default value.

6. Click **Save** and then click **Close**.

7. If you want to use two-factor authentication for Universal Broker, enable the **Show** toggle for **Authentication Settings**. Then enable and configure settings for one of the security services supported by Universal Broker: RSA SecurID or RADIUS.

   **Note** You must configure the appropriate RADIUS or RSA SecurID service on the Unified Access Gateway instance for every participating pod. The configurations of all Unified Access Gateway instances within a participating pod must match each other and must be identical to the configurations of Unified Access Gateway instances across every other participating pod. Otherwise, authentication to the Universal Broker service fails.

   For example, if you want to use RADIUS authentication for your Universal Broker, you must configure the identical RADIUS service on every Unified Access Gateway instance across all participating pods. You cannot configure RADIUS on some participating pods and RSA SecurID on other participating pods.

**Select a Brokering Method for End-User Assignments**

In some cases, before you can create assignments to provide remote resources to your users from your cloud-connected pods, you must select a brokering method to use across your tenant account. Your selected brokering method determines the types of end-user assignments that you can create from the specified type of pod and how the resources in these assignments are allocated to users.
The cloud control plane provides two distinct brokering options for allocating remote resources from your cloud-connected pods to end users. Universal Broker and single-pod brokering.

**Universal Broker**

Available for the following types of cloud-connected pods:

- Horizon pods hosted on premises or in VMware Cloud on AWS
- Pods deployed in Microsoft Azure at the July 2020 release’s manifest or later. The pod manifest that was released in July 2020 is 2298.0.

> **Important** Universal Broker is available only if you have deployed all your pods in Microsoft Azure at the July 2020 release’s manifest or later. Also, to support the successful setup of Universal Broker, verify that all your pods in Microsoft Azure are online and in a healthy, ready state. If you deployed any of your pods in Microsoft Azure prior to the July 2020 release, Universal Broker is not an available brokering option and single-pod brokering is used as the default.

**Single-Pod Broker**

Available only for pods in Microsoft Azure.

- If all your pods in Microsoft Azure were newly deployed at the July 2020 release’s manifest (2298.0) or later, you must explicitly select **Single-Pod Broker** in the Broker selection page to use this classic brokering method.
- If at least one of your pods in Microsoft Azure was deployed prior to the July 2020 release, you do not have the option of selecting a brokering method and single-pod broker is used implicitly as the default.

You can select distinct brokering methods for Horizon pods hosted on premises or in VMware Cloud on AWS and for pods in Microsoft Azure. For more detailed information, see **Introduction to Universal Broker and Single-Pod Broker**.

**Prerequisites**

Verify that:

- You have carefully reviewed the information in **Introduction to Universal Broker and Single-Pod Broker** to determine the brokering method that you want to select for each type of pod.

> **Important** The **Introduction to Universal Broker and Single-Pod Broker** documentation topic contains important details about the features and availability of each brokering method, the types of end-user assignments they support, and how they might address your specific use cases. Since your brokering selection becomes a permanent, tenant-wide setting that cannot be changed, ensure that you thoroughly review this documentation topic before making your selection.

- You have deployed either:

  - At least one Horizon pod hosted on premises or in VMware Cloud on AWS
At least one pod in Microsoft Azure

**Note** To select a brokering option for your pods in Microsoft Azure, you must have deployed all of these pods at the July 2020 release's manifest or later. If any one of the pods was deployed prior to the July 2020 release, you do not have the option of selecting a brokering method and single-pod broker is used by default for all pods in Microsoft Azure across your tenant account.

You have registered an Active Directory domain with your Horizon Cloud environment and assigned the Horizon Cloud Super Administrator role to an Active Directory domain group. See [Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment](#).

The Broker selection page remains locked until you have completed these steps.

**Procedure**

1. Do one of the following:
   - In the **Getting Started** page, navigate to **General Setup > Broker** and click **Go**.
   - Select **Settings > Broker**.

   The Broker selection page appears. The exact appearance of this page depends on various factors, including the pod type for which you are selecting a brokering method and whether you have already made a broker selection for another pod type. For example:

   - The following screenshot shows the Broker selection page when you have deployed only pods in Microsoft Azure at the July 2020 release's manifest or later and no other pods.

   ![Broker Selection Page](image)

   - The following screenshot shows the Broker selection page when you have deployed only Horizon pods hosted on premises or in VMware Cloud on AWS, and no other pods.

   ![Broker Selection Page](image)
Important  The brokering selection you make is permanent and applies to all the pods of the specified type that you deploy across your tenant account. Once you click the Select button for a brokering method, you cannot change to the other method. You cannot use one brokering method for some assignments from a given pod type and a different brokering method for other assignments from that same pod type. The brokering method that you select becomes a permanent, irreversible, and tenant-wide setting for the specified pod type.

Important  If you intend to select Universal Broker as the brokering method for your pods in Microsoft Azure, ensure that all these pods are online and in a healthy, ready state. The Universal Broker service needs to communicate with the pods and perform some configuration steps on the pods to complete the setup process. If any of the pods in Microsoft Azure are offline or unavailable, the Universal Broker setup will fail.

2  Select the brokering method that you want to use.

- To select Universal Broker, click Select under the Universal Broker section. This action opens the configuration wizard for Universal Broker.
- To select single-pod brokering for pods in Microsoft Azure, click Show More to expand the Single-Pod Broker section. Then click Select under that section.

What to do next

Do one of the following:

- If you selected Universal Broker, complete the steps in the broker configuration wizard as described in Configure Universal Broker.

- If you selected single-pod brokering, no further configuration is required. You can proceed to create VDI desktop assignments, session desktop assignments, and application assignments based on resources from your pods in Microsoft Azure. For detailed information, see the subtopics under Chapter 7 Introduction to Horizon Cloud Pods in Microsoft Azure.

Configure Universal Broker

To use Universal Broker to allocate resources from multi-cloud assignments, you must configure certain settings. These settings include the fully qualified domain name (FQDN) for the Universal
Broker service and optional two-factor authentication. You can also configure session timeout values and user access to certain Horizon features.

The configuration wizard for Universal Broker opens automatically after you first select Universal Broker as your tenant-wide brokering method. You can also open the configuration wizard manually.

**Prerequisites**

Prepare the required system components according to your pod type.

**Horizon pods deployed on premises or in VMware Cloud on AWS:**

- Configure the required ports, as described in [Horizon Pods - Port and Protocol Requirements for Universal Broker](#).
- **Horizon Pods - Install the Universal Broker Plugin on the Connection Server.**
- **Horizon Pods - Configure Unified Access Gateway for Use with Universal Broker.** If you want Universal Broker to use two-factor authentication for your Horizon pods, configure the appropriate RADIUS or RSA SecurID service on each Unified Access Gateway instance within every participating pod.
- Select Universal Broker as your tenant-wide brokering method for Horizon pods, as described in [Select a Brokering Method for End-User Assignments](#).

**Pods in Microsoft Azure:**

- Verify that the required DNS names for your regional Universal Broker instance are resolvable and reachable. See the "Pod Deployment and Operations DNS Requirements" table in [DNS Requirements for a Horizon Cloud Pod in Microsoft Azure](#).
- Configure the required ports and protocols, as described in the "Ports and Protocols Required by Universal Broker" section in [Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later](#).
- If you want Universal Broker to use two-factor authentication for your pods in Microsoft Azure, configure the RADIUS service on each Unified Access Gateway instance within every participating pod. See [Enable Two-Factor Authentication on a Horizon Cloud Pod's Gateways](#).
- Select Universal Broker as your tenant-wide brokering method for pods in Microsoft Azure, as described in [Select a Brokering Method for End-User Assignments](#).

**Important** Ensure that all your pods in Microsoft Azure are online and in a healthy, ready state. The Universal Broker service needs to communicate with the pods and perform some configuration steps on the pods to complete the setup process. If any of the pods are offline or unavailable, the Universal Broker setup fails.
Procedure

1. If needed, open the configuration wizard for setting up Universal Broker.
   - In the **Getting Started** page, go to **General Setup > Broker** and click **Go**. Then click **Set Up** to specify a new configuration, or click the pencil icon to edit an existing configuration.
   - Select **Settings > Broker**. Then click **Set Up** to specify a new configuration, or click the pencil icon to edit an existing configuration.

The configuration wizard for Universal Broker appears.
2 In the FQDN page of the wizard, configure the settings for your brokering connection FQDN. These settings define the dedicated connection address that your end users will use to access resources allocated by Universal Broker.

**Note** When you modify a subdomain or FQDN setting, it might take some time for the change to take effect across all your DNS servers.

a For Type, select either a **VMware Provided** or **Custom** fully qualified domain name (FQDN).

b Specify additional settings for the selected FQDN type.

- If you selected the **VMware Provided** type, specify settings as follows.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub Domain</td>
<td>Enter the unique DNS name of a valid subdomain in your network configuration that represents your company or organization. This subdomain is prefixed to the VMware-provided domain to form the brokering FQDN.</td>
</tr>
<tr>
<td>Brokering FQDN</td>
<td>This read-only field displays the configured FQDN. The FQDN uses the format https://&lt;your_sub-domain&gt;vmwarehorizon.com. Provide this FQDN to your end users to allow them to connect to the Universal Broker service using Horizon Client. Universal Broker manages the DNS and SSL validation of this FQDN.</td>
</tr>
</tbody>
</table>

The following screenshot shows an example of the configuration wizard with the settings for a VMware-provided FQDN filled in.
If you selected the **Custom** type, specify settings as follows.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brokering FQDN</td>
<td>Enter the custom FQDN that your end users will use to access the Universal Broker service. Your custom FQDN functions as an alias to the automatically generated VMware-provided FQDN that completes the connection to the service. You must be the owner of the domain name specified in your custom FQDN and provide a certificate that can validate that domain. <strong>Note</strong> Your custom FQDN, also known as the connection URL, represents your company or organization. Ensure that you have the proper authorization to use this custom FQDN. <strong>Important</strong> You must create a CNAME record on your DNS server that maps your custom FQDN to the VMware-provided FQDN representing the internal connection address of the Universal Broker service. For example, the record might map vdi.examplecompany.com to <code>&lt;auto-generated string&gt;.vmwarehorizon.com</code>.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Click <strong>Browse</strong> and upload the certificate (in password-protected PFX format) that validates your brokering FQDN. The certificate must be signed by a trusted CA, and the certificate’s Subject Alternative Name (SAN) must match the FQDN.</td>
</tr>
</tbody>
</table>
The PFX file must contain the entire certificate chain and the private key: domain certificate, intermediate certificates, root CA certificate, private key. The Universal Broker service uses this certificate to establish trusted connection sessions with clients.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter the password for the PFX certificate file.</td>
</tr>
<tr>
<td>VMware Provided FQDN</td>
<td>This read-only field displays the VMware-provided FQDN that is automatically generated for the brokering service. The FQDN takes the format https://&lt;auto-generated string&gt;.vmwarehorizon.com. The VMware-provided FQDN is not visible to end users and represents the internal connection address of the Universal Broker service. Your custom FQDN functions as an alias to the VMware-provided FQDN. <strong>Important</strong> You must set up an alias association by creating a CNAME record on your DNS server that maps your custom FQDN to the VMware-provided FQDN. For example, the record might map vdi.examplecompany.com to &lt;auto-generated string&gt;.vmwarehorizon.com.</td>
</tr>
</tbody>
</table>

The following screenshot shows an example of the configuration wizard with the settings for a custom FQDN filled in.

![Configuration Wizard Screenshot]

When you are finished configuring the FQDN settings, click **Next** to proceed to the next page of the wizard.
3 (Optional) In the **Authentication** page of the wizard, configure two-factor authentication.

By default, Universal Broker authenticates users solely through their Active Directory user name and password. You can implement two-factor authentication by specifying an additional authentication method.

**Important** To use two-factor authentication for Universal Broker, you must first configure the appropriate authentication service on each Unified Access Gateway instance within every participating pod. The configurations of Unified Access Gateway instances must be identical within and across participating pods.

For example, if you want to use RADIUS authentication, you must configure the RADIUS service on each Unified Access Gateway instance across all participating Horizon pods and pods in Microsoft Azure.

Do not delete any Unified Access Gateway instances within the participating pods. Since Universal Broker relies on Unified Access Gateway for the protocol traffic between Horizon Client and virtual resources, users cannot access provisioned resources from a participating pod if you delete the Unified Access Gateway instance on that pod.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Factor Authentication</td>
<td>To use two-factor authentication, enable this toggle. When you enable the toggle, you are presented with additional options for configuring two-factor authentication.</td>
</tr>
</tbody>
</table>
| Type                  | Specify the authentication method that you want to use in addition to the Active Directory user name and password.  
- To use two-factor authentication across both your Horizon pods and pods in Microsoft Azure, select **RADIUS**.  
- To use two-factor authentication for your Horizon pods only, select **RSA SecurID**.  
**Note** In this release, RSA SecurID is supported on Horizon pods but not on pods in Microsoft Azure. If you select **RSA SecurID**, users' RSA authentication requests are attempted through the Unified Access Gateway instances of your Horizon pods only. Active Directory user name and password authentication requests are attempted through the Unified Access Gateway instances of either Horizon pods or pods in Microsoft Azure. |
| Maintain User Name    | Enable this toggle to maintain the user’s Active Directory user name during authentication to Universal Broker. When enabled:  
- The user must have the same user name credentials for the additional authentication method as for their Active Directory authentication to Universal Broker.  
- The user cannot change the user name in the client login screen.  
If this toggle is disabled, the user is allowed to type a different user name in the login screen. |
### Setting Description

#### Show Hint Text
Enable this toggle to configure a text string that displays in the client login screen to help prompt the user for their credentials to the additional authentication method.

#### Custom Hint Text
Enter the text string that you want to display in the client login screen. The specified hint appears to the end user as Enter your DisplayHint user name and password, where DisplayHint is the text string you enter in this text box. This hint can help guide users to enter the correct credentials. For example, entering the phrase Company user name and domain password below for results in a prompt to the end user that states: Enter your Company user name and domain password below for user name and password.

The following screenshot shows an example of the configuration wizard with two-factor authentication settings filled in.

![Configuration Wizard Screenshot]

When you are finished configuring two-factor authentication, click **Next** to proceed to the next page of the wizard.

4. In the **Settings** page of the configuration wizard, configure **Durations** settings for Horizon Client.

These timeout settings apply to the connection session between Horizon Client and the assigned desktop allocated by Universal Broker. These settings do not apply to the user's login session to the guest operating system of the assigned desktop. When Universal Broker detects the timeout conditions specified by these settings, it closes the user's Horizon Client connection session.
### Setting | Description
--- | ---
**Client Heartbeat Interval** | Controls the interval, in minutes, between Horizon Client heartbeats and the state of the user’s connection to Universal Broker. These heartbeats report to Universal Broker how much idle time has passed during the Horizon Client connection session. Idle time is measured when no interaction occurs with the end-point device running Horizon Client. This idle time is not affected by inactivity in the login session to the guest operating system that underlies the user’s assigned desktop. In large desktop deployments, increasing the **Client Heartbeat Interval** might reduce network traffic and improve performance.

**Client Idle User** | Maximum idle time, in minutes, allowed during a connection session between Horizon Client and Universal Broker. When the maximum time is reached, the user’s authentication period expires, and Universal Broker closes all active Horizon Client sessions. To reopen a connection session, the user must reenter their authentication credentials on the Universal Broker login screen.

*Note* To avoid disconnecting users unexpectedly from their assigned desktops, set the **Client Idle User** timeout to a value that is at least double that of the **Client Heartbeat Interval**.

**Client Broker Session** | Maximum time, in minutes, allowed for a Horizon Client connection session before the user’s authentication expires. The time starts when the user authenticates to Universal Broker. When the session timeout occurs, the user can continue to work in their assigned desktop. However, if they perform an action (such as changing settings) that requires communication with Universal Broker, Horizon Client prompts them to reenter their Universal Broker credentials.

*Note* The **Client Broker Session** timeout must be greater than or equal to the sum of the **Client Heartbeat Interval** value and the **Client Idle User** timeout.

**Client Credential Cache** | Controls whether to store user login credentials in the client system cache. Enter 1 to store user credentials in the cache. Enter 0 if you do not want to store user credentials in the cache.

5 In the **Settings** page of the configuration wizard, configure **Policy Details**.

Policy Details control whether end users can access certain Horizon features, provided that the features are available on the desktop and client.

### Setting | Description
--- | ---
**Multimedia Redirection (MMR)** | Enable this toggle to allow your end users access to the Multimedia Redirection feature, if the feature is available on the desktop and client.

**USB Access** | Enable this toggle to allow your end users to the USB Redirection feature, if the feature is available on the desktop and client.
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Clean Up HTML Access Credentials When Tab is Closed | Enabling this setting removes a user's credentials from cache when a user closes a tab that connects to a remote desktop, or closes a tab that connects to the desktop selection page, in the HTML Access client. When this setting is enabled, credentials are also removed from cache in the following HTML Access client scenarios:  
  - A user refreshes the desktop selection page or the remote session page.  
  - The server presents a self-signed certificate, a user starts a remote desktop, and the user accepts the certificate when the security warning appears.  
  - A user runs a URI command in the tab that contains the remote session.  
  When this setting is disabled, the credentials remain in cache. |
| Allow Client to Wait for Powered-Off VM           | Enabling this setting allows Horizon Client to retry connection requests to a remote desktop that is currently unavailable. For example, a client user might request a desktop that is currently powered off. With this setting enabled, Horizon Client can resend its connection request and establish a connection session when the desktop is powered on and available. |

When you are finished configuring Policy Details, click **Next** to proceed to the next step of the wizard.

6. Review your settings in the **Summary** page, and then click **Finish** to save and apply the configuration.

It typically takes a few seconds for the configuration settings to take full effect in the Universal Broker service, as DNS records are propagated across the DNS servers in all global regions. Depending on your system and network conditions, however, this process might sometimes take up to 30 minutes to complete. During this time, the Universal Broker service is unavailable. When the setup is completed successfully, the Broker section on the Getting Started page shows the **Complete** and the **Settings > Broker** page shows the **Enabled** status with a green dot.

**Important** If the Universal Broker setup fails, the **Settings > Broker** page shows the **Error** status with a red alert icon. To remediate the configuration failure and set up the Universal Broker service, contact VMware Support as described in VMware Knowledge Base (KB) article 2006985.

### What to do next

- If you have configured Universal Broker for Horizon pods deployed on premises or in VMware Cloud on AWS, proceed to change the pods to managed state. See **Horizon Pods - Change a Pod to Managed State**.
If you have configured Universal Broker for pods deployed in Microsoft Azure, proceed to create end-user assignments. See Creating Assignments in a Universal Broker Environment.

High-Level Steps for Setting Up Horizon Cloud Multi-Cloud Assignments (MCA) for Your Horizon Cloud Tenant

This topic summarizes the high-level procedures that you must complete to set up multi-cloud assignments brokered by Universal Broker.

High-Level Steps for Configuring Multi-Cloud Assignments Provisioned by On-Premises Horizon Pods or Horizon Pods in VMware Cloud on AWS

To set up multi-cloud assignments of resources from Horizon pods, complete the following high-level procedures.

1. Verify that the system components in your Horizon pod environment meet the necessary System Requirements for Universal Broker.

2. Onboard the participating Horizon pods to Horizon Cloud using Horizon Cloud Connector version 1.6 or later. See High-Level Workflow When You are Onboarding an Existing Manually Deployed Horizon Pod as Your First Pod to Your Horizon Cloud Tenant Environment.

3. For each participating pod, prepare the necessary system components for working with Universal Broker.
   a. Horizon Pods - Install the Universal Broker Plugin on the Connection Server. You must install the plugin on every Connection Server instance within the pod.
   b. Horizon Pods - Configure Unified Access Gateway for Use with Universal Broker. You must configure every Unified Access Gateway instance within the pod. If you want to use two-factor authentication for Universal Broker, you must configure the same authentication settings for every Unified Access Gateway instance across all participating pods.

4. Select Universal Broker as the brokering method for Horizon pods in your Horizon Cloud tenant. See Select a Brokering Method for End-User Assignments.


6. Enable each participating pod for multi-cloud assignments, as described in Horizon Pods - Change a Pod to Managed State.

7. Define the site configuration and home site associations for your Horizon Cloud tenant. See Configuring Sites for Universal Broker and Configuring Home Sites for Universal Broker.

8. Within the participating pods, configure desktop pools with the mandatory settings required by Universal Broker. See Horizon Pods - Prepare an Existing Desktop Pool for Use in a Multi-Cloud Assignment and Horizon Pods - Create a New Desktop Pool for Multi-Cloud Assignments.
9. Configure the multi-cloud assignments. See Horizon Pods - Create a Multi-Cloud Assignment of VDI Desktops.

**High-Level Steps for Configuring Multi-Cloud Assignments Provisioned by Pods in Microsoft Azure**

To set up multi-cloud assignments of resources from pods in Microsoft Azure, complete the following high-level procedures.

1. Deploy each pod at pod manifest 2298.0 or later.

   **Note** Universal Broker is only supported if you deploy all your pods in Microsoft Azure at pod manifest 2298.0 or later. The pod manifest 2298.0 debuted with the service's July 2020 release.

2. Verify that the system components in your pod meet the necessary System Requirements for Universal Broker.


5. Define the site configuration and home site associations for your Horizon Cloud tenant. See Configuring Sites for Universal Broker and Configuring Home Sites for Universal Broker.

6. Configure the multi-cloud assignments. See Pods in Microsoft Azure - Create a VDI Multi-Cloud Assignment.

**Working with Sites in a Universal Broker Environment**

You can use sites to help Universal Broker determine how to search for and allocate remote resources to your end users. A site is a collection of cloud-connected pods in the same physical location, typically in a single data center.

**Configuring Sites and Home Sites**

By default, a Horizon pod deployed on premises or in VMware Cloud on AWS is placed in monitored state. When you change a pod from monitored to managed state to support the creation of assignments, you are prompted to associate the pod with a new or existing site.

When you select Universal Broker as the brokering method for your pods in Microsoft Azure, it creates a default site called Default-Site. Participating pods in Microsoft Azure are automatically added to the Default-Site. Later, you can configure new sites and move pods from the Default-Site to a configured site.

You can also associate a user or a group of users with a specific site, called a **home site**.
Sites can serve as a useful part of a disaster recovery solution. For example, you can add pods in different data centers to different sites and entitle users and groups to an assignment that spans those sites. If a data center in one site becomes unavailable, Universal Broker can use desktops from an available site to fulfill user requests.

Use the Horizon Cloud Administration Console to configure sites and home sites. See Configuring Sites for Universal Broker and Configuring Home Sites for Universal Broker.

Using Sites to Define Desktop Search and Allocation Behavior

When a user accesses an assignment, Universal Broker searches for an available desktop from the pools participating in that assignment. By default, Universal Broker gives preference to the user's home site, the site physically closest to the user, and other sites, in that order.

For assignments that contain dedicated desktop pools, Universal Broker uses the default search behavior only the first time a user requests a desktop. After Universal Broker allocates a dedicated desktop in this first session, it returns the user directly to the same desktop in subsequent sessions.

You can modify the default search and allocation behavior for individual assignments by configuring site policies and home site overrides. For example, Universal Broker can give preference to the site physically closest to the user instead of the user's home site. Universal Broker can also restrict the scope of the search to desktops from a specific site.

You can also designate a home site override for an assignment. In this case, Universal Broker begins searching for available desktops in the override site instead of the user's home site.

You can configure site policy and home site override settings when you create an assignment, as described in Horizon Pods - Create a Multi-Cloud Assignment of VDI Desktops or Pods in Microsoft Azure - Create a VDI Multi-Cloud Assignment. You can also modify existing site policy and home site override settings by editing an assignment, as described in Edit a Multi-Cloud Assignment in Your Horizon Cloud Tenant Environment.

Note To resolve the physical locations of users, Universal Broker uses GeoLite2 data created by MaxMind, available from https://www.maxmind.com.

Configuring Sites for Universal Broker

You can use the Sites tab on the Capacity page to configure sites for Universal Broker. A pod must be associated with a site before it can participate in multi-cloud assignments brokered by Universal Broker.

When you change a Horizon pod from monitored to managed state, you are prompted to associate the pod with a new or existing site.

Pods in Microsoft Azure are automatically added to a default site called Default-Site. Later, you can configure new sites and move pods from the Default-Site to a configured site.

The Sites tab on the Settings > Capacity page shows the list of configured sites in your Universal Broker environment and reports the number of pods associated with each site.
Site-Level Actions Available on the Sites Tab

You can perform the following actions from the Sites tab.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New</strong></td>
<td>Click <strong>New</strong> to create a site in your Universal Broker environment. Enter values for <strong>Name</strong> and <strong>Description</strong>, and click <strong>Save</strong>. For example, enter <strong>San Francisco</strong> as the name of the site that corresponds to your data center situated in San Francisco. The newly created site is added to the Sites list.</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Select a site in the list and click <strong>Edit</strong> to modify the name and description of the site.</td>
</tr>
</tbody>
</table>
| **Delete** | The **Delete** action lets you remove a site permanently from your Universal Broker environment. Before you delete a site, clear the site of any associations with specific pods, users, or assignments:  
- Move each pod in the site to a different site by modifying the pod's site association. See Configuring the Site Association for a Pod.  
- Verify that:  
  - The site is not configured as the home site for any user or group. See Configuring Home Sites for Universal Broker.  
  - The site is not configured as the home site override for any multi-cloud assignment. See Edit a Multi-Cloud Assignment in Your Horizon Cloud Tenant Environment.  
  
**Note** If you have any multi-cloud assignments that use the deleted site as a home site or home site override, Universal Broker will have problems delivering desktops from these assignments.  
To delete a site permanently, select a site in the list and click **Delete**. |
Configuring the Site Association for a Pod

You can configure the site association for a pod by doing one of the following:

- When changing a Horizon pod from monitored to managed state, specify a new or existing site to associate with the pod. See Horizon Pods - Change a Pod to Managed State.

- Change the site association for either a Horizon pod or a pod in Microsoft Azure by editing the pod’s characteristics. Click the Pods tab on the Capacity page, select the pod in the list, and click Edit. See Pods — Available Pod-Level Actions.

Configuring Home Sites for Universal Broker

You can associate a user or a group of users with a specific site in a Universal Broker environment, called a home site. Home sites help you define how Universal Broker searches for and allocates desktops from multi-cloud assignments to your end users.

One use case for home sites involves managing the desktop allocation for roaming users and groups. For example, if a user has a home site in San Francisco but is visiting London, Universal Broker begins searching in the San Francisco site to fulfill the user’s desktop request rather than allocating a desktop closer to the user.

Introducing the Users and Groups Page

The Users and Groups page lists the users and groups who are entitled to multi-cloud assignments in your Universal Broker environment. The page also lets you assign a home site to a user or group.

To open the Users and Groups page, select Settings > Users and Groups.

The Users and Groups page reports the following information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Displays the name of the user or group.</td>
</tr>
<tr>
<td>Domain</td>
<td>Displays the Active Directory domain in which the user or group resides.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of user account.</td>
</tr>
<tr>
<td>Home Site</td>
<td>Displays the name of the home site associated with the user or group.</td>
</tr>
</tbody>
</table>
Actions Available on the Users and Groups Page

You can perform the following actions from the Users and Groups page.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>The New action lets you create a home site assignment that associates a home site with the selected user or group. See Configuring a Home Site Assignment.</td>
</tr>
<tr>
<td>Edit</td>
<td>Click Edit to change the home site associated with the selected user or group.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click Delete to remove the existing home site assignment from the selected user or group.</td>
</tr>
</tbody>
</table>

Configuring a Home Site Assignment

To associate a home site with a user or group, perform the following steps.


2. On the Users page of the wizard, specify the user or group that will receive the home site assignment.
   a. For Domain, specify the Active Directory domain in which the user or group resides.
      
      **Note** Only cloud-configured domains are available for selection.
   b. For Find Users, enter the first few characters of the user or group name, and select the user or group of users from the list that appears. Your selection is added to the Selected Users / User Groups list.
      
      **Note** To remove a user or group from the list, select the check box to the left of the user or group, and click Remove.

3. Specify the details of the home site assignment.
   a. Select the check box next to the user or group that will receive the home site assignment.
b Click **Assign Home Site** and select a site from the menu.

c Click **Next**.

4 Review the settings on the Summary page, and then click **Finish**.

The configured user or group appears in the Users and Groups list, with the associated home site indicated under the Home Site column.

### Horizon Pods - Enabling a Cloud-Connected Pod for Multi-Cloud Assignments

The Horizon Cloud Administration Console's Capacity page displays the current state of those Horizon pods that are connected to your Horizon Cloud tenant under the **State** column. In this release, a cloud-connected Horizon pod can be in either monitored or managed state. Only when the pod is in managed state can you use that pod's resources in multi-cloud assignments (MCAs).

#### Monitored State

Monitored state is the default state of a pod after you first connect the pod to your Horizon Cloud environment. The following list describes the features available for a pod in monitored state:

- The Dashboard page provides an overall health report on the components of a monitored pod. This page also displays information about resource usage, current user sessions, and connection statistics for the pod. See **Health Visibility and Insights into Your Cloud-Connected Pods Provided by the Cloud Monitoring Service in Horizon Cloud**.

- The Capacity page displays details about the pod such as its status, location, and state. See **Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types**.

- The console provides a user-based search feature from which you can perform help-desk operations to support your users. See **Chapter 3 Introducing the Cloud Monitoring Service's Unified Visibility, Health Monitoring, and Help Desk Features Provided in Horizon Cloud**.

#### Managed State

If a monitored pod meets certain requirements, you can change the pod's state to the managed state. See **Horizon Pods - Change a Pod to Managed State**.

A managed pod offers all the features available for a monitored pod. In addition, you can create multi-cloud assignments that use resources from a managed pod, and manage those multi-cloud assignments using the Horizon Cloud Administration Console. For more information, see **Managing Multi-Cloud Assignments in Your Horizon Cloud Tenant Environment**.
Horizon Pods - Change a Pod to Managed State

If a cloud-connected Horizon pod meets certain requirements, you can change the pod to managed state. Changing a pod to managed state lets you use the pod in multi-cloud assignments.

**Note** If you are selecting your very first Horizon pod for multi-cloud assignments and have enabled and configured Universal Broker for the first time, the **Configure Universal Broker for Pod** dialog box opens automatically after you finish configuring the Universal Broker settings. You can skip to step 3 of the following procedure to proceed with configuring the selected pod.

**Prerequisites**

- Ensure that the pod meets the requirements for Universal Broker, as described in **System Requirements for Universal Broker**.
- Install the Universal Broker plugin on every Connection Server instance within the pod. See **Horizon Pods - Install the Universal Broker Plugin on the Connection Server**.
- Configure each Unified Access Gateway instance within the pod. See **Horizon Pods - Configure Unified Access Gateway for Use with Universal Broker**.

  If you want to use two-factor authentication for Universal Broker, ensure that all Unified Access Gateway instances within the pod are configured with the same two-factor authentication settings. Also, ensure that these settings match the two-factor authentication settings on every Unified Access Gateway instance across all the other pods participating in multi-cloud assignments.

- Enable and configure Universal Broker for use with multi-cloud assignments. See **Select a Brokering Method for End-User Assignments** and **Configure Universal Broker**.

**Procedure**

1. Select **Settings > Capacity**. Select the **Pods** tab.
2. Select the pod in the list and then select **More > Change State**.

  The **Configure Universal Broker for Pod** dialog box appears.
Configure Universal Broker for Pod

Configuring Universal Broker will change the pod to a managed state so it can deliver assignments. The pod must have a unique FQDN, and must have the same 2-factor authentication settings as other pods that use Universal Broker.

<table>
<thead>
<tr>
<th>Site</th>
<th>New</th>
<th>Existing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod FQDN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. In the **Configure Universal Broker for Pod** dialog box, configure the pod's site association.
   - To associate the pod with a new site, select **New** and enter the name of the new site.
   - To associate the pod with an existing site, select **Existing** and select a site from the drop-down menu.

4. Enter the pod's unique FQDN. The FQDN is typically defined as follows:
   - If the pod has multiple Unified Access Gateway instances, specify the address of the local load balancer as the pod's FQDN.
   - If the pod has only one Unified Access Gateway instance, specify the address of that Unified Access Gateway instance as the pod's FQDN.

5. Click **Validate & Save**.

**Results**

The pod undergoes a validation process to ensure that it meets all the necessary configurations described in **System Requirements for Universal Broker**. If the pod passes the validation process, it is enabled for participation in multi-cloud assignments and the Capacity page displays the pod's state as **Managed**.

**Note** If the pod does not pass the validation process, a message appears with details describing the system configuration that is missing (for example, the Universal Broker plugin is not installed). Perform the necessary actions to correct the pod's configuration before you reattempt to change the pod to managed state.

**Horizon Pods - Change a Pod to Monitored State**

To change a Horizon pod from managed state to monitored state, you must first disconnect the pod and then redeploy it again to Horizon Cloud. After you redeploy the pod, it appears on the Capacity page in monitored state.
Procedure

1  Remove the pod from any desktop assignments that include that pod. For detailed instructions, see Edit a Multi-Cloud Assignment in Your Horizon Cloud Tenant Environment.

2  Disconnect the pod from Horizon Cloud. For detailed instructions, see Removing Cloud-Connected Horizon Pods from Use with Horizon Cloud.

   The pod is disconnected from Horizon Cloud, and the pod’s name disappears from the Capacity page.

   *Note* You do not need to perform the steps described in Clear the Cloud-Managed Properties from a Horizon Pod that was Offline During the Process to Disconnect it from Horizon Cloud.

3  Redeploy the pod to Horizon Cloud. For more information, see Deploying Pods Using the Capacity Page.

Results

The redeployed pod appears on the Capacity page in monitored state.

Creating and Managing Multi-Cloud Assignments in Your Horizon Cloud Tenant Environment

A multi-cloud assignment consists of a collection of desktop pools from one or more cloud-connected pods. Users and groups entitled to a multi-cloud assignment can access and use virtual desktops from the desktop pools in that assignment.

Horizon Pods - Preparing Desktop Pools for Multi-Cloud Assignments

To participate in a multi-cloud assignment, a desktop pool on a Horizon pod must be prepared with the mandatory settings required by Universal Broker. You can create a new desktop pool with these mandatory settings or you can modify an existing desktop pool to make it eligible for use with Universal Broker and multi-cloud assignments.

Horizon Pods - Create a New Desktop Pool for Multi-Cloud Assignments

Use the following steps to create and prepare a desktop pool on a Horizon pod that can be added to a multi-cloud assignment. To support the use of Universal Broker as the brokering technology for the multi-cloud assignment, you must configure the desktop pool with certain mandatory settings.

   *Note* Manual desktop pools are not eligible to participate in multi-cloud assignments.

Procedure

1  Log in to the Horizon Console user interface for any Connection Server instance in the target pod.
In Horizon Console, select **Inventory > Desktops**.

3 Click **Add**.

The Add Pool wizard appears.

4 To configure settings for the new pool, follow the prompts in the wizard. For detailed instructions, see *Setting Up Virtual Desktops in Horizon*, which is part of the *VMware Horizon documentation set* in Docs.vmware.com.

Configure the following mandatory settings.

a **Type** page: Select **Automated Desktop Pool** or **Manual Desktop Pool**.

b **vCenter Server** page: Select **Instant Clone** or **Full Virtual Machines**

c **User Assignment** page: Select **Floating** or **Dedicated**. If you select **Dedicated**, select **Enable automatic assignment**.

Do not configure any manual assignments of machines to users.

d **Desktop Pool Settings** page: Select **Cloud Managed**. Universal Broker only recognizes desktop pools marked as **Cloud Managed**.

![Add Pool wizard](image)

**Note** You cannot use Horizon Console to delete or disable a desktop pool configured as **Cloud Managed**.

e **Remote Display Settings** page: Select the default display protocol for the desktop pool.

f To configure additional settings for the pool, continue to follow the prompts in the wizard. When you are finished, click **Submit** to create the pool.

5 If you configured a dedicated pool for use in a Universal Broker environment, remove any user assignments from virtual machines included in the pool. For more information, see *Setting Up Virtual Desktops in Horizon*, which is part of the *VMware Horizon documentation set* in Docs.vmware.com.
What to do next

Proceed to **Horizon Pods - Create a Multi-Cloud Assignment of VDI Desktops**.

**Horizon Pods - Prepare an Existing Desktop Pool for Use in a Multi-Cloud Assignment**

Use the following steps to prepare an existing desktop pool in a Horizon pod for use in a multi-cloud assignment brokered by Universal Broker. Universal Broker only supports desktop pools configured with certain mandatory settings.

To use an existing desktop pool in multi-cloud assignments brokered by Universal Broker, you must configure the pool with the mandatory settings described in the following procedure. You must also remove all local entitlements from the pool and any user assignments from virtual machines included in the pool.

**Note** Manual desktop pools are not eligible to participate in multi-cloud assignments.

**Procedure**

1. Log in to the Horizon Console user interface for any Connection Server instance in the pod that includes the desktop pool.

2. In Horizon Console, select **Inventory > Desktops**. In the list, select the desktop pool that you want to use in multi-cloud assignments and click **Edit**.

   The Edit Pool wizard appears.

3. Click the **General** tab. Under **User Assignment**, select **Enable automatic assignment** (if this option is available for the pool type).
4. Click the **Desktop Pool Settings** tab and specify the following settings.
   
a. For **State**, select **Enabled**.
   
b. For **Connection Server restrictions**, click **Browse**, select **No Restrictions**, and then click **Submit**.
   
c. Under **General**, select **Cloud Managed**. Universal Broker only recognizes desktop pools marked as **Cloud Managed**.

5. To save the configuration and close the Edit Pool wizard, click **OK**.

6. To remove all local entitlements from the desktop pool, select the pool on the Desktop Pools page and select **Entitlements > Remove Entitlements**.

7. For a dedicated pool, remove any user assignments from virtual machines included in the pool. For more information, see *Setting Up Virtual Desktops in Horizon*, which is part of the VMware Horizon documentation set in Docs.vmware.com.

**What to do next**

Proceed to **Horizon Pods - Create a Multi-Cloud Assignment of VDI Desktops**.

**Horizon Pods - Remove a Desktop Pool from a Multi-Cloud Assignment**

To remove a desktop pool from a multi-cloud assignment configured on Horizon pods, you must perform the proper sequence of steps in the proper order. You must first modify the assignment containing the pool and then clear the **Cloud Managed** setting on the pool.
After you complete this sequence, the desktop pool becomes available for local entitlements configured in Horizon Console.

**Important** Always use the proper sequence of steps to remove a desktop pool from a multi-cloud assignment. Do not attempt to remove pools by manually clearing the Cloud Assigned setting in Horizon Console. If you manually clear Cloud Assigned, the pool still retains its association with the multi-cloud assignment and Universal Broker can still provision desktops from the pool to users requesting the assignment.

**Procedure**

1. In the Horizon Cloud Administration Console, edit the multi-cloud assignment that contains the desktop pool.
   a. In the left pane of the console, click **Assignments**. Select **On-Prem & VMware Cloud** from the Assignments menu.
   b. On the Assignments page, select the check box next to the assignment that contains the desktop pool and click **Edit**.
   c. In the Edit Desktop Assignment wizard, navigate to the Desktop page and deselect the desktop pool that you want to remove.
   d. Click **Finish**.

2. Log in to the Horizon Console user interface for any Connection Server instance in the pod that contains the desktop pool. Then modify the configuration settings for the pool.
   a. In Horizon Console, select **Inventory > Desktops**. The Edit Pool wizard appears.
   b. Select the desktop pool in the list and click **Edit**.
   c. Click the **Desktop Pool Settings** tab. Under **General**, verify that the Cloud Assigned setting is cleared.

   The Cloud Assigned setting is automatically cleared when you remove the pool from its multi-cloud assignment in the Horizon Cloud Administration Console.
d  Under **General**, clear the **Cloud Managed** setting.

The pool is now available for local entitlements in Horizon Console.

The following screenshot shows the configuration for a desktop pool that is available for local entitlements and no longer participates in multi-cloud assignments.

![Edit Pool - demo-static-pool](image)

<table>
<thead>
<tr>
<th>General</th>
<th>Desktop Pool Settings</th>
<th>Provisioning Settings</th>
<th>vCenter Settings</th>
<th>Guest Customization</th>
<th>Advanced Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Cloud Managed</td>
<td>□ Cloud Assigned</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connection Server restrictions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
</tr>
<tr>
<td>Category Folder:</td>
</tr>
</tbody>
</table>

| Cancel | OK |

e  Click **OK** to close the Edit Pool wizard.

**Creating Assignments in a Universal Broker Environment**

If you selected Universal Broker as your tenant-wide brokering method, you can create assignments of VDI desktops that span multiple cloud-connected Horizon pods deployed on premises or in VMware Cloud on AWS or that span multiple pods in Microsoft Azure. You can also create assignments of RDSH resources from pods in Microsoft Azure. When you entitle an assignment to your end users, Universal Broker searches for and allocates resources to those users based on the site configuration, user request, and desktop availability.

For instructions on creating VDI desktop assignments in a Universal Broker environment, see the subtopics under this documentation topic.

The process for creating RDSH resource assignments in a Universal Broker environment is the same as the process in a single-pod brokering environment.

- For instructions on creating an assignment of RDSH session desktops, see **Create an RDSH Session Desktop Assignment**.

- For instructions on creating an assignment of RDSH remote applications, see **Remote Applications - Create a Remote Application Assignment for Remote Applications Provisioned By Horizon Cloud Pods in Microsoft Azure**.
You can only create assignments of RDSH session desktops or remote applications from pods in Microsoft Azure. This release of Universal Broker does not support assignments of RDSH resources from Horizon pods.

When creating an assignment of RDSH resources, you can include session desktops from only a single pod in Microsoft Azure. This release does not support assignments of session desktops that span multiple pods in Microsoft Azure.

**Horizon Pods - Create a Multi-Cloud Assignment of VDI Desktops**

To provide end users with virtual desktops provisioned by on-premises Horizon pods or Horizon pods in VMware Cloud on AWS, you create a multi-cloud assignment. The desktop pools in an assignment can span one or more cloud-connected Horizon pods that are in managed state.

**Prerequisites**

- Change your cloud-connected Horizon pods to managed state. See [Horizon Pods - Enabling a Cloud-Connected Pod for Multi-Cloud Assignments](#).
- Configure sites and home site associations for your brokering environment, as described in [Configuring Sites for Universal Broker](#) and [Configuring Home Sites for Universal Broker](#).
- Using Horizon Console, configure desktop pools on the cloud-connected pods that you want to include in the assignment.

  See [Horizon Pods - Create a New Desktop Pool for Multi-Cloud Assignments](#) and [Horizon Pods - Prepare an Existing Desktop Pool for Use in a Multi-Cloud Assignment](#). Ensure that the desktop pools meet the configuration requirements for Universal Broker, as described in those topics.

**Procedure**

1. In the left pane of the console, click **Assignments**. If a submenu appears, select the option for VDI desktops.

2. On the Assignments page, select **New** and select the submenu option for pods deployed on premises or in VMware Cloud on AWS.

   The New Desktop Assignment wizard appears.
3 On the Definition page, configure the required settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Type</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Floating</strong>: In a floating assignment, a user receives a different virtual machine with a different machine name with each login. With floating assignments, you can create desktops that shifts of users can use and that are sized based on the maximum number of concurrent users. For example, 300 users can use an assignment of 100 desktops if they work in shifts of 100 users at a time. With floating assignments, the user might see different host names for each desktop session.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Dedicated</strong>: In a dedicated assignment, each virtual desktop gets mapped to a specific user. Each mapped user returns to the same desktop at every login. When a dedicated desktop is mapped to a specific user, that desktop is said to be assigned to that user.</td>
</tr>
<tr>
<td>Note</td>
<td>This setting becomes read-only when you are editing an existing assignment.</td>
</tr>
<tr>
<td>Desktop Name</td>
<td>Enter a user-friendly name for the assignment. Entitled end users might see a form of this assignment name in the client they use to access their desktops. The name must contain only letters, hyphens, and numbers. Spaces are not allowed. The name cannot start with a non-alphabetic character.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description for the assignment.</td>
</tr>
<tr>
<td>Select Pod(s)</td>
<td>Select the check box next to each pod containing desktop pools that you want to add to the assignment. You can select multiple pods to create an assignment of desktop pools from different pods.</td>
</tr>
<tr>
<td>Scope</td>
<td>To specify where the broker can search for desktops in response to a user's desktop request, select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Any Site</strong>: allows the broker to search for available desktops located in any configured geographic site.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Restrict to One Site</strong>: instructs the broker to search only for available desktops located in the user's default site, as specified by the <code>Site Connection Affinity</code> setting.</td>
</tr>
<tr>
<td></td>
<td>For an introduction to sites and desktop allocation, see <em>Working with Sites in a Universal Broker Environment</em>.</td>
</tr>
<tr>
<td>Site Connection Affinity</td>
<td>This setting specifies a certain geographic site as the default site for the user. When the user requests a desktop, the broker begins searching in the default site for available desktops. If no available desktops are found in the default site and no site restrictions are in effect, the broker continues searching for desktops beyond the default site. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Nearest Site</strong>: specifies the nearest geographic site as the default site for the user.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Home Site</strong>: specifies the user's home site (or the home site of the group that includes the user) as the default site for that user.</td>
</tr>
<tr>
<td></td>
<td>- To allow the user to access desktops beyond their configured home site, do not enable <code>Home Site Restriction</code>.</td>
</tr>
<tr>
<td></td>
<td>- To restrict the user to their configured home site when accessing desktops, enable <code>Home Site Restriction</code>.</td>
</tr>
<tr>
<td>Important</td>
<td>If you enable <code>Home Site Restriction</code>, the user (or the group that includes the user) must have a configured home site before they can access any desktops.</td>
</tr>
</tbody>
</table>

After you configure the Definition settings, click **Next** to proceed to the next page of the wizard.
On the Desktop page, specify the configuration properties and policies used to filter the desktop pools that can be added to the multi-cloud assignment.

For example, if you specify **Windows 10 (64-bit)** for Operating System and enable the **Allow Users to Restart VMs** policy, only desktop pools based on Windows 10 (64-bit) that have the **Allow Users to Restart VMs** policy enabled are available for inclusion in the assignment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Specify the operating system of the desktop pools that you want to include in the assignment.</td>
</tr>
<tr>
<td>Note</td>
<td>This setting becomes read-only when you are editing an existing assignment.</td>
</tr>
<tr>
<td>Default Display Protocol</td>
<td>Select the default display protocol of the desktop pools that you want to include in the assignment.</td>
</tr>
<tr>
<td>Allow Users to Choose Protocol</td>
<td>This policy filters desktop pools based on whether they allow users to select a display protocol other than the default.</td>
</tr>
<tr>
<td>Note</td>
<td>This setting becomes read-only when you are editing an existing assignment.</td>
</tr>
<tr>
<td>HTML Access</td>
<td>This policy filters desktop pools based on whether they allow users to connect to virtual desktops from a Web browser using the HTML Access client. For more information about this feature, see the VMware Horizon HTML Access Documentation.</td>
</tr>
<tr>
<td>Allow Users to Restart VMs</td>
<td>This policy filters desktop pools based on whether they allow users to restart virtual machines with a graceful operating system restart. This policy applies only to an automated pool or a manual pool that contains vCenter Server virtual machines.</td>
</tr>
<tr>
<td>Note</td>
<td>This setting becomes read-only when you are editing an existing assignment.</td>
</tr>
<tr>
<td>Clean Up Redundant Sessions</td>
<td>This policy specifies whether to close duplicate user sessions automatically. Duplicate sessions can occur when a pod that contains a session goes offline, the user logs in again and starts another session, and the problem pod comes back online with the original session. When duplicate sessions occur, Horizon Client prompts the user to select a session. This policy determines what happens to sessions that the user does not select. When this policy is disabled, users must manually close their own extra sessions, either by logging off in Horizon Client or by launching the sessions and logging them off.</td>
</tr>
<tr>
<td>Select Desktop Pools</td>
<td>Select the check box next to each desktop pool that you want to add to the assignment. You can add multiple pools to a single assignment. If you cannot find the desktop pool that you want in the list, verify the following:</td>
</tr>
<tr>
<td></td>
<td>- The desktop pool is not a manual pool. Manual desktop pools are not eligible to participate in multi-cloud assignments.</td>
</tr>
<tr>
<td></td>
<td>- The properties and policies of the desktop pool match the properties and policies that you specified for this multi-cloud assignment. For example, if you specified <strong>Windows 10 (64-bit)</strong> for Operating System and enabled the <strong>Allow Users to Restart VMs</strong> policy, the desktop pool must be based on Windows 10 (64-bit) and have the <strong>Allow Users to Restart VMs</strong> policy enabled.</td>
</tr>
<tr>
<td></td>
<td>- The desktop pool meets the configuration requirements for supporting Universal Broker, as described in Horizon Pods - Prepare an Existing Desktop Pool for Use in a Multi-Cloud Assignment.</td>
</tr>
</tbody>
</table>
After you configure the Desktop settings, click **Next** to proceed to the next page of the wizard.

5 On the Users page, specify the users and user groups that you want to entitle to the assignment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Specify the Active Directory domain in which the users and groups reside.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Only cloud-configured domains are available for selection.</td>
</tr>
<tr>
<td>Find Users</td>
<td>Type the first few characters of the user or group name, and select the users or group of users from the list that appears. Your selection is added to the <strong>Selected Users / User Groups</strong> list. You can use the <strong>Remove</strong> button to delete a selected user or group from the list.</td>
</tr>
<tr>
<td>Assign Home Site</td>
<td>Use this optional setting to configure a home site override for the selected user or group accessing this assignment. In this case, Universal Broker begins searching for available desktops in the override site instead of the user or group’s configured home site. For example, suppose that a user has a home site in San Francisco but you specify New York as the override site. When the user accesses the assignment, Universal Broker first searches for available desktops in New York instead of in San Francisco.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The <strong>Assign Home Site</strong> menu is available only if you selected <strong>Home Site</strong> for <strong>Site Connection Affinity</strong> on the Definition page of the wizard.</td>
</tr>
<tr>
<td></td>
<td>To specify a home site override, select the user or group and click <strong>Assign Home Site</strong>. The Assign Home Site menu displays all the available sites for pods participating in this assignment.</td>
</tr>
<tr>
<td></td>
<td>- To specify an override site as the default instead of the user or group’s configured home site, select the override site in the menu.</td>
</tr>
<tr>
<td></td>
<td>- To remove the override site and use the user or group’s configured home site instead, select <strong>Clear Home Site</strong>.</td>
</tr>
</tbody>
</table>

After you configure the Users settings, click **Next** to proceed to the next page of the wizard.

6 Review the settings on the Summary page, and then click **Finish**.

Results

The newly created assignment appears in the list on the Assignments page.

Each desktop pool included in the assignment is now marked as **Cloud Assigned** in the **Edit Pool** wizard in Horizon Console. You cannot use Horizon Console to delete or disable a desktop pool marked as **Cloud Assigned**.
If a Horizon Client user logs in to a floating desktop from a multi-cloud assignment, they might encounter a duplicate connection session, even when the Clean Up Redundant Sessions policy enabled. If the user attempts to log out manually from the duplicate session, they receive the error message “You do not have a current session from which to log off.” The error occurs because the duplicate session has already been closed through the assignment’s policy but Horizon Client does not yet reflect the session’s closed state. When the user closes the error message, the Horizon Client refreshes its display and the duplicate session is no longer visible.

**Pods in Microsoft Azure - Create a VDI Multi-Cloud Assignment**

You use the Assignment configuration wizard to create VDI multi-cloud assignments of desktops provisioned by multiple pods in Microsoft Azure.

**Prerequisites**

- Select and configure Universal Broker as the brokering method for your pods in Microsoft Azure. See Select a Brokering Method for End-User Assignments and Configure Universal Broker.

- Configure sites and home site associations for your brokering environment, as described in Configuring Sites for Universal Broker and Configuring Home Sites for Universal Broker.
- Verify that you have at least one published image, with a Microsoft Windows client operating system. You cannot create a VDI multi-cloud assignment without such an image. To verify, navigate to the Images page and make sure it lists an appropriate image. For steps on creating a published image, see Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

- Decide whether you want the desktops to have encrypted disks. You must specify disk encryption when creating the VDI multi-cloud assignment. You cannot later add disk encryption after the assignment is created. For a description of the disk capability, see Using Microsoft Azure Disk Encryption with Your Farms and VDI Desktops in Your Horizon Cloud Environment.

  **Important** This release does not support having disk encryption for floating VDI assignments that use image VMs with attached data disks. Make sure the image that you plan to use in the assignment does not have data disks.

- Decide whether you want the ability to use NSX Cloud features with the desktop VMs. You must enable NSX Cloud management when creating the VDI multi-cloud assignment. You cannot later enable the assignment for NSX Cloud management after the assignment is created. The published image you select for this assignment must have the NSX agent installed in it. You must have installed the NSX agent before publishing the image. See VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure and its subtopics.

  **Important** To use both NSX Cloud features and disk encryption, ensure the image's installed NSX agent is the latest agent version. Using disk encryption with previous versions of the NSX agent is not supported.

**Procedure**

1. In the left pane of the console, click **Assignments** and select the submenu option for VDI desktops.

2. On the Assignments page, click **New** and select the submenu option for desktops in Microsoft Azure.

   The New Desktop Assignment window opens to the first wizard step.

3. Select **Floating**.
4 On the Definition page, configure the required settings.

**Note** You might have to use the scroll bar to see all the settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Desktop Type</strong></td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Floating</strong>: In a floating assignment, a user receives a different virtual machine with a different machine name with each login. With floating assignments, you can create desktops that shifts of users can use and that are sized based on the maximum number of concurrent users. For example, 300 users can use an assignment of 100 desktops if they work in shifts of 100 users at a time. With floating assignments, the user might see different host names for each desktop session.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Dedicated</strong>: In a dedicated assignment, each virtual desktop gets mapped to a specific user. Each mapped user returns to the same desktop at every login. When a dedicated desktop is mapped to a specific user, that desktop is said to be assigned to that user.</td>
</tr>
</tbody>
</table>

**Note** This setting becomes read-only when you are editing an existing assignment.

<table>
<thead>
<tr>
<th>Assignment Name</th>
<th>Enter a user-friendly name for the assignment. Entitled end users might see a form of this assignment name in the client they use to access their desktops. The name must contain only letters, hyphens, and numbers. Spaces are not allowed. The name cannot start with a non-alphabetic character.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter an optional description for the assignment.</td>
</tr>
<tr>
<td>Select Pod(s)</td>
<td>Select the check box next to each pod containing desktop pools that you want to add to the assignment. You can select multiple pods to create an assignment of desktop pools from different pods.</td>
</tr>
</tbody>
</table>
### Setting Description

**Scope**

To specify where the broker can search for desktops in response to a user's desktop request, select one of the following options:

- **Any Site** allows the broker to search for available desktops located in any configured geographic site.
- **Restrict to One Site** instructs the broker to search only for available desktops located in the user's default site, as specified by the **Connection Affinity** setting.

For an introduction to sites and desktop allocation, see Working with Sites in a Universal Broker Environment.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Affinity</strong></td>
<td>This setting specifies a certain geographic site as the default site for the user. When the user requests a desktop, the broker begins searching in the default site for available desktops. If no available desktops are found in the default site and no site restrictions are in effect, the broker continues searching for desktops beyond the default site. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td><strong>Nearest Site</strong> specifies the nearest geographic site as the default site for the user.</td>
</tr>
<tr>
<td></td>
<td><strong>Home Site</strong> specifies the user's home site (or the home site of the group that includes the user) as the default site for that user.</td>
</tr>
</tbody>
</table>

**Note**  If you select **Home Site**, the **Assign Home Site** setting becomes available on the Users page in a later step of the wizard.

- To allow the user to access desktops beyond their configured home site, do not enable **Home Site Restriction**.
- To restrict the user to their configured home site when accessing desktops, enable **Home Site Restriction**.

**Important**  If you enable **Home Site Restriction**, the user (or the group that includes the user) must have a configured home site before they can access any desktops.

After you configure the Definition settings, click **Next** to proceed to the next page of the wizard.
5 On the Desktops page of the wizard, configure the required settings.

**Note** You might have to use the scroll bar to see all the settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Set one or more filters to control the models available in the <strong>Models</strong> drop-down menu. You can filter models by type, series, number of CPUs, memory, and tags. For more information about selecting models, see Managing VM Types and Sizes for Farms and Assignments, which describes the options on the VM Types &amp; Sizes page (<strong>Settings &gt; VM Types &amp; Sizes</strong>). To set a filter, you first select the criterion in the drop-down menu and then enter one or more desired values. By default, there is a single filter with the criterion 'Tag' the value 'VMware Recommended'. You can edit this first filter and add more filters connected by And and Or operators. The following are the criteria you can use for filters and descriptions of the values you can enter for each.</td>
</tr>
<tr>
<td></td>
<td><strong>Type</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Filter Models" /></td>
</tr>
<tr>
<td></td>
<td>When you select this option, there is only value available in the second drop-down menu:</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="GPU and High Performance - Models with GPU" /></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you select a GPU model (for example, Standard_NV6), then the list of images shown will contain only images that were created with the Include GPU flag selected, so you need at least one such image to create a farm or pool using a GPU model. If you select a non-GPU model, then the list of images shown will contain only images that were created without the Include GPU flag.</td>
</tr>
<tr>
<td></td>
<td><strong>Series</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Filter Models" /></td>
</tr>
<tr>
<td></td>
<td>When you select this option, you can then select a series of models from a second drop-down menu. You can also filter this list by entering text in the <strong>Filter</strong> text box at the top of the list.</td>
</tr>
<tr>
<td></td>
<td><strong>CPUs</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Filter Models" /></td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Setting</td>
<td>When you select this option, you can then enter a CPU range.</td>
</tr>
</tbody>
</table>

**Important** For production environments, to avoid unexpected end-user connection issues, use VM models that have a minimum of two (2) CPUs.

- **Memory**

- **Tag**

When you select this option, you can then select a tag from a second drop-down menu. You can also filter this list by entering text in the Filter text box at the top of the list. Tags available in the drop-down menu are both hard-coded system tags and custom tags that you created on the VM Types & Sizes page ([Settings > VM Types & Sizes](#)). You can set additional filters by performing the following steps for each filter:

  a. Click the + link.
  b. Select either And or Or as the operator between the previous filter and the new one you are creating.
  c. Set the new filter by selecting a criterion and entering values.

**Model**

Select the model to use for the desktop instances. The menu only displays model choices that are available in all the selected pods participating in the assignment. This selection defines the set of underlying resources that are used when the desktop instances are created, in terms of capacity (compute, storage, and so on).

**Important** For production environments, select a VM model that has a minimum of two (2) CPUs. VMware scale testing has shown that using 2 CPUs or more avoids unexpected end-user connection issues. Even though the system does not prevent you from choosing a VM model with a single CPU, you should use such models for tests or proof-of-concepts only.

**Disk Type**

Select a supported disk type from the available options. The menu only displays disk type options that are available in all the selected pods participating in the assignment. Disk type options are based on the model selected, and your Azure subscription and region. The following are some commonly available disk types:

- Standard HDD - Default disk type.
- Standard SSD
- Premium SSD - Option only appears if you selected a model that supports premium I/O.

You can edit your selection after creating the assignment if necessary.
### Setting | Description
--- | ---
**Disk Size** | Enter the OS disk size in GB for the VMs in this assignment.  
- The default value is the base image OS disk size (typically 128 GB).  
- If you edit the size, the value you enter must be greater than the base image OS disk size, and cannot exceed the largest size (typically 1024 GB) supported by the selected model.  
- You can also edit this value later.  

**Important** If you edit the disk size, there are additional actions you must take to ensure that the VMs are created as expected. For more information, see [Required Administrator Actions When the Disk Size for a Farm or VDI Desktop Assignment is Increased](#).

**OS System** | Specify the operating system of the VMs that you want to include in the assignment.

**Domain** | Select the Active Directory domain registered with your environment.

**Encrypt Disks** | Select Yes if you want the desktop instances to have encrypted disks.  

**Important**  
- If you want disk encryption, you must make this selection when creating the VDI multi-cloud assignment. You cannot later add disk encryption after the assignment is created.  
- To use both NSX Cloud features and disk encryption, the image's installed NSX agent must be the latest agent version. Using disk encryption with previous versions of the NSX agent is not supported.

**NSX Cloud Managed** | Select Yes if you want to use features of NSX Cloud with the assignment’s desktop instances. For a description of using NSX Cloud features with your desktops in Microsoft Azure, see [VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure](#) and its subtopics.  

**Important**  
- If you want to use NSX Cloud with the desktop instances, you must make this selection when creating the VDI multi-cloud assignment. You cannot later enable NSX Cloud management after the assignment is created.  
- For the NSX Cloud management features to work with the assignment’s desktop instances, the image that you select for this assignment must have the NSX agent already installed on it. When you set this toggle to Yes, ensure that the image you select in Image has the NSX agent installed on it. The system does not verify if the selected image has the NSX agent when it creates the assignment.  
- To use both NSX Cloud features and disk encryption, the image's installed NSX agent must be the latest agent version. Using disk encryption with previous versions of the NSX agent is not supported.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Image**        | Select the image on each pod that you want to assign to end users. To view information about the selected image, click Details. Only those published images in each pod corresponding to the OS System selection are listed here. A published image, sometimes called a sealed image or an assignable image, is one that was published to the system by converting a golden image into a desktop.  
  
  **Note** If the error message "Please select a valid image to continue" appears when you attempt to select an image, there might be a problem with the image. Go to Inventory > Images to view the status of the problem image and perform the suggested remediation procedure.  
  
  Since you can select a different image to use for each pod participating in the assignment, end users might receive different session experiences based on how Universal Broker allocates resources from the assignment. For example, one user might receive a desktop from Pod A which uses a specific image. However, another user who receives a desktop from Pod B might have a different session experience based on the desktop image used by Pod B.  
  
  **Important**  
  - If you set the Encrypt Disks to Yes, ensure that the image you select here does not have data disks attached to it. Use of disk encryption of VMs with data disks for floating VDI assignments is not supported in this release.  
  - If you set the NSX Cloud Managed toggle to Yes, ensure that the image you select here has the NSX agent installed on it. For the NSX Cloud management features to work with the assignment's desktop instances, the image that you select for this assignment must have the NSX agent already installed on it. The system does not verify if the selected image has the NSX agent when it creates the VDI desktop assignment. |
| **VM Names Prefix** | Base name for the desktop VMs created in this assignment. The VM names have numbers appended to this base name, for example, win10-1, win10-2. The name must start with a letter and can contain only letters, dashes, and numbers. The end users see this name when they go to access a desktop from this assignment. For example, when an end user runs Horizon Client to use one of the desktops, this name is the one displayed in Horizon Client. |
| **Default Protocol** | Select a default display protocol you want the end-user sessions to use. Circumstances might occur that cause another protocol to be used instead of the default protocol. For example, the client device does not support the default protocol or the end user overrides the default protocol selection.  
  
  **Note** For images with the Microsoft Windows 7 Enterprise operating system, RDP is the only supported choice. |
| **Preferred Client** | Select the preferred client used when end users start their desktops from the Workspace™ ONE™ platform's portal, either a Horizon Client or a browser for HTML Access.  
  
  **Note** For images with the Microsoft Windows 7 Enterprise operating system, Horizon Client is the only supported choice. |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you have a Windows Client</td>
<td>The wizard asks you to confirm you have an eligible license to use the Microsoft Windows operating system that is in the image and which will be in the desktop VMs. Follow the on-screen instructions. For a client operating system, Horizon Cloud sets the assignment’s desktop VMs to use the Windows Client license type by default and you cannot change that setting.</td>
</tr>
<tr>
<td>License</td>
<td></td>
</tr>
<tr>
<td>Power Off Protect Time</td>
<td>Specify the number of minutes that you want the system to wait before automatically powering off a powered-on desktop. You can enter a value from 1 to 60. The default is 30 minutes. This protect time is used primarily for the situations where the system will automatically power off a desktop VM. You can use this Power Off Protect Time setting to tell the system to wait the specified time before starting to power off the VM to meet the threshold setting in the Power Management field. The system waits the time specified for the Power Off Protect Time before powering off the VM to match the configured schedule. The default wait time is 30 minutes.</td>
</tr>
</tbody>
</table>
Optionally configure the advanced properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer OU</strong></td>
<td>Active Directory Organizational Unit where the desktop VMs are to be located. Enter the Active Directory Organizational Unit using the distinguished name, for example, ou=RootOrgName,DC=DomainComponent,DC=eng, and so on. The OU and each path in a nested OU can contain any combination of letters, numbers, special characters, and spaces, and can have a maximum of 64 characters. If you must use nested Organization Units, see Considerations For Using Nested Active Directory Domain Organizational Units.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If the Computer OU is set to CN=Computers, the system uses the default Active Directory Computers container for VMs. Your Active Directory might have this default container redirected to an organizational unit class container.</td>
</tr>
<tr>
<td><strong>Run once script</strong></td>
<td>(Optional) Location of a script that you want run in the assignment's desktop VMs after the VM creation process.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The script must end with a reboot step to reboot the VM. Otherwise, the end user will not be able to log in the desktop until doing a manual restart. A sample reboot line as a Windows command is: shutdown /r /t 0</td>
</tr>
<tr>
<td></td>
<td>The reason why the script must end with a reboot step is due to the sequence when the script is run after the sysprep process. When the system creates a desktop VM for the assignment, the VM boots up and completes the sysprep process in the Windows operating system. When the sysprep process completes, the agent in the desktop VM reaches out to do the domain join. At the same time, the agent gets the script path you specify here. The agent sets the Windows RunOnce path (System run once) and then restarts the desktop VM. On the next restart, the system logs in to the Windows operating system using the local administrator account and runs the script. It is only after another subsequent restart, specified in the script, that the desktop VM is ready for a user to log in.</td>
</tr>
<tr>
<td><strong>Log off Disconnected Sessions</strong></td>
<td>Specify when you want the system to log the user out of a disconnected desktop session.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The sessions governed by the Log off Disconnected Sessions, Session Timeout Interval, and Max Session Lifetime settings are the user logins to the desktops' Windows operating system. These sessions are not the user logins in Horizon Client, Horizon HTML Access, or Workspace ONE.</td>
</tr>
<tr>
<td></td>
<td>The user’s session begins when the user authenticates to the desktop’s Windows operating system.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Session Timeout Interval</strong></td>
<td>This time interval is the amount of time the end users' sessions can be idle before the system forces a log out from the desktops. This time-out applies to the logged-in session to the underlying Windows operating system. The time you specify here is different from the time-out settings that govern the end users' Horizon Client or HTML Access logged-in session.</td>
</tr>
<tr>
<td><strong>Caution</strong></td>
<td>When the system forces the log-off in the underlying Windows operating system session, any unsaved data is lost. To prevent an unintended loss of data, set this interval high enough to accommodate the business needs of your end users.</td>
</tr>
<tr>
<td></td>
<td>The default interval is one week (10080 minutes).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If no user activity occurs before the timeout interval is reached, a message appears in the desktop that indicates that the user will be logged off if they do not click <strong>OK</strong> in the next 30 seconds. If the logout occurs, any unsaved user data, such as documents or files, is lost.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Max Session Lifetime</strong></td>
<td>Specify the maximum number of minutes the system should allow for a single user session.</td>
</tr>
</tbody>
</table>
## Power Management Mode

**Note** This setting is only available if you have set the desktop type to *Floating*.

The power management settings are related to the thresholds at which the system automatically increases and shrinks the number of powered-on desktop instances in the floating VDI desktop assignment according to usage. When the usage increases above an upper bound, the system powers up a new desktop instance. When the usage shrinks below a lower bound, the system shuts down deallocates desktop VMs as end users log out from the desktops.

The power management selections balance capacity cost with faster availability:

- **Select Optimize for Performance** when you want the system to power on the next desktop instance sooner rather than later. Even though you are spending more by having the next desktop ready to go before the user demand requires it, this setting increases the chance that when users try to start a desktop from the assignment, the desktop is already powered up to meet that demand.

- **Select Optimize for Power** when you want the system to wait as long as possible before powering on the next desktop instance. The occupancy of the assignment’s set of desktops is higher before the system powers up the next desktop instance. Even though this selection minimizes capacity costs by having more utilization of the existing desktops, this setting increases the chance that there might be a delay when new users try to log in because they might have to wait during the time system has to power on desktops.

- **Select Balanced** to strike a balance between capacity costs and time-to-availability for users.

The low and high thresholds for each selection are:

- **Optimize for Performance**
  - Low threshold: 23%
  - High threshold: 50%

- **Optimize for Power**
  - Low threshold: 38%
  - High threshold: 80%

- **Balanced**
  - Low threshold: 31%
  - High threshold: 66%

## Azure Resource Tags

(Optional) Create custom tags to be applied to Azure resource groups. Azure resource tags are only applied to the resource groups, and are not inherited by the resources in the groups.

To create the first tag, enter information in the Name and Value fields. To create an additional tag, click **Add** and then enter information in the Name and Value fields that appear below the existing ones.

- You can create a maximum of 10 tags.
- The tag name is limited to 512 characters, and the tag value is limited to 256 characters. For storage accounts, the tag name is limited to 128 characters, and the tag value is limited to 256 characters.
- Tag names cannot contain the following characters:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>&lt; &gt; % &amp; \ ? /</code></td>
</tr>
<tr>
<td></td>
<td>Tag names cannot contain these case-insensitive strings:</td>
</tr>
<tr>
<td></td>
<td>‘azure’, ‘windows’, ‘microsoft’</td>
</tr>
<tr>
<td></td>
<td>After an assignment has been created, you can add more Azure resource tags</td>
</tr>
<tr>
<td></td>
<td>and edit or delete tags for that assignment.</td>
</tr>
</tbody>
</table>

After you configure the Desktop settings, click **Next** to proceed to the next page of the wizard.
On the Capacity page of the wizard, make the following settings.

a If you are creating a dedicated VDI desktop assignment, click **Global Configuration for all Pods** and configure settings that apply to all pods.

**Note** If there are pods listed that are on manifest versions older than October 2020, these settings do not apply to them and a message appears indicating that. The manifest version number for October 2020 is found in the *Horizon Cloud Service Release Notes*.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Desktop Deletions</td>
<td>This sets the number of desktop VMs that can be deleted in the assignment before counting them against the rate you set for Deletion Protection. Select one of the following options from the drop-down menu.</td>
</tr>
<tr>
<td></td>
<td>■ Unlimited - Unlimited desktop VMs can be deleted from the assignment. In this case, the Deletion Protection setting is no longer relevant.</td>
</tr>
<tr>
<td></td>
<td>■ None - No additional desktop VMs can be deleted before counting them against the rate you set for Deletion Protection. In this case, the system uses only the Deletion Protection to authorize or block deletions. None is the default value for Deletion Protection.</td>
</tr>
<tr>
<td></td>
<td>■ Custom - Number of additional desktop VMs that can be deleted before counting them against the rate you set for Deletion Protection. If you select Custom, you must also enter a numerical value for Custom Delete Count.</td>
</tr>
<tr>
<td></td>
<td>For example, you might set Max Desktop Deletions to 10 and Deletion Protection to 1. In this case, after the first 10 VMs are deleted (no matter how long it takes for the count to reach 10), the system only allows 1 additional VM to be deleted per hour from that time forward.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> If you specify a new image for a dedicated desktop assignment, the system changes the Max Desktop Deletions setting if necessary so that all unassigned desktop VMs can be rebuilt with the new image.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you select Unlimited for Deletion Protection, there is no need to use the Max Desktop Deletions setting.</td>
</tr>
<tr>
<td>Custom Delete Count</td>
<td>If you selected Custom for Max Desktop Deletions, enter the number of additional desktop VMs that can be deleted before counting them against the rate you set for Deletion Protection. The number you enter must between 1 and 2000.</td>
</tr>
</tbody>
</table>

For more information about the Deletion Protection setting, see *Customizable General Settings for Your Horizon Cloud Tenant Environment*.

To prevent all VM deletions in a dedicated desktop assignment, use the Prevent Deletions setting on the Assignments page. See *Prevent Deletions or Allow Deletions for a Multi-Cloud Dedicated Desktop Assignment*. 
**Note** Settings that you make here can be overridden for a particular pod in the next step below.

b Configure the required settings for each participating pod by clicking the arrow icon next to the pod in the pod list.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Power Management Schedule</strong></td>
<td>To help optimize savings and performance of the desktop VMs in Microsoft Azure, you can optionally configure schedules to adjust the minimum number of powered-on desktop instances on a recurring weekly basis.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> In a Floating assignment, you can manage any of the desktop instances using the power management schedule. In a Dedicated assignment, you can only manage unassigned desktop instances with the schedule.</td>
</tr>
</tbody>
</table>

For example:

- For weekends or night hours when you know that your end users will not be using their desktops, you can have a schedule for zero or a low number of powered-on desktops (for a Floating assignment) or powered-on unassigned desktops (for a Dedicated assignment).

- For specific days or specific hourly stretches that you can predict will have increased end user demand, you can have a schedule that increases the minimum number of powered-on desktops to be available to meet that demand.

You can specify up to 10 schedules for the assignment. If any schedules have overlapping time periods but specify different minimum desktop numbers, the system uses the largest value of minimum desktops for the overlapping time period.

1 Click the calendar icon under the Min Desktops column to open the **Add Power Management Schedule** screen for that pod.
2 Select the days for the first schedule.
3 Specify the applicable hours in the specified days. Either:
   - Select the **All Day** check box to have this schedule in effect for all hours of the specified days.
   - Specify start and end times for the time period in each day.

**Note** Encrypted VMs take longer to power on than non-encrypted VMs. If you have set Encrypt Disks to Yes, and you want 100% of the encrypted VMs to be ready for end-user connections at a particular time of day, you might have to set an earlier start time here. See **When Scheduling Power Management for Farms and VDI Desktop Assignments That Have Large Numbers of Encrypted VMs**.

4 Select the time zone. The time zone closest to your end users’ location is recommended. As appropriate for the selected time zone, Daylight Savings Time is automatically applied.
Option | Description
---|---
**Note** | If two schedules have the same time zone setting and have overlapping times, a warning is displayed. However, if two schedules have different time zone settings and overlap, the warning is not displayed. As an example, if you have two all-day Saturday schedules and one has **Europe/London** time zone selected and the other has **America/Toronto** selected, the overlap warning does not display.

5 | In the **Min Desktops** field, type the minimum number of desktops you want powered on during the specified time period. During the specified time period, that number of desktops at a minimum will be powered on to be available to take end user requests during that time.

- In a **Floating** assignment, this number can range from zero (0) up to the number specified for **Max Desktops** for the pod.
- In a **Dedicated** assignment, this number can range from zero (0) up to the total number of unassigned desktop instances for the pod.

When this number is zero (0) and there are no active end user sessions at the schedule's starting time point, the pod's desktops are powered off. In that scenario, if an end user later attempts to connect to a desktop from this assignment during the scheduled time period, there will be a delay before the desktop is in a usable state because the underlying desktop VM has to power on.

6 | To create additional power management schedules, click **Add Schedule**.

**Note** | By default, when a user logs out from a desktop at a time that lies outside of a schedule's time period, the system protects the desktop VM from powering off for the time specified in the **Power Off Protect Time** field. The default is 30 minutes.

**Min VMs**
**Max VMs**

Specify the minimum number and maximum number of desktops you want in this assignment. When the assignment is first created, the system deploys the number of desktops specified in the **Max VMs** setting, and then powers off the desktops except the number specified for **Min VMs**.

Only the minimum number of desktop instances is initially powered on. As end-user demand increases, the system powers on additional desktops, up to the **Max VMs** number. Then as end-user demand shrinks, the system powers off the desktops, until it reaches the **Min VMs** number.

A desktop must be free of a logged-in user session before the system will power it off.

When you specify zero (0) for **Min VMs**, it indicates that you want the system to power off all the assignment's desktops until there is end-user demand for a desktop.

**Quiescing VMs**

This setting controls the number of unassigned desktops in this dedicated VDI desktop assignment that can be concurrently quiesced during the time the assignment's image is being updated. For example, when you later edit this dedicated VDI desktop assignment to use another image, the system will power off at the same time this number of unassigned desktops. Then the system performs the required actions to provision the new image to that set of powered-off unassigned desktops.
Option | Description
--- | ---
**Note** | Desktops in a dedicated VDI desktop assignment that are mapped to users are said to be assigned to those users. Unassigned desktops in a dedicated VDI desktop assignment are desktops which have not yet been mapped to specific users.

**Max Desktop Deletions** | This option appears for dedicated VDI desktop assignments only. See the description in the table above. Changes you make here override any settings for all pods you made in the previous step.

**Custom Delete Count** | This option appears for dedicated VDI desktop assignments only. See the description in the table above. Changes you make here override any settings for all pods you made in the previous step.

After you configure the Capacity settings, click **Next** to proceed to the next page of the wizard.

7. On the Users page, specify the users and user groups that you want to entitle to the assignment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Domain** | Specify the Active Directory domain in which the users and groups reside.  
**Note** | Only cloud-configured domains are available for selection.  

| **Find Users** | Type the first few characters of the user or group name, and select the users or group of users from the list that appears.  
Your selection is added to the **Selected Users / User Groups** list. You can use the **Remove** button to delete a selected user or group from the list. |

| **Assign Home Site** | **Note** | This setting is available only if you selected **Home Site** for **Connection Affinity** on the Definition page of the wizard.  
Use this optional setting to configure a home site override for the selected user or group accessing this assignment. In this case, Universal Broker begins searching for available desktops in the override site instead of the user or group’s configured home site.  
For example, suppose that a user has a home site in San Francisco but you specify New York as the override site. When the user accesses the assignment, Universal Broker first searches for available desktops in New York instead of in San Francisco.  
To specify a home site override, select the user or group and click **Assign Home Site**. The Assign Home Site menu displays all the available sites for pods participating in this assignment.  
- To specify an override site as the default instead of the user or group’s configured home site, select the override site in the menu.  
- To remove the override site and use the user or group’s configured home site instead, select **Clear Home Site**. |

After you configure the Users settings, click **Next** to proceed to the next page of the wizard.

8. On the Summary page, review the configuration and then click **Finish**.
Results

The system begins the process of configuring the desktop instances to provide VDI desktops to the selected users.

**Note** Creation of an encrypted desktop VM takes approximately twice as long as creating a non-encrypted VM. As a result, the end-to-end time to complete creating a VDI desktop assignment that has disk encryption enabled is approximately twice as long as creating that VDI desktop assignment without disk encryption enabled.

What to do next

If the image for this floating VDI desktop assignment has applications that require opening special ports, you might need to modify this assignment’s associated Network Security Group (NSG) in Microsoft Azure. For details about the NSG, see About Network Security Groups and Your VDI Desktops.

If you specified NSX Cloud management for this assignment, you can use your NSX Cloud environment’s Service Manager (CSM) to see that the desktop VMs are managed in NSX Cloud. Log in to your environment’s CSM and navigate to Clouds > Azure > Instances. When that Instances page shows a status of Managed for the desktop instances, you can start implementing NSX policies on them.

Pods in Microsoft Azure - View Details About a VDI Multi-Cloud Assignment

You can use the Assignments page and its detailed subpages to monitor the status of a VDI multi-cloud assignment based on pods in Microsoft Azure.

**Information on the Assignments Page**

The following columns on the main Assignments page provide useful information about a VDI multi-cloud assignment. To show optional columns, use the customization button at the bottom left of the Assignments page.

<table>
<thead>
<tr>
<th>Information Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration</strong></td>
<td>Indicates the current progress of a request to change the assignment configuration. A configuration change can involve the creation of a new assignment or the editing or deletion of an existing assignment. When the change request has been propagated across all the participant pods in the assignment, this column displays the Complete status.</td>
</tr>
<tr>
<td><strong>Health</strong></td>
<td>Indicates the assignment’s state of readiness. While the assignment undergoes configuration changes, such as when desktops are provisioned from participant pods during the creation of an assignment, this column displays the In Progress status with cycling arrows. To view details about the task in progress, click the assignment’s name to open the assignment details page as described in the next section of this topic. When all configuration tasks on all participant pods are complete and the assignment is ready for use, this column shows the Online status with a green checkmark.</td>
</tr>
<tr>
<td><strong>Site</strong></td>
<td>Hovering over this column displays a list of all the sites associated with participant pods in the assignment.</td>
</tr>
</tbody>
</table>
### Information Column Description

<table>
<thead>
<tr>
<th>Information Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod</td>
<td>This column displays the total number of pods participating in the assignment. Hovering over this column displays a list of all the participant pods.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Total capacity of the assignment, expressed as an integer value. This value is calculated as the sum of the maximum number of virtual machines provided by all desktop pools associated with the assignment. For example, suppose that the assignment includes four desktop pools, and each of these desktop pools provides a maximum of one virtual machine (VM). The total capacity is calculated as follows: ((\text{Maximum VM count for the first desktop pool}) + (\text{maximum VM count for the second desktop pool}) + (\text{maximum VM count for the third desktop pool}) + (\text{maximum VM count for the fourth desktop pool}) = 1+1+1+1 = 4).</td>
</tr>
<tr>
<td>User Group</td>
<td>This optional column indicates the total number of user groups that are entitled to the assignment.</td>
</tr>
<tr>
<td>Occupancy</td>
<td>This optional column indicates the used or assigned portion of the assignment’s total capacity, expressed as a percentage value. The occupancy is based on users logged in through both global entitlements (such as this VDI multi-cloud assignment) and local entitlements at the pod level. - The occupancy for a floating assignment is calculated by first summing up the number of logged-in user sessions (including sessions in connected, disconnected, and idle states) across all the floating desktop pools in the assignment. The sum of user sessions is then divided by the total capacity to yield a fractional value. Finally, the fractional value is multiplied by 100 to obtain the occupancy percentage. - The occupancy for a dedicated assignment is calculated by first totaling the number of assigned virtual machines from all the dedicated desktop pools in the assignment. The total is divided by the total capacity to yield a fractional value and then multiplied by 100 to obtain the occupancy percentage. For example, suppose that a floating assignment includes four desktop pools, for a total capacity of 4. There are two user sessions currently active. The occupancy equals ((2/4)*100 = 50%).</td>
</tr>
</tbody>
</table>

### Information on the Assignment Details Page

To view more information about the health status of an assignment, click the assignment’s name on the main Assignments page to open the assignment details page.

On the **Summary** tab of the assignment details page, you can view a list of the participant pods, including the individual health status of each pod.

<table>
<thead>
<tr>
<th>Pods</th>
<th>Health</th>
<th>Configuration</th>
<th>Pod</th>
<th>Site</th>
<th>Region</th>
<th>Available Agents</th>
<th>Platform</th>
<th>No. of Machines</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Complete" /></td>
<td>McaAzurePod1</td>
<td>Bengaluru</td>
<td>-</td>
<td>-</td>
<td>Azure</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><img src="image2" alt="Complete" /></td>
<td>McaAzurePod2</td>
<td>Bengaluru</td>
<td>-</td>
<td>-</td>
<td>Azure</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To view more details about the health status of a pod, click the **System Activity** tab and select the name of the pod from the drop-down menu. The System Activity tab displays a list of current and recent tasks running on the pod and the status of each task. Clicking a task description in the list displays further details about the task’s processes.
If the pod has a problem condition, a description of the problem appears in the System Activity tab. In this case, you can use the information to troubleshoot the problem condition and bring the assignment's Health status back to Online.

**Considerations for Assignments in a Universal Broker Environment When a Pod Goes Offline**

When working with end-user assignments in a Universal Broker environment, you may experience limited availability of resources in an assignment if one of its participating pods loses connectivity and goes offline.

You may encounter the following situations when working with end-user assignments in a Universal Broker environment.

**Floating VDI Assignments**

- If a floating VDI assignment includes desktops from multiple pods and one or more participating pods go offline, Universal Broker allocates desktops from the remaining online pods to fulfill users' requests, provided that the requests do not exceed maximum capacity.

- If a participating pod in a floating VDI assignment goes offline and then comes back online later, the end user may see multiple connection sessions for that assignment across multiple pods. The multiple instances typically represent the earlier session established with the pod that went offline and a later session allocated from a different online pod to fulfill the user's request. When the user selects one of the sessions, the other session is automatically logged off.

**Dedicated VDI Assignments**

- If an end user has received a dedicated desktop from a dedicated VDI assignment and the pod containing that desktop goes offline, the user loses access to the desktop. The user regains access to the desktop only when the pod comes back online.

- If an end user has not received a dedicated desktop yet from the assignment and one or more participating pods go offline, Universal Broker allocates a desktop from one of the remaining online pods to fulfill the user's request, provided that the request does not exceed maximum capacity.
RDSH Session Desktop and Applications Assignments

- If a pod participating in an RDSH assignment goes offline, you cannot access the assignment or any of the included session desktops in Horizon Cloud Administration Console. Although end users can still see the session desktops in the assignment, any attempt to open a connection session with a desktop will fail. The assignment and session desktops will become available again in the console and to end users when the pod comes back online.

- If an RDSH assignment includes applications from a participating pod that goes offline, you cannot access those particular applications in the console. Although end users can still see remote applications from the offline pod, any attempt to start a session with these applications will fail. Applications in the assignment from pods other than the offline pod remain available in the console and to end users. Applications from the offline pod will become available again in the console and to end users when the pod comes back online.

Managing Multi-Cloud Assignments in Your Horizon Cloud Tenant Environment

You can perform several actions on the assignments listed on the Assignments page.

**Note**  Horizon Universal Console does not restrict you from using Horizon Console to edit desktop pools associated with a multi-cloud assignment. Horizon Universal Console also does not sync its desktop pool data with data from Horizon Console. Therefore, Horizon Universal Console might display inconsistent information about assignments at times.

For example, if you use Horizon Console to delete a desktop pool associated with an assignment, Horizon Universal Console still displays the deleted desktop pool as part of the assignment. To resolve this consistency, manually delete the desktop pool from the assignment using the Edit Desktop Assignment wizard.

**Actions You Can Perform on the Assignments Page**

At a page level, you can perform the following actions on the listed assignments.

**New**

Clicking this button starts the New Desktop Assignment wizard, which guides you through the steps to create a desktop assignment. For instructions on how to use the wizard, see Horizon Pods - Create a Multi-Cloud Assignment of VDI Desktops.

**Edit**

You can select the check box next to an existing desktop assignment and click this button to start the Edit Desktop Assignment wizard. This wizard lets you change certain configuration options for the desktop assignment. The wizard is similar to the New Desktop Assignment wizard, with read-only settings for those options that cannot be changed for an existing desktop assignment.

**Delete**
You can select the check box next to an existing desktop assignment and click this button to delete the assignment. A message appears asking you to confirm the action. To delete the desktop assignment permanently, click **Delete** in the confirmation message. For more information, see [Delete a Multi-Cloud Assignment from Your Horizon Cloud Environment](#).

The desktop pools included in an assignment remain intact after the assignment is deleted.

**Information and Actions on a Desktop Assignment's Detailed Pages**

For desktop assignments, you can perform actions specific to those assignment types from within the assignment's detailed pages. To see these detailed pages, locate the assignment within the console's assignment-related pages and click its name. Initially the Summary page is displayed.

**Summary page**

- Capacity and Usage

  The Summary page shows information about the current capacity and usage of the desktop assignment.
<table>
<thead>
<tr>
<th>Usage Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktops</td>
<td>Total capacity of the desktop assignment, expressed as an integer value. This value is calculated as the sum of the maximum number of virtual machines provided by all desktop pools associated with the desktop assignment. For example, suppose that the desktop assignment includes four desktop pools, and each of these desktop pools provides a maximum of one virtual machine (VM). The Desktops capacity is calculated as follows: ((\text{Maximum VM count for first desktop pool}) + (\text{maximum VM count for second desktop pool}) + (\text{maximum VM count for third desktop pool}) + (\text{maximum VM count for fourth desktop pool}) = 1+1+1+1 = 4.)</td>
</tr>
<tr>
<td>Occupancy</td>
<td>The used or assigned portion of the total Desktops capacity, expressed as a percentage value. The Occupancy is based on users logged in through both global entitlements (such as the Horizon Cloud desktop assignment) and local entitlements. The Occupancy for a floating desktop assignment is calculated by first summing up the number of logged-in user sessions (including sessions in connected, disconnected, and idle states) across all the floating desktop pools in the assignment. The logins can originate from both global entitlements (such as the Horizon Cloud desktop assignment) and local entitlements. The sum of user sessions is then divided by the Desktops capacity to yield a fractional value. Finally, the fractional value is multiplied by 100 to obtain the Occupancy percentage. The Occupancy for a dedicated desktop assignment is calculated by first totaling the number of assigned virtual machines from all the dedicated desktop pools in the assignment. The total is divided by the Desktops capacity to yield a fractional value and then multiplied by 100 to obtain the Occupancy percentage. For example, suppose that a floating desktop assignment includes four desktop pools, for a total Desktops capacity of 4. There are two user sessions currently in effect. The Occupancy equals ((2/4)*100 = 50%).</td>
</tr>
<tr>
<td>Active Users</td>
<td>The total number of users who are currently logged in and connected to a session on a desktop, expressed as an integer value.Disconnected and idle sessions are excluded from this count. The Active Users count is based on users logged in and connected through both global entitlements (such as the Horizon Cloud desktop assignment) and local entitlements. The Active Users count is calculated by adding up the total number of connected sessions for each desktop in the assignment. For example, suppose that a desktop assignment includes four desktop pools. There is one connected user session for one of the desktop pools. There are no connected user sessions for any of the remaining three desktop pools. In this case, the Active Users count is 1.</td>
</tr>
</tbody>
</table>
The Summary page displays a read-only list of the assignment's current settings, organized under the categories Definition, Desktops, and Users. For instructions on how to modify the settings, see Edit a Multi-Cloud Assignment in Your Horizon Cloud Tenant Environment.

System Activity page

The System Activity page displays activity in the desktop assignment due to system actions, such as powering off desktops to meet the power management schedule.

You can cancel some tasks before they complete by selecting the task in the list and clicking Cancel Tasks.

- Before attempting to select a task for cancellation, refresh the view to update the status for the tasks displayed.
- If a task is currently in a state where the system allows you to cancel it, you can select the check box corresponding to that cancellable task.
- A maximum of 100 tasks at a time can be cancelled for a given pod.

The table below shows tasks that you can cancel.
<table>
<thead>
<tr>
<th>Task</th>
<th>Cancel When Task is in Queued State</th>
<th>Cancel When Task is in Running State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Farm Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Note the following:</td>
<td>Note the following:</td>
</tr>
<tr>
<td></td>
<td>- When the system has automatically created an expansion task for an RDSH farm, the farm must be offline before you can cancel that task.</td>
<td>- When the system has automatically created an expansion task for an RDSH farm, the farm must be offline before you can cancel that task.</td>
</tr>
<tr>
<td></td>
<td>- You can only cancel this task for pods at the manifest version for October 2020 or later. The manifest version is found in the <em>Horizon Cloud Service Release Notes</em>.</td>
<td>- Resources that have already been created, such as VMs and OS/data disks, are destroyed when the task is canceled. When VMs are destroyed or not created, this changes the size of the assignment.</td>
</tr>
<tr>
<td>Assignment Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Note the following:</td>
<td>Note the following:</td>
</tr>
<tr>
<td></td>
<td>- When the system has automatically created an expansion task for a VDI desktop assignment and assignment creation or update is in progress, tasks can be cancelled. After assignment creation/update is finished, no tasks can be cancelled.</td>
<td>- You can only cancel this task for pods at the manifest version for October 2020 or later. The manifest version is found in the <em>Horizon Cloud Service Release Notes</em>.</td>
</tr>
<tr>
<td>Convert VM to Image</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you cancel this task, and wish to retry it, first confirm that the VM is in a state where it can be converted. If you are not sure, power off and then power on the VM.</td>
<td><strong>Note</strong> If you cancel this task, and wish to retry it, first confirm that the VM is in a state where it can be converted. If you are not sure, power off and then power on the VM.</td>
</tr>
</tbody>
</table>

**Edit a Multi-Cloud Assignment in Your Horizon Cloud Tenant Environment**

You can use the **Edit** button on the Horizon Cloud Administration Console’s Assignments page to change the configuration settings for an existing multi-cloud assignment.
Procedure

1. In the left pane of the console, click **Assignments**. If you have cloud-connected Horizon pods, select **On-Prem & VMware Cloud** from the Assignments menu.

2. On the Assignments page, select the check box next to an existing assignment and click **Edit**.
   
   The Edit Desktop Assignment wizard appears. This wizard is similar to the New Desktop Assignment wizard, with read-only settings for those options that cannot be changed for an existing desktop assignment.

3. Follow the prompts in the wizard to change the configuration settings for the assignment as needed.

   For instructions on how to use the wizard, see *Horizon Pods - Create a Multi-Cloud Assignment of VDI Desktops*.

   **Note**  Some configuration settings cannot be changed for an existing assignment. For example, you cannot change the desktop type from Floating to Dedicated. Instead, you must create a new assignment and specify the desktop type at the time of creation.

Delete a Multi-Cloud Assignment from Your Horizon Cloud Environment

You can permanently delete an assignment from the Assignments page.

When you delete an assignment, users who received the assignment can no longer access it. However, the desktop pools included in the assignment remain intact.

Procedure

1. In the left pane of the Horizon Cloud Administration Console, click **Assignments**. If you have configured the console for hybrid cloud capacity, select **On-Prem & VMware Cloud** from the Assignments menu.

2. On the Assignments page, select the check box next to an existing desktop assignment and click **Delete**.

3. At the message asking you to confirm the action, click **Delete**.

   **Note**  The deletion of the assignment does not happen immediately and can take some time to finish.

Prevent Deletions or Allow Deletions for a Multi-Cloud Dedicated Desktop Assignment

You can prevent deletions or allow deletions of VMs for a dedicated desktop assignment using a setting on the **Assignments** page.
The **Prevent Deletions** option causes the system to deny all requests to delete a desktop VM from a dedicated desktop assignment. You can also set limits on VM deletions using the following options.

- **Deletion Protection** - For more information, see [Customizable General Settings for Your Horizon Cloud Tenant Environment](#).
- **Max Desktop Deletions** - You can set this option when creating or editing a dedicated desktop assignment. The option is described in [Pods in Microsoft Azure - Create a VDI Multi-Cloud Assignment](#).

**Important** If you specify a new image for a dedicated desktop assignment that has deletion prevention enabled, the system deactivates deletion prevention and changes deletion settings so that all unassigned desktop VMs can be rebuilt with the new image.

**Note** In the notifications at the top of the page, the notifications that appear regarding deletion protection currently display the name of the assignment incorrectly, with additional characters appended to the name. This is a known issue and is being fixed in the next release.

### Prevent Deletions

1. On the **Assignments** page, select the check box for the assignment.
   - Options for the assignment are enabled.
2. Click **More > Prevent Deletions**.
   - A dialog box displays asking you to confirm that you want to prevent deletions for the assignment.
3. Click **Continue**.
   - A message displays indicating that the operation was successful.

### Allow Deletions

1. On the **Assignments** page, select the check box for the assignment.
   - Options for the assignment are enabled.
2. Click **More > Allow Deletions**.
   - A dialog box displays asking you to confirm that you want to allow deletions for the assignment.
3. Click **Continue**.
   - A message displays indicating that the operation was successful.
Introduction to Horizon Cloud Pods in Microsoft Azure

You must have a subscription for cloud capacity in Microsoft Azure and then bring that subscription information to pair that cloud capacity with Horizon Cloud. After the pod is deployed in Microsoft Azure, you use the administrative console —named the Horizon Cloud Administration Console or console for short — to create golden images, farms and VDI desktops, assign use of desktops and applications to your users, as well as how to perform other administrative tasks. From a pod located in Microsoft Azure, your end users can securely access their desktops and applications from any device. You can choose where the desktops and applications reside, based on the location of the deployed pod.

For the overall introduction to Horizon Cloud, see Chapter 1 Introduction to Horizon Cloud and Onboarding Pods to Become Cloud-Connected Pods. For the suggested workflow of activities for a pod in Microsoft Azure, see High-Level Workflow for When Your Very First Horizon Cloud Cloud-Connected Pod is from Using the Pod Deployer to Deploy a Pod into Microsoft Azure.

Horizon Cloud Pod Deployed in Microsoft Azure

You connect your Microsoft Azure subscription to Horizon Cloud to manage and deliver VDI desktops and RDSH-served desktops and applications. Setting up the environment involves an automated deployment of the pod into your Microsoft Azure capacity.
The pod deployed by Horizon Cloud into Microsoft Azure has a physical regional location in a Microsoft Azure cloud. In the pod deployment wizard, you select where to place the pod, according to the regions available for your particular Microsoft Azure subscription. You also select an existing virtual network (VNet) that the pod will use in your selected region. You have the option to deploy an external gateway configuration with the pod, with that external gateway's resources deployed either into the same VNet as the pod or into a separate VNet that is peered with the pod's VNet.

**Note** You preconfigure your Microsoft Azure environment with the pod VNet (and with the external gateway VNet if using that configuration option). You can either create in advance those subnets that the pod and external gateway configuration require, or let the pod deployer create the subnets during deployment. If you do not create the subnets in advance, the pod deployer creates the subnets as it deploys the required VMs and resources into your environment. If you choose to have the pod deployer create its required subnets, you have to know what IP address spaces you want to use for the pod's subnets before you start the deployment wizard. If you choose to create the subnets in advance, you must ensure they meet certain requirements before you start the deployment process. For details about requirements when you create the subnets in advance, see [In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure](#) and [When Using Existing Subnets for a Horizon Cloud Pod in Microsoft Azure](#).

**Important** This pod in Microsoft Azure is not a tenant. This pod does not adhere to the exact same set of characteristics that defines a tenant and which you would expect from a tenant. For example, even though a tenant would have a one-to-one mapping to an Active Directory domain and be isolated from other tenants, all of the Horizon Cloud pods in Microsoft Azure that are deployed using the same Horizon Cloud customer account record need to be able to reach the same Active Directory servers and the DNS configuration needs to resolve all of those Active Directory domains.

To do multi-tenancy, you would set up multiple Horizon Cloud customer account records. The Horizon Cloud customer account record, which is created when you registered with VMware to use the Horizon Cloud Service and is associated with your My VMware credentials, is more like a tenant. A Horizon Cloud customer account record is isolated from other Horizon Cloud customer account records. A single customer account record maps to multiple pods, and when someone uses any of the account credentials associated with that customer account record to log in to the administrative console, the console reflects all of the pods that are mapped to that customer account record.

The pod deployment process automatically creates a set of resource groups in your Microsoft Azure capacity. Resource groups are used to organize the assets that the environment needs and creates, such as:

- VMs for the pod's manager instance (multiple VMs for a pod that is enabled for high availability)
- VMs for the Unified Access Gateway instances and their load balancers
VM for the connector VM in the external gateway configuration when you deploy that configuration in a VNet separate from the pod’s VNet

VMs for the RDSH-capable golden images

VMs for the VDI desktop golden images

VMs for the assignable (published, sealed) images that are made from the golden images

VMs for the RDSH farms that provide the RDSH desktops and remote applications

VMs for the VDI desktops

Additional assets that the VMs and the environment require for supported operations, such as network interfaces, IP addresses, disks, key vaults, Microsoft Azure Database for PostgreSQL server resource, and various items along those lines. The pod deployment process can create the required virtual subnets also, using the values you specify in the deployment wizard.

All of the resource groups created by Horizon Cloud in your Microsoft Azure environment are named using the prefix *vmw-hcs*.

**Caution** Do not manually modify or delete the pod-related resources using the Microsoft Azure portal except for:

- Manual creation of golden images.
- Modifying farm and VDI desktop assignment network security groups as need to configure ports for your business circumstances.

Horizon Cloud automatically configures the pod-related resources to ensure the pod operates as designed. Never manually change settings for the resources that Horizon Cloud automatically creates and deploys during workflows, including assigned IP addresses or names, and so on.

Never manually power off VM instances or delete them directly using the Microsoft Azure portal. Never manually delete the manager VM or Unified Access Gateway VMs. Never manually delete NICs from the resource groups, especially from the Unified Access Gateway resource groups. If you change the generated settings or manually power off VMs or manually delete VMs or NICs that were created by the pod deployer, unpredictable results can occur and pod operations, pod updates, and pod deletion operations might encounter failures.

The following diagram illustrates a deployed pod that is enabled for high availability and has both the external and internal types of Unified Access Gateway configurations. In this diagram, RG means resource group. The Unified Access Gateway instances in the external Unified Access Gateway configuration have NICs on the demilitarized (DMZ) network. When your pod has the external Unified Access Gateway configuration, your end users located in the Internet, outside your corporate network, can access their pod-provisioned virtual desktops and applications through that configuration. When your pod has the internal Unified Access Gateway configuration, your end users located in your intranet, inside your corporate network, can make
trusted connections to their pod-provisioned virtual desktops and applications through that gateway. The pod deployment wizard provides the option to deploy the pod with both configurations up front. Alternatively, you can deploy the pod with only one gateway configuration and edit the deployed pod to add the other type of gateway configuration later.

You can also choose not to enable the high availability option in the deployment wizard, and then edit the deployed pod later to enable high availability on it. A new pod is always deployed with the Azure Postgres database and pod load balancer, even when you do not enable the high availability option in the wizard. Having those assets available allows for easy enablement of high availability on an already deployed pod. The second pod manager VM is only deployed when high availability is enabled on the pod.
Figure 7-1. Illustration of the Horizon Cloud Pod Architecture for a Pod with High Availability Enabled and Configured with Both External and Internal Unified Access Gateway Configurations
The following diagram illustrates the resources that are deployed when you choose the option to have the external gateway residing in its own VNet, separate from the pod’s VNet. The two VNets must be peered. This diagram also applies when you choose the option to have the external gateway's resources deployed using a Microsoft Azure subscription that is different than the one used for the pod. Because VNets cannot cross subscriptions, choosing to deploy the external gateway into its own subscription is a subset of choosing the external gateway to reside in its own VNet.

**Tip** Deploying the external gateway configuration into its own VNet gives you the ability to deploy these Horizon Cloud pods into complex Microsoft Azure environments that use **hub-spoke network topology in Microsoft Azure**.

**Figure 7-2. Illustration of the External Gateway's Architecture Elements When the External Gateway is Deployed into Its Own VNet, Separate from the Pod’s VNet**

---

**Subscriptions and Number of Pods**

Be mindful about the number of pods you deploy into a single subscription, especially if you plan to have each pod running at a large scale. Even though multiple pods can be deployed into a single Microsoft Azure subscription, whether all into one region or spread across multiple regions, Microsoft Azure imposes certain limits within a single subscription. Because of those Microsoft Azure limits, deployment of a large number of pods into a single subscription increases the
likelihood of hitting those limits. Numerous variables, and combinations of those variables, are involved in reaching those limits, such as the number of pods, the number of farms and assignments within each pod, the number of farm RDSH VMs within each pod, the number of desktops within each assignment, and so on.

If you plan to have pods running at a large scale, consider adopting the approach of having multiple subscriptions with those multiple subscriptions under one Microsoft Azure account. Microsoft Azure customers use this approach, and often prefer it, because it provides some benefits for ongoing management of the subscriptions. Using this approach, you would deploy a single pod per subscription, roll up those subscriptions in a single primary account, and avoid the chances of hitting the Microsoft Azure limits that are imposed on a single subscription.

When You Have Existing Pods That Were Deployed Prior to This Current Horizon Cloud Release

As described in Updating Your Horizon Cloud Pod, VMware updates the Horizon Cloud software components periodically to include new features and bug fixes. The in-cloud management environment is updated on a weekly basis and the binaries that are the basis of the pod software components are typically updated on a roughly quarterly basis. The Horizon Cloud Service documentation page provides access to the Release Notes page which provides What's New lists for each calendar timepoint at which substantive customer-visible features have debuted.

When you deploy a new pod, that pod is always created at the manifest version that is the latest one for the current in-production service environment. As an example, if you created a new pod in August 2019, that pod was deployed with software components that were current for Horizon Cloud as of that date. Depending on how long you have been using your Horizon Cloud environment, on a given calendar date, your overall Horizon Cloud environment might include some pods that are at the latest released version and some that are at an earlier released version which are not yet updated to the latest manifest.

Important In general, the content in this Administration Guide describes features, workflows, and behaviors that are available in the current in-production release and which are applicable when your pod is at the latest pod manifest version which was made available in this current release. The cloud-based console in which you perform management and administrative tasks is dynamic. The console's Web-based interface will typically display messages when an area or action in the console requires upgrading the pod to use that feature. For a pod that existed prior to this release, some workflows might require different steps than are described in this Administration Guide. For a list of workflows in this release that are now different for pods at the latest manifest version, if any, see the documentation topic For Current Customers with Existing Cloud-Connected Pods — About Horizon Cloud Releases and the sections it contains.
Microsoft Azure Terminology and References

The VMware Horizon Cloud Service on Microsoft Azure product documentation uses the applicable Microsoft Azure terminology as appropriate in the descriptions and task steps of the VMware Horizon Cloud Service on Microsoft Azure workflows. If the Microsoft Azure terminology is unfamiliar to you, you can use the following applicable references in the Microsoft Azure product documentation to learn more.

**Note** All capitalization and spelling in the citations below follow the same capitalization and spelling found in the linked-to articles in the Microsoft Azure documentation itself.

<table>
<thead>
<tr>
<th>Useful Microsoft Azure References</th>
<th>Description</th>
</tr>
</thead>
</table>
| Microsoft Azure glossary: A dictionary of cloud terminology on the Azure platform | Use this glossary to learn the meaning of terms as used in the Microsoft Azure cloud context, for terms such as load balancer, region, resource group, subscription, virtual machine, and virtual network (vnet).  
**Note** The Microsoft Azure glossary does not include the term service principal because the service principal is a resource automatically created in Microsoft Azure when an application registration is created in Microsoft Azure. The reason why you create an application registration in your Microsoft Azure subscription is because that is the way you authorize Horizon Cloud as an application to use your Microsoft Azure capacity. The application registration and its companion service principal enable the Horizon Cloud cloud service acting as an application to access resources in your Microsoft Azure subscription. Use the next reference below to learn about applications and service principals that can access resources in Microsoft Azure. |
| Use portal to create an Azure Active Directory application and service principal that can access resources | Use this article to learn about the relationship between an application and a service principal in a Microsoft Azure cloud. |
| Azure Resource Manager overview | Use this article to learn about the relationships between resources, resource groups, and the Resource Manager in Microsoft Azure. |
| Azure VNet | Use this article to learn about the Azure Virtual Network (VNet) service in Microsoft Azure. See also Azure Virtual Network FAQs. |
| Azure VNet Peering | Use this article to learn about virtual network peering in Microsoft Azure. |
| Hub-spoke network topology in Azure | Use this article to learn about hub-spoke network topology in Microsoft Azure. |
| Microsoft Azure ExpressRoute Overview | Use this article to learn about Microsoft Azure ExpressRoute and how you can use it to establish connections between your on-premises networks, Microsoft Azure, and your Horizon Cloud pods. |
| About VPN Gateway Planning and design for VPN Gateway Create a Site-To-Site connection in the Azure portal | Use these articles to learn about how to configure VPNs in Microsoft Azure. |
| What is Azure Load Balancer? | Use this article to learn about the Azure load balancers that are deployed for a pod: the load balancer for the pod manager VMs and the load balancers for the gateway configurations. |
Useful Microsoft Azure References

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What is Azure Database for PostgreSQL?</strong></td>
</tr>
<tr>
<td>Use this article to learn about the Microsoft Azure Database for PostgreSQL service.</td>
</tr>
<tr>
<td><strong>What is Windows Virtual Desktop?</strong></td>
</tr>
</tbody>
</table>
| Use this article to learn about Microsoft Windows Virtual Desktop and how it relates to Microsoft Windows 10 Enterprise multi-session and Microsoft Windows 7 Enterprise with Extended Security Updates. When your Horizon Cloud tenant account has the configuration for Horizon Cloud Service on Microsoft Azure extending Microsoft Windows Virtual Desktop, support is provided for using Microsoft Windows 10 Enterprise multi-session and Microsoft Windows 7 Enterprise with your pods deployed in Microsoft Azure.

This chapter includes the following topics:

- High Availability and Your Horizon Cloud Pod in Microsoft Azure
- Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure
- Using Microsoft Azure Disk Encryption with Your Farms and VDI Desktops in Your Horizon Cloud Environment
- Using Data Disks with Virtual Desktops from a Horizon Cloud Pod in Microsoft Azure
- VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure
- Managing VM Types and Sizes for Farms and Assignments
- Farms in Horizon Cloud
- Applications in Your Horizon Cloud Inventory
- About Desktop Assignments for Your Horizon Cloud Environment's Pods in Microsoft Azure
- Create a URL Redirection Customization and Assign it to Users
- Managing Published Images for Horizon Cloud Pods in Microsoft Azure
- Managing Assignments Provisioned By Horizon Cloud Pods in Microsoft Azure
- Updating the Agent-Related Software Used by Horizon Cloud
- Managing Your Horizon Cloud Pods Deployed in Microsoft Azure
- Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access
- Configure True SSO for Use with Your Horizon Cloud Environment
- End User Connections to Desktops and Applications Provided by Your Horizon Cloud Environment

**High Availability and Your Horizon Cloud Pod in Microsoft Azure**

Starting with the September 2019 quarterly service release, the architecture of a Horizon Cloud pod in Microsoft Azure supports having high availability for the pod. New pods deployed by the
pod deployer after the September 2019 service release and older pods updated to manifest versions 1600 or later will all get this latest pod architecture. This pod architecture includes a Microsoft Azure Database for PostgreSQL server resource, a Microsoft Azure load balancer, and a Microsoft Azure availability set. When high availability is enabled on a pod of this architecture, an extra pod manager VM is added to the pod, for a total of two pod manager VMs, connected to the Microsoft Azure load balancer. This configuration enables the pod to continue to operate even if one manager VM experiences an issue. If one manager VM goes down, all traffic is automatically routed to the other manager VM without any manual intervention.

For new pods, you can deploy the pod with high availability enabled from the start, or deploy the pod with high availability turned off and enable it later. For existing pods that are updated to a pod manifest that gets this latest pod architecture, the update process does not automatically enable high availability on the pod. You can enable high availability on an updated pod after both these items are in place:

- The pod update process is completed on that pod
- The agents are updated on all of the pod's existing image VMs, farm RDSH-capable VMs, and VDI desktop VMs to the agent version that is compatible with the updated pod

The pod's details page reports whether high availability is enabled or disabled for that pod. For the steps to enable high availability on a pod where it is disabled, see Enable High Availability on a Horizon Cloud Pod in Microsoft Azure.

High Availability Design for a Pod in Microsoft Azure

In addition to having two pod manager VMs, the pod also has a Microsoft Azure load balancer resource, a Microsoft Azure availability set, and a Microsoft Azure Database for PostgreSQL server resource. This design provides for overall pod resiliency and fail over if one of the pod manager VMs experiences an issue or goes down.

**Important** A pod created new in the September 2019 release level is always deployed with a Microsoft Azure Database for PostgreSQL server resource, the Microsoft Azure load balancer, and availability set. Even when you toggle off the **High Availability** option in the pod deployment wizard, the resulting pod has those new pod architecture's elements. Also, a pod created in a prior release and then updated to the September 2019 release level results in a pod with this new design: the Microsoft Azure Database for PostgreSQL server resource, the Microsoft Azure load balancer, and availability set, even though high availability is not automatically enabled in the update process. Standardizing on this pod design for all pods with manifest versions 1600 or later allows for the ease of enabling high availability on an already deployed pod. The second pod manager VM is only deployed when the high availability feature is enabled on the pod.

These resources reside in the pod's resource group and you can view their details in your subscription when you log in to the Microsoft Azure portal. For information about identifying the pod's resource groups, see Resource Groups Created For a Pod Deployed In Microsoft Azure.

**Microsoft Azure availability set**
As described in the Microsoft Azure documentation, a combination of a Microsoft Azure load balancer with availability sets provides the highest application resiliency. An availability set, or availability zone as it is sometimes referred to in the Microsoft Azure documentation, in each Microsoft Azure region is a combination of a fault domain and an update domain. By using an availability set, each of the pod's manager VMs is deployed on separate physical hardware within the same Microsoft Azure data center. The availability set enforces the manager VMs to reside on separate physical hardware. This separation of back end hardware minimizes the likelihood of both manager VMs experiencing downtime at the same time. Only if the entire Microsoft Azure data center goes down would both manager VMs be affected.

**Microsoft Azure load balancer**

The deployed load balancer resource is connected to the pod's tenant subnet. This load balancer is used to route traffic to the pod's manager VMs according to the pod-deployer-configured health probe and rules. The manager VMs are added to this load balancer's back end pool. One manager VM assumes the role of the active broker for the end-user client connections to the pod-provisioned desktops and applications. The load balancer determines broker affinity based on the defined rules and health probe of the manager VMs in the back end pool. Based on the determined broker affinity, the load balancer routes all broker traffic seamlessly to the manager VM that is the active broker until a fail over occurs. Then the other manager VM becomes the active broker and the load balancer routes the brokering requests to that VM. When this fail over occurs, a notification is sent to the administrative console to inform you of this change in which manager VM is the active broker.

The pod load balancer sits between the end-user client connection requests and the pod's manager VMs. When the pod is configured with a gateway configuration, traffic from the Unified Access Gateway instances routes to the pod's Microsoft Azure load balancer. That Azure load balancer routes that traffic to the manager VM that is the active broker. When the pod has no gateway configuration, and you have configured the pod for direct connections, such as over VPN, the end-user client connections go to the pod's Microsoft Azure load balancer, which routes that traffic to the manager VM that is the active broker.

**Microsoft Azure Database for PostgreSQL - Single Server**

The pod has a Microsoft Azure Database for PostgreSQL server that uses the Single Server deployment option. Use of this server provides for centralizing data needed for pod operations and eliminates the need to use data replication across the manager VMs. In the current release, the following configuration is used:

- PostgreSQL version 10
- Memory Optimized
- Compute generation: Gen 5
- vCores: 2
- Storage: 10 GB
- Auto-growth: No
Backup Storage: Locally redundant

See the Microsoft documentation for information about their Memory Optimized configuration:

- Pricing tiers in Azure Database for PostgreSQL - Single Server
- Pricing - Azure Database for PostgreSQL

Cost Impact in Your Microsoft Azure Subscription for Pods Created in or Updated to This Release Level

The elements required to support high availability in this release have some cost implications in your Microsoft Azure subscription. All pods created new at this release level and pods updated to this release level incur a cost for the managed Microsoft Azure Database for PostgreSQL server. A pod enabled with high availability also incurs a cost for running the additional manager VM. As of this writing, there are no costs for use of the Azure Load Balancer or availability set that are deployed for all pods created at, or updated to, this release level.

For pricing estimates of the Microsoft Azure Database for PostgreSQL configuration described above that is used in the current release, see https://azure.microsoft.com/en-us/pricing/details/postgresql/server/.

Enable High Availability on a Horizon Cloud Pod in Microsoft Azure

Starting with the September 2019 Horizon Cloud release, pods updated to that release's manifest version and pods newly created at that release level provide the option to be enabled for high availability. For a pod on which the feature is disabled, you can enable high availability by following these steps.

As described in High Availability and Your Horizon Cloud Pod in Microsoft Azure, when a pod is enabled for high availability, it has two manager VMs. When the pod's details page says high availability is disabled, the pod has only one manager VM. Then, when you edit the pod to enable high availability on it, a second manager VM is deployed to the pod's resource group, and that VM is configured in the pod's Microsoft Azure load balancer and availability set.

**Important** Enabling the pod for high availability is a one-time action. After a pod is enabled for high availability, you cannot later revert the configuration and disable the feature on the pod.

**Prerequisites**

Verify you meet these criteria before editing the pod to enable high availability.

- The pod software must be at manifest version 1600 or later to be enabled for high availability. You can see a pod's manifest version by navigating to the pod's details page from the Capacity page.
If the pod was updated from a manifest version earlier than 1600, before you can enable it for high availability, you must update the agents on all of the pod’s image VMs, farm RDSH VMs, and desktop assignment VMs to the September 2019 agent release level. For information about updating the agents, see Updating the Agent-Related Software Used by Horizon Cloud and its subtopics.

Ensure your subscription used by the pod has enough quota and cores to accommodate creation of the temporary jump box VM used for system configuration actions on Horizon Cloud pods. This jump box VM orchestrates the configuration update activity on the pod’s resources, such as the pod’s load balancer. The system deletes the jump box and its artifacts and resource groups when the configuration activity is finished.

Ensure your subscription has enough quota and cores to accommodate creation of the additional pod manager VM.

Procedure

1. Navigate to the pod’s details page from the Capacity page.
2. Click Edit.
3. In the High Availability section, switch on the toggle for Enabled.
4. Click Save & Exit.
5. Confirm the update.

Results

The system creates a resource group for the jump box VM that orchestrates the activity to enable high availability on the pod and deploys the jump box VM. The jump box VM orchestrates updating the pod’s configuration. On the pod’s details page, the cluster status shows Pending state. When the configuration activity is finished, the cluster status shows Ready state. The overall process takes several minutes to complete.

Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure

Before you can start delivering desktops or RDS-based remote applications to your end users from your deployed pod, you must create at least one assignable desktop image. Creating this assignable image is a multi-step process: a base virtual machine (VM) must be created and paired with the cloud plane, then customized according to your organization’s needs, and then converted into an assignable desktop image.

An assignable image is an image that has successfully completed the Horizon Cloud sealing process and Horizon Cloud can use it to provision RDS farms (in the case of RDS-based images) or VDI desktops (in the case of client-based images). Other terms sometimes used to describe such images are sealed images and published images. Sealing an image is sometimes referred to as publishing the image or converting the image to a desktop.
Creating the image involves this high-level sequence.

**Important** Tech Preview: Use of App Volumes with Microsoft 10 Enterprise multi-session is currently in tech preview. During the tech preview, when you are creating a desktop image using Microsoft 10 Enterprise multi-session for the purpose of using App Volumes with that image, you must follow a slightly different sequence of steps to get to a published image than the steps below. See Tech Preview - How To Configure a Microsoft Windows 10 Multi-Session Image for Use with App Volumes Features in Horizon Cloud Pods in Microsoft Azure.

### First, Create a Base Virtual Machine (VM)

You create a base VM either using the automated wizard or manually.

- The recommended and standard way is to use the Import VM from Marketplace wizard's option to create the base VM using one of the supported VM configurations from the Microsoft Azure Marketplace. Using the wizard automates building the virtual machine (VM) and configuring the VM to conform to the Horizon Cloud environment's requirements, including installing and configuring the appropriate agent-related software. The wizard also provides options for optimizing the VM, which can prevent Microsoft Windows Sysprep errors from occurring. From the console's Inventory page, start the wizard by clicking **Import**. For steps, see Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it with Horizon Cloud.

  **Tip** The wizard provides toggles that result in agent-related options getting installed in the VM, such as the App Volumes Agent and the Horizon Agent's remote experience features. Before selecting the remote experience features in the wizard, read Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance from Horizon Cloud Farms and Desktops.

- An alternative to the standard way is to use the Microsoft Azure portal and manually perform all of the steps that the wizard automates. For information about these manual steps see Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud. In that manual workflow, you must manually run the Horizon Agents Installer (HAI) to install the required agent software that allows for the VM to be paired with Horizon Cloud.

  **Important** If you use this alternative method, you are responsible for ensuring the resulting VM conforms to the configuration required by the Horizon Cloud environment. Applying the same configuration that are described for the automated wizard's Optimize Windows Image and Remove Windows Store Apps options is strongly recommended. Use of those configurations helps avoid Microsoft Windows Sysprep issues that might occur when the VM is later published as an image. See Deciding to Optimize the Windows Image When Using the Import Virtual Machine from Marketplace Wizard and Using the Remove Windows Store Apps Option When Using the Import Desktop Wizard.
Second, Pair the Image VM with Horizon Cloud

**Note** For a pod that has a manifest version lower than 1600 and you run the automated wizard to create an image in that pod, the resulting VM is automatically paired with the cloud. In this case, the Imported VMs page will indicate the agent is in an active state. For this situation, you proceed with Third, Customize the VM.

The following table describes what the Imported VMs page's Agent Status column will display for the listed cases where the resulting VM is not yet paired, even though it has the agent software installed on it.

<table>
<thead>
<tr>
<th>Pod Manifest</th>
<th>Creation Method</th>
<th>Displayed Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1600 or higher (created after the September 2019 service release)</td>
<td>Automated wizard</td>
<td>Not Paired (Import Successful)</td>
</tr>
<tr>
<td>1600 or higher (created after the September 2019 service release)</td>
<td>Manual</td>
<td>Not Paired</td>
</tr>
<tr>
<td>Prior to 1600</td>
<td>Manual</td>
<td>Not Paired</td>
</tr>
</tbody>
</table>

The following screenshot illustrates a VM that is successfully created using the automated wizard, but which is not yet paired with the cloud.

![Imported VMs](image)

In either of the above cases, you must explicitly pair the VM with Horizon Cloud. The specific steps to explicitly pair the VM depend on the manifest version of the pod in which the VM is located.

**For a pod of manifest version 1600 or higher**

On the Imported VMs page, you use the **Reset Agent Pairing** action on the VM to explicitly pair the VM with Horizon Cloud. This process can take several minutes. During the pairing process, the VM is restarted and its agent status changes to Unknown to Active. You have to refresh the page using the circular arrow icon to see the status changes.

**For a pod of manifest versions lower than 1600**
When the VM was created manually, you explicitly pair the VM by following the steps in *Manually Pair the Configured Virtual Machine with Horizon Cloud For Pods with Manifests Lower Than 1600*.

The pairing process is completed when the Agent Status column displays Active and an agent version, such as 19.4.0. The following screenshot illustrates a VM after the pairing process is completed.

![Agent Status](image)

**Third, Customize the VM**

When the pairing process completes and after refreshing the page, the VM's agent status shows as active, then you customize the image VM's guest Windows operating system (OS) with the third-party applications you want to provide to your end users, as well as configure any OS-level settings such as customized wallpaper, fonts and colors, drivers, and other such items. For steps, see *Customize the Imported VM's Windows Operating System* and *Install NVIDIA Graphics Drivers in a GPU-Enabled VM Imported in Horizon Cloud*.

**Important** Starting with the December 2019 service release, the Import Virtual Machine wizard provides the option of either having the wizard-created VM joined to a specified Active Directory domain or not having the VM joined to the domain. Prior to the December 2019 service release, the wizard-created VM was always automatically joined to the domain. Your organization might also choose to join manually created VMs to a domain, to allow for domain admin accounts to log in and customize those VMs prior to sealing them.

If the base VM was joined to the domain in the creation process, then domain admin accounts can log in to the VM to customize it. However, when your pod has not yet updated to manifest version 1230 or later, and if your organization has a policy that prevents use of local administrator accounts on domain-joined VMs, you will not be able to log in to the image VM to customize it until you configure the DaaS Direct Connect Users local group with those domain accounts you want used for customizing the image. Prior to pod manifest 1230, the agent software installed in a domain-joined VM prevented domain accounts from directly connecting to that VM. For details, see *When Your Pod is Not Yet Updated to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image*.

**Configure the VM for Optimal Remote Experience Performance**

After you have customized the VM for your specific organizational needs, follow the steps in *Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance from Horizon Cloud Farms and Desktops* to ensure your end users will receive optimal remote experience performance from their assigned desktops and applications.
Finally, Convert that Image VM to a Published Image

You use the New Image workflow to convert that VM to an assignable desktop image. For steps, see Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

After the VM is converted, the image’s Published status on the Images page indicates Horizon Cloud has sealed the image VM for use in the environment. When you see that the image on the Inventory - Images page displays the Published status, you can create:

- From an RDS-based image, RDSH farms created based on that image. You can create both types of farms from the same published RDS-based image: desktop farms to provide end-user access to session-based desktops and application farms to provide access to remote applications. When you have created a farm, you can then use it to make assignments to users. See Farms in Horizon Cloud.

- From a Windows client-based image, VDI desktop assignments based on that image. See Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure and Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure.

About the VMware Dynamic Environment Manager Agent Software and Creating Desktop Images in a Horizon Cloud Pod in Microsoft Azure

Starting with the July 2019 Horizon Cloud release, installation of the VMware Dynamic Environment Manager agent is incorporated into both the Horizon Agents Installer and the automated Import Desktop workflow. The VMware Dynamic Environment Manager agent component is also called the FlexEngine client component. The Horizon Agents Installer is the software package that installs the agent-related software in a new image VM, when you run the Import Desktop workflow or manually create an image VM. When you Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it with Horizon Cloud, the Horizon Agents Installer runs behind the scenes to install the agents. When you Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud, you download and run the Horizon Agents Installer as part of those steps.

The July 2019 Horizon Cloud release corresponds with the 19.2 version of Horizon Agents Installer. The VMware Dynamic Environment Manager files are installed into the resulting image VM into file paths as described below.

For a pod with manifest version 1493 and later, when the base image VM is created in that pod using the automated Import Desktop workflow

This pod version is the first one in which the VMware Dynamic Environment Manager components are installed automatically into these base images by default. The resulting install file path is C:\Program Files\VMware\Horizon Agents\User Environment.

For a pod with manifest version 1493 and later, when the base image VM is created using the manual method
This pod version is the first one in which the Horizon Agents Installer has the option to install the VMware Dynamic Environment Manager components. If you choose to install that option when you run the Horizon Agents Installer in that manually created base VM, the resulting install file path is C:\Program Files\VMware\Horizon Agents\User Environment.

For a pod with manifest version earlier than 1493, when the base image VM is created in that pod using the automated Import Desktop workflow or using the manual creation method

In this case, the automated workflow does not install the VMware Dynamic Environment Manager components by default into the resulting VM. For base images in those older pods, you have to manually run the standalone VMware Dynamic Environment Manager installer that you download from the Horizon Cloud Downloads page in https://my.vmware.com. In this case, the resulting install file path is C:\Program Files\Immidio\Flex Profiles.

Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it with Horizon Cloud

For a pod in Microsoft Azure, you can use the Import Virtual Machine – Marketplace wizard to create the virtual machine (VM) using an operating system image from the Microsoft Azure Marketplace. In the process, the VM is automatically configured with the elements and agent-related software required to conform to the Horizon Cloud environment’s requirements. At the end of the creation process, the VM is listed on the Imported VMs page and you can take further actions on it, such as pairing the VM with the cloud plane, customizing the VM, installing additional drivers, and so on.

Pods of different manifest versions require different subsequent steps on the VM that results from the Import Virtual Machine wizard.

Pod manifests 1600 and later

Starting with pod manifest 1600, the automated workflow results in a VM that is not yet paired with Horizon Cloud. After the VM is created and listed on the Imported VMs page, you use the Reset Agent Pairing action on it to pair it with the cloud plane.

Pod manifests earlier than 1600

When the wizard creates a VM in a pod with a manifest earlier than 1600, the automated workflow pairs the VM with the cloud plane in the process. At the end of the process, the resulting VM is listed on the Imported VMs page with the agent in the active state.

Remember Like all of the console, this wizard’s user interface is dynamic. The wizard’s displayed selections and options will automatically change as you go through the wizard selecting items in lists and enabling or disabling toggles. The wizard’s displayed items will also reflect what your Horizon Cloud tenant account is licensed to use. If you read something here and you do not see it as you go through the wizard in real time, try changing a selection that is set in the upper portion of the wizard to see how the wizard’s options change. After trying that, if you still do not see what is described, then that item most probably does not apply to your account’s configuration.
By default, the system enables **Optimize Windows Image**, regardless of operating system. For non-multi-session Windows 10 operating systems, the system also enables **Remove Windows Store Apps** by default. Keeping those options enabled is strongly recommended to help prevent you from encountering Microsoft Windows Sysprep issues that might occur when the VM is later published as an image.

Also by default, in the **Advanced Options** section, the wizard enables the various toggles to install those agent-related custom setup options that are both appropriate and relevant according to your other selections in the wizard, and which are supported for use in the Horizon Cloud environment with the selected operating system. If you want to change the default selections, expand the **Advanced Options** section in the **Import Virtual Machine – Marketplace** window and set the toggles according to your needs.

As an example, an agent option that provides 3D support only in operating systems that support RDS or multi-session use cases is enabled by default in the **Advanced Options** section only when you have selected one of those operating systems in the **OS** drop-down list. When you have selected a client operating system for VDI use cases, in which that agent option is not applicable, that agent option is not selected for installation.

**Tip** Starting with the December 2019 service release, the Import Virtual Machine wizard provides the option of either having the wizard-created VM joined to a specified Active Directory domain or not having the VM joined to the domain at the end of the creation process. Prior to the December 2019 service release, the wizard-created VM was always automatically joined to an Active Directory domain that you specified in the wizard.

However, due to a known issue, if you are using the wizard with a pod of manifest earlier than 1600, you should enable the **Domain Join** option and have the wizard join the VM to a domain. Until the known issue is fixed, if you are using the wizard to create a VM in a pod with a manifest lower than 1600 and you disable the **Domain Join** toggle, the import VM process fails in the final steps of the process. For updated information about this issue, see the December 2019 release information in the Release Notes. The Release Notes page is linked from the **Horizon Cloud documentation page**.
Prerequisites

**Important** When you are importing the VM intending to use it with the App Volumes features, make sure that you explicitly enable the **Domain Join** toggle. Domain joining the imported VM is a requirement for using App Volumes with it and that toggle is not set by default. You must explicitly enable that toggle.

Tech Preview: Use of App Volumes with Microsoft Windows 10 Enterprise multi-session is currently in tech preview. During this tech preview, use of the wizard’s **App Volumes Agent** toggle to install the App Volumes Agent into the base VM is not provided when **OS** is set to one of the Microsoft Windows 10 Enterprise multi-session operating systems. When one of those operating systems is selected in this wizard’s **OS** field, that toggle is not visible in the **Advanced Options** section. In this case, after you see the imported VM is successfully imported on the Imported VMs page, you must perform some additional steps to configure the imported VM with the App Volumes Agent. See **Tech Preview - How To Configure a Microsoft Windows 10 Multi-Session Image for Use with App Volumes Features in Horizon Cloud Pods in Microsoft Azure**.

Procedure

1. On the Imported VMs page, click **Import**.

2. In the Import wizard, choose the pod in which to create the VM by first selecting the pod's associated location and then selecting the pod from the list of pods at that location.

   After you select a location, the choices in the **Pod** list are filtered to show the pods available in the selected location.

   **Important** If you are planning to use this image for GPU-enabled desktops or remote applications, ensure that the selected pod resides in a Microsoft Azure region that supports GPU-enabled virtual machines (VMs). GPU-enabled VMs are only available in some Microsoft Azure regions. See **Microsoft Azure Products by region** for details.
Select the details for the base VM.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OS</strong></td>
<td>Select the Microsoft Windows operating system to use for the image's underlying VM.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This drop-down menu takes a few moments to populate the entries.</td>
</tr>
<tr>
<td></td>
<td>■ If you are going to use this image for VDI desktops, select one of the non-server, non-multi-session operating systems that are listed in the drop-down list. To create a VDI desktop image, do not select one of those server or multi-session types of operating systems.</td>
</tr>
<tr>
<td></td>
<td>■ If you are going to use this image for provisioning items that support shared usage, such as RDSH session desktops or RDS-based remote applications, select one of the listed server or multi-session operating systems.</td>
</tr>
<tr>
<td><strong>Include GPU</strong></td>
<td>Enable this toggle to specify a GPU-enabled VM for this base VM. This option is not supported for the Windows 7 operating system. Therefore, you will not see this wizard option due to the dynamic nature of the wizard if you selected a Windows 7 operating system.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> When enabling GPU, after the base VM is created, you must log into the VM's operating system and install the supported NVIDIA graphics drivers to get the GPU capabilities of the Microsoft Azure GPU-enabled VM. You install the drivers after the VM import process is completed.</td>
</tr>
<tr>
<td></td>
<td>If this VM is created in a pod at manifest 1600 or later, you usually install the drivers after using the <strong>Reset Agent Pairing</strong> action on the VM as described in Step 9 below.</td>
</tr>
<tr>
<td><strong>Domain Join</strong></td>
<td>Enable this toggle to specify that the resulting VM will be joined to one of Active Directory domains that are registered with your Horizon Cloud tenant as part of the automated process. When enabled, select the Active Directory domain from the drop-down list. The resulting VM will be joined to the selected domain. Domain administrator accounts in that domain will be able to log in to the resulting VM.</td>
</tr>
<tr>
<td></td>
<td>When this toggle is disabled, the resulting VM is not joined to an Active Directory domain. Only the account credentials that you specify in Step 5 below can be used to log in to the resulting VM.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> When you are planning to use this VM for provisioning App Volumes applications, you must enable the <strong>Domain Join</strong> toggle. Installation of the App Volumes Agent requires the VM to be joined to the domain.</td>
</tr>
<tr>
<td><strong>Enable Public IP Address</strong></td>
<td>Enable this toggle to configure a public IP address for this base VM. When enabled, the VM gets both a private IP address and a public one. When this toggle is disabled, the VM is configured with only a private IP address in your Microsoft Azure environment.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Optimize Windows Image     | By default, this toggle is enabled to create a base VM that meets VMware recommendations and best practices for optimizing a VM’s Microsoft Windows operating system. This optimization includes adjusting default operating system services features to meet the best practices, such as:  
  - Disabling physical desktop features that are irrelevant in a virtual environment, to provide more efficient VM performance.  
  - Disabling certain Windows system services, such as Windows Update, so that control of that service is isolated to administrators instead of the end users.  
  For more details, see Deciding to Optimize the Windows Image When Using the Import Virtual Machine from Marketplace Wizard.  
  **Important** Keeping the default setting is strongly recommended to help prevent you from encountering Microsoft Windows Sysprep issues that might occur when the VM is later published as an image. |
| Remove Windows Store Apps  | This toggle is visible only when OS is set to a non-multi-session Windows 10 operating system. By default, this toggle is enabled to create a base VM that:  
  - Disables the Windows Store Installer Service.  
  - Removes most of the Windows Store applications that come in those base Windows 10 operating systems by default. These Windows 10 default applications are ones provided by AppX packages in the operating system.  
  **Important**  
  - Even when the toggle is enabled, the system retains some AppX packages by default, based on a system-defined allowed list. These allowed AppX packages remain installed in the VM at the end of the import VM process. For the list, visit the topic link below.  
  - Keeping the default setting is strongly recommended to help prevent you from encountering Microsoft Windows Sysprep issues that might occur when the VM is later published as an image.  
  For more details, see Using the Remove Windows Store Apps Option When Using the Import Desktop Wizard. |
|                            |                                                                                                                                                                                                             |
4 Provide administration details.

**Note** The user name and password you enter must meet the Microsoft requirements for acceptable user names and passwords for creating a VM in Microsoft Azure. For the list of requirements, see [username requirements](#) and [password requirements](#) in the Microsoft documentation.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>Type the admin name that you want for the VM’s local administrator account. This local administrator account is created in the VM during the process. This name will be used for the local admin account to access the VM’s operating system, and also used during the convert to image process. This name can be a maximum of 15 characters in length, must not end in a period (&quot;.&quot;), and must not be one of the admin names that are not allowed when creating a VM in Microsoft Azure. <strong>Important</strong> Ensure you can remember this local administrator account information (this name and the password that you specify in the <strong>Password</strong> text box), or that you write it down so you can retrieve the information later. You will need these credentials when you want to add any third-party applications to this base image and when performing the New Image workflow to publish this image to the system.</td>
</tr>
</tbody>
</table>
| **Password**    | Type the password that you want for that administrator account. The password must adhere to the Microsoft Azure password rules:  
- Must not be one of the admin account passwords that are not allowed when creating a VM in Microsoft Azure  
- Must be from 12 through 123 characters in length and meet three out of the following four complexity requirements:  
  - Contain a lowercase character  
  - Contain an uppercase character  
  - Contain a digit  
  - Contain a special character, such as (!@#$%^&*)                                                                 |
| **Verify Password** | Re-type the password.                                                                                                                                                                                                                     |
| **Windows license question** | As you go through making selections in the wizard's user interface, the wizard might display this question in the form of a toggle and check box combination. Follow the on-screen guidance. As described in Licensing section of *VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist For New Pod Deployments*, Horizon Cloud does not provide any guest operating system licensing required for use of Microsoft Windows operating systems that you use in the course of using the Horizon Cloud workflows. You, the customer, have the responsibility to have valid and eligible Microsoft licenses that entitle you to create the Windows-based desktop VMs and RDSH VMs that you choose to use in your Horizon Cloud tenant environment. |
5 In the **Name** field, provide a name for the VM and an optional description.

**Important** Do not enter a name that was previously used for an imported VM that has been converted into an assignable image in your Horizon Cloud environment. For example, if an imported VM was converted into an assignable image so that it is listed on the Images page, do not enter the same name here. Due to a known issue, the VM creation process fails silently if you reuse a name that is already listed on the Images page. The system will not create the VM in Microsoft Azure, however, an error message does not appear in the administrative console.

The name must adhere to the following rules:

- It cannot contain an underscore character (_).
- It can have only alphanumeric characters and the hyphen.
- The name must start with an alphabetic character (not a number).
- The name cannot end with a hyphen (-).

6 Use the toggles in the **Advanced Options** section to customize the Horizon agent features that will be installed in the VM.

When the option's toggle is enabled, the corresponding feature will be installed in the VM. In addition to the options you see selected in this wizard, the workflow process always installs the following key features by default.

- **Horizon agent - HTML5 Multimedia Redirection.** Redirects HTML5 multimedia content in a Chrome or Edge browser to the user's local system to optimize performance.
- **Horizon agent - Horizon Performance Tracker.** Monitors the performance of the display protocol and system resource usage.
- **Horizon agent - vRealize Operations Desktop Agent.** Collects activity-related data from user sessions in the desktop instance or farm RDSH VMs based on this image, and sends that data to the Horizon Cloud cloud monitoring service (CMS) for historical data collection and reporting.
VMware Dynamic Environment Manager client components. The FlexEngine client component is installed using its typical mode. This feature enables use of VMware Dynamic Environment Manager features with the desktop VMs and RDSH VMs that are provisioned based on this image.

Attention  For the Windows 7 Enterprise operating system, the only optional agent features that can be installed using the toggles are the USB Redirection and Help Desk options. Also, even though the system will install the preceding four agent features into a Windows 7 Enterprise VM by default, the HTML5 Multimedia Redirection option and Horizon Performance Tracker are not supported for use in Windows 7 Enterprise.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>App Volumes Agent</strong></td>
<td>The wizard makes this toggle available when the OS choice is set to a client operating system and the Domain Join toggle is enabled. Enable this toggle to install the App Volumes Agent in the base VM to support having images with the ability to provision native applications for end-user VDI desktops.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Tech Preview: Use of App Volumes with Microsoft Windows 10 Enterprise multi-session is currently in tech preview. During this tech preview, use of the wizard’s App Volumes Agent toggle to install the App Volumes Agent into the base VM is not provided when OS is set to one of the Microsoft Windows 10 Enterprise multi-session operating systems. As a result, this toggle is not visible when one of those operating systems is selected. In this case, after you see the imported VM is successfully imported on the Imported VMs page, you must perform some additional steps to configure the imported VM with the App Volumes Agent. See Tech Preview - How To Configure a Microsoft Windows 10 Multi-Session Image for Use with App Volumes Features in Horizon Cloud Pods in Microsoft Azure.</td>
</tr>
<tr>
<td><strong>Enable Flash MMR</strong></td>
<td>Provides the ability to redirect Flash multimedia content that is streamed to the virtual desktop to stream directly to the client computer and decoded on the client system, to optimize performance. The client system plays the media content, offloading the demand on the virtual desktop. This agent option is not supported for use with Microsoft Windows 10 Enterprise multi-session or with Windows 7 Enterprise.</td>
</tr>
<tr>
<td><strong>3D support in RDSH</strong></td>
<td>Applicable when the OS choice is set to a Windows Server or Windows 10 multi-session operating system. Provides 3D graphics support to applications that run on a GPU-enabled RDSH VM.</td>
</tr>
<tr>
<td><strong>3D support in Windows 10 Multi-Session</strong></td>
<td></td>
</tr>
<tr>
<td><strong>MMR for Terminal Services</strong></td>
<td>Provides the ability to redirect multimedia content that is streamed to the virtual desktop to stream directly to the client computer and decoded on the client system, to optimize performance. The client system plays the media content, offloading the demand on the virtual desktop.</td>
</tr>
<tr>
<td><strong>Client Drive Redirection</strong></td>
<td>Allows Horizon Client users to share local drives with their virtual desktops and RDS-based applications.</td>
</tr>
<tr>
<td><strong>Skype for Business</strong></td>
<td>Provides the ability to use the virtual desktops to make optimized audio and video calls with Skype for Business.</td>
</tr>
<tr>
<td><strong>Webcam Support (Real-Time Audio Video RTAV)</strong></td>
<td>Redirects webcam and audio devices that are connected to the users' client systems so that those devices can be used on the virtual desktop.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Smart Card</td>
<td>Not installed by default. Lets users authenticate with smart cards when they use the PCoIP or Blast Extreme display protocol.</td>
</tr>
<tr>
<td>VMware Print</td>
<td>Installs and configures the Horizon Agent's VMware Integrated Printing feature in the imported VM. This feature allows users to use any printer available on their client computers, without installing additional drivers.</td>
</tr>
<tr>
<td>Scanner Redirection</td>
<td>Not installed by default. Redirects scanning and imaging devices that are connected to the users' client systems so that they can be used on the virtual desktop or RDS-based application.</td>
</tr>
<tr>
<td>USB Redirection</td>
<td>Not installed by default. Gives users access to locally connected USB flash drives and hard disks in the virtual desktops and RDS-based applications.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> For guidance on using USB redirection securely, see the Horizon 7 Security guide and the Configuring Remote Desktop Features in Horizon 7 guide. The Horizon version 7.12 of those guides are at security guide and remote desktop features guide. For example, you can use group policy settings to disable USB redirection for specific users.</td>
</tr>
<tr>
<td>URL Redirection</td>
<td>Not installed by default. Allows Horizon Client to determine which URLs should be handled using the virtual desktop or application instead of using the users' client system, and open those URLs using the virtual desktop or RDS-based application.</td>
</tr>
<tr>
<td>Serial Port Redirection</td>
<td>Not installed by default. Redirects devices that are connected to the serial ports on the users' client systems so that they can be used on the virtual desktop or RDS-based application.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Geolocation Redirection</td>
<td>Not installed by default. Allows for sharing the client system's geolocation information with Internet Explorer 11 on the virtual desktop. This option results in the Horizon Geolocation Redirection option installed when the agent is installed in the VM. Additional requirements are needed after the imported VM is ready. For details, see the VMware Horizon documentation topic System Requirements for Geolocation Redirection (Horizon version 7.12).</td>
</tr>
<tr>
<td>Help Desk</td>
<td>Provides the ability to collect real-time performance-related, detailed desktop and session metrics from live desktop sessions. Live sessions are sessions that are active, idle, or disconnected. Logged-off sessions are not in this set of live sessions. Those metrics can help you troubleshoot the health of the virtual desktops. Those metrics are used in About the User Card Feature in Your Horizon Cloud Environment, which is part of the system's help-desk-related features. Note If you turn off this toggle, performance-related metrics from live user sessions in the desktop instances or farm RDSH instances based on this image are not collected. As a result, real-time live user-session data will not be sent to the cloud monitoring service (CMS). As a result, such live user-session data cannot be reported in the user card for such sessions or within reports on the Reports page. For details, see About the User Card Feature in Your Horizon Cloud Environment and Reports Page. To collect historical session data, in addition to the vRealize Operations Desktop Agent that the Import Virtual Machine wizard installs by default, your Horizon Cloud environment must also have the CMS sessions feature enabled in the General Settings page. If the CMS sessions feature is disabled, historical session data will not be available to you in the console. To verify the CMS sessions feature's setting in your environment, see the Monitoring table row in Customizable General Settings for Your Horizon Cloud Tenant Environment.</td>
</tr>
</tbody>
</table>

For extended details about the preceding agent-related options used for VDI desktops and RDS hosts, as well as about all of the Horizon agent features that are always installed by default, see Horizon Agent Custom Setup Options (for those options applicable to a VDI desktop) and Horizon Agent Custom Setup Options for an RDS Host in the VMware Horizon product documentation.

7 Click **Import**.

The system begins creating and configuring the VM. It can take approximately 45 minutes for the overall process to finish at its final point where:

- For pods of manifest 1600 and later, the VM is listed on the Imported VMs page with powered-on status (green dot) and with an agent status of **Not Paired**.
- For pods of manifests prior to 1600, the VM is listed on the Imported VMs page with powered-on status (green dot) an agent status of **Active**.

When the VM is initially instantiated in the Microsoft Azure cloud, its name appears on the Imported VMs page. Use the refresh icon to see the latest status of the VM on the page.
If the VM creation process fails, the system generates a notification about the failure and displays a **Failed** link in the Agent Version column. Clicking that link opens the Notification page where you can read the reason for the failure.

**Important** When creating an image in Microsoft Azure China cloud, the process can take up to two (2) hours to complete. The process is subject to geographic network issues that can cause slow download speeds as the binaries are downloaded from the cloud control plane.

8 If the VM is in a pod of manifest 1600 and later, after the automated process is finished and you refresh the page to see the resulting VM with its green powered-on dot and an agent status of **Not Paired**, use the **Reset Agent Pairing** action on the VM to pair it with **Horizon Cloud**.

**Important** Skip this step if you are using a pod of manifest earlier than 1600. In pods that are at versions earlier than this release, the automated wizard results in a VM that is paired with Horizon Cloud with the agent in active state. If you see the resulting VM has an agent status of **Active** and an agent version number like 19.2, the process is complete.

If your pod has manifest 1600 and later, after the automated process is finished, the resulting VM is not yet paired with Horizon Cloud. The VM's Agent Status column will display **Not Paired (Import Successful)**, as illustrated in the following screenshot.

```
Imported VMs

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>IP Address</th>
<th>Agent Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>lakJun21a</td>
<td>51.143.9.39</td>
<td>Not Paired (Import Successful)</td>
</tr>
</tbody>
</table>
```

**Important** Tech Preview: If you are preparing a VM with Microsoft Windows 10 Enterprise multi-session for use with App Volumes, do not reset the agent pairing at this point. Continue with the steps in **Tech Preview - How To Configure a Microsoft Windows 10 Multi-Session Image for Use with App Volumes Features in Horizon Cloud Pods in Microsoft Azure** before doing the pairing step.

Select the VM and then click **More > Reset Agent Pairing**. The system pairs the VM with the cloud plane. This process can take several minutes to complete. During the pairing process, the VM is restarted and its agent status changes from **Not Paired (Import Successful)** to **Unknown** to **Active**. Use the circular arrow icon to refresh the Imported VMs page to see the VM's current status.
Results

The VM pairing process is completed when the Agent Status column displays Active and an agent version, such as 19.3.0. The following screenshot illustrates a VM after the pairing process is completed.

![Screenshot of VM pairing process](image)

What to do next

Customize the image’s Windows operating system, including configuring things like wallpapers and installing the applications you want the VM to provide to your end users. If you enabled a public IP address for the VM, you can connect to the created VM by using the IP address displayed on the Imported VMs page in an RDP client like Microsoft Remote Desktop Connection. For details, see [Customize the Imported VM’s Windows Operating System](#).

**Note** If your pod is configured to use a proxy, you are responsible for providing a way for the virtual desktop VMs and farm RDSH VMs to be configured with the proxy.

If you selected one of the Microsoft Windows 10 Enterprise multi-session operating systems that includes Office 365, you might need to enable shared computer activation for Office 365 ProPlus so that your end users will be able to use Office 365 applications that are provisioned from the RDS farms based on this VM. For detailed information, see the Microsoft documentation topic [Overview of shared computer activation for Office 365 ProPlus](#).

If you selected **Yes** for **Include GPU**, you must log into the VM’s operating system and install the supported NVIDIA graphics drivers to get the GPU capabilities of the Microsoft Azure GPU-enabled VM. You install the drivers after the VM is created and the Imported VMs page shows that the agent-related status is active. See [Install NVIDIA Graphics Drivers in a GPU-Enabled VM Imported in Horizon Cloud](#).

If you want to use the features of NSX Cloud and its NSX-T Data Center components with the farm RDSH instances or VDI assignment desktop instances based on this VM, you must log into the VM’s operating system and install the NSX agent before publishing the image. See the topics [VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure](#) and [Install the NSX Agent in the Horizon Cloud Imported Image VM](#).

The import process installs the VMware Dynamic Environment Manager client components by default. The FlexEngine client component is installed using its typical mode. The installation path in the resulting VM is `C:\Program Files\VMware\Horizon Agents\User Environment Manager`. If you want to use VMware Dynamic Environment Manager with the desktop VMs and farm RDSH VMs based on this image, configure a separate file server in your Microsoft Azure subscription.
that has at least SMB 2 enabled. Then configure VMware Dynamic Environment Manager using that file server. Also configure the GPO settings that are required when the FlexEngine is installed in its typical mode. For details, see the VMware Dynamic Environment Manager documentation topics in the Dynamic Environment Manager product documentation.

Deciding to Optimize the Windows Image When Using the Import Virtual Machine from Marketplace Wizard

The Import Virtual Machine from Marketplace wizard has an option for configuring the Microsoft Windows operating system in the imported virtual machine (VM) with some specific optimizations. With that option selected, the image creation process results in a VM that is configured in a way that helps prevent failures during the subsequent publishing action on that VM in Horizon Cloud. This wizard option is available for all of the operating systems provided in the Import Virtual Machine wizard.

Important This wizard option is not the equivalent of running the VMware Operating System Optimization Tool (OSOT) and having that tool optimize the VM. Enabling the option in the Import Virtual Machine wizard does not perform the same things that the VMware Operating System Optimization Tool does and does not run the OSOT tool in the VM.

The resulting settings depend on which Windows operating system is installed in the imported VM.

All Windows Operating Systems

When the optimizing option is selected, the image creation process disables the Windows Update feature by:

- Adding a registry property to prevent automatic updates. The property's value is set to 1.

<table>
<thead>
<tr>
<th>Path</th>
<th>Property name</th>
<th>Property value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU</td>
<td>NoAutoUpdate</td>
<td>1</td>
</tr>
</tbody>
</table>

- Stopping and disabling the `wuauserv` service. This system service is used by the Windows Update feature.

Windows 10 Client and Windows 10 Enterprise Multi-Session Operating Systems Only

When the optimizing option is selected, the import VM process disables these scheduled tasks, if present.

<table>
<thead>
<tr>
<th>In Task Scheduler &gt; Task Scheduler Library</th>
<th>Task Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>\Microsoft\Windows\UpdateOrchestrator</td>
<td>Reboot</td>
</tr>
<tr>
<td></td>
<td>Schedule Scan</td>
</tr>
<tr>
<td></td>
<td>USO_Broker_Display</td>
</tr>
</tbody>
</table>
Using the Remove Windows Store Apps Option When Using the Import Desktop Wizard

The Import Desktop wizard has an option for removing most of the Windows Store apps from the non-multi-session Microsoft Windows 10 client-type operating systems on the base virtual machine (VM). With that option selected, the image creation process results in a VM that avoids many of the typical reasons for the image publishing process to fail. Use that option especially to reduce the risk of Sysprep errors from occurring during the publishing process.

**Note** Even when the wizard's **Remove Windows Store Apps** toggle is enabled, the system retains some appx packages by default, based on a system-defined allowed list implemented in the system. The appx packages on this allowed list remain installed in the base VM at the end of the import VM process. For this list of appx packages, see the section at the bottom of this topic.

For creating a VM with a Microsoft Windows 10 operating system, the automated image creation process uses the versions that are available in the Microsoft Azure Marketplace. As described in the Microsoft documentation at [Understand the different apps included in Windows 10](https://docs.microsoft.com/en-us/windows/apps/prerequisites/windows-store-apps-list), Microsoft Windows 10 client-type systems typically include installed Windows apps and provisioned Windows apps, installed in the directory `c:\Program Files\WindowsApps`. In addition to those apps that are pre-installed in that directory, after the operating system is up and running, it will also silently automatically download from the Windows Store and install various Windows Store Apps that Microsoft calls suggested apps. Almost all of these apps can cause issues with the Microsoft System Preparation (Sysprep) utility. The publishing workflow depends on that utility. The Sysprep issues that typically result if many of these Windows apps remain in the VM's operating system are industry known, described in the following resources:

- VMware KB 2079196
- Microsoft KB 2769827
- Microsoft MVP article 615
Removing most of these pre-installed Windows Store apps and preventing the VM’s operating system from automatically and silently installing new suggested ones aims to reduce the risk of such Sysprep issues from occurring when you publish the image. These Windows apps exist as AppX packages in the operating system. When the option to remove Windows Store apps is selected, the image creation process makes the following changes in the VM’s operating system.

- Configures these registry values to disable the Windows Store automatic download and the Microsoft Consumer Experience.

<table>
<thead>
<tr>
<th>Registry Path</th>
<th>Property Name</th>
<th>Value</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\WindowsStore</td>
<td>AutoDownload</td>
<td>2</td>
<td>Disables automatic download of Windows Store apps</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows\CloudContent</td>
<td>DisableWindowsConsumerFeatures</td>
<td>1</td>
<td>Disables the Microsoft Consumer Experience</td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows \CurrentVersion\ContentDeliveryManager</td>
<td>SilentInstalledAppsEnabled</td>
<td>0</td>
<td>Disables the automatic installation of suggested Windows Stores apps that Microsoft Windows will otherwise silently and automatically download and install</td>
</tr>
</tbody>
</table>

- Stops and disables the Windows Store Install Service (InstallService service).

- Removes the AppX packages (files with extension .appx) that are installed in the VM’s operating system and which are not on the system-defined allowed list. The image creation script first gets the names of the AppX packages that are in the VM’s operating system using a command similar to:

```powershell
Get-AppxPackage -AllUsers | Select-Object -Property Name, PackageFullName | Sort-Object -Property Name
```

Then for each AppX package that is not in the system’s allowed list, the script removes the excluded AppX package using commands similar to:

```powershell
Remove-AppxPackage -Name appx-name
```

Then the script also removes the application-provisioning packages associated with each excluded AppX package using commands similar to:

```powershell
Get-AppxProvisionedPackage -Online | Where-Object {$_.DisplayName -like appx-name} | Remove-AppxProvisionedPackage -Online
```
System-Defined Allowed AppX Packages

The following AppX packages are in the system's allowed list by default. They remain in the resulting base VM at the end of the import VM process, even when the Remove Windows Store Apps toggle is enabled.

- 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.XboxIdentityProvider
- Microsoft.XboxSpeechToTextOverlay
- Windows.CBSPreview
- Windows.immersivecontrolpanel
- Windows.PrintDialog

Customize the Imported VM's Windows Operating System

After the imported virtual machine (VM) is created and you have paired it to Horizon Cloud, but before you convert it into a published image, you customize the VM's guest Windows operating system (OS) to install and configure the things you want and need in the image. After the VM has gone through this customization, it is sometimes called a golden image, to indicate the image is configured with all of the items that meet your business needs for the end-user desktops and remote applications that will be based on that image.

Use the links listed further below for the steps to further customize the VM. For additional tuning of the image VM to provide an improved configuration for using VMware Blast Extreme, a best practice is to follow the guidance in Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance from Horizon Cloud Farms and Desktops. Also read the VMware Blast Extreme Optimization Guide and perform additional tuning for codec options in the image according to that guide's recommendations for codec options.
About Ways to Avoid Sysprep Issues If You Did Not Use The Following Options in the Import VM Wizard or When You Manually Created the Base Image VM

If you created the base image using the Import Virtual Machine wizard and you enabled the following listed options in the wizard, the system configured the VM to avoid some typical issues that have been observed during the Microsoft Windows System Preparation (Sysprep) process that runs when the imported VM is converted to a sealed image.

- **Optimize Windows Image** toggle — available in the wizard for all the operating systems selectable in the wizard. This option is described in Deciding to Optimize the Windows Image When Using the Import Virtual Machine from Marketplace Wizard.

- **Remove Windows Store Apps** toggle — available in the wizard for the Windows 10 client-type operating systems. This option is described in Using the Remove Windows Store Apps Option When Using the Import Desktop Wizard.

If you did not use those options in the Import Virtual Machine wizard, or if you manually created the imported VM, sometimes issues have been observed to occur during the sealing process, especially those related to the Microsoft Windows System Preparation (Sysprep) process. In addition to following the steps in the topics linked further below, you might try follow some of the methods listed below before converting the imported VM to a published, sealed image.

- Manually configure the base image VM's services and registry keys according to the same settings the system uses when the **Optimize Windows Image** and **Remove Windows Store Apps** toggles are set to **Yes**. Use the links in the preceding list to read about those settings.

- Remove the Microsoft Windows appx packages as described in VMware KB 2079196, Microsoft KB 2769827, and Microsoft MVP article 615. For Windows 10, run the appx package removal steps under all accounts, removing the same apps from each and every account. Do not delete accounts or profiles from the image until you have run the appx removal steps for every account. For details about the package removal commands that the image creation process runs when you use the Import Virtual Machine wizard's **Remove Windows Store Apps** toggle, see Using the Remove Windows Store Apps Option When Using the Import Desktop Wizard.

- Try following the advice described in the VMware Windows Operating System Optimization Tool Guide. Even though that guide is written in the context of other VMware virtual desktop products and includes mention of Windows operating system other than those supported in your Horizon Cloud environment, it provides details on how to use the VMware OS Optimization Tool (OSOT) on a VM.

**Important** Please keep in mind that, although widely used, the VMware OS Optimization Tool (OSOT) is what is called a VMware fling and therefore its support processes are governed by the VMware Flings Terms of Use. Flings are offered as-is and they are not covered by the VMware Support Request process or the VMware Horizon Service Agreement. As of this writing, the avenue to get help when using the VMware OS Optimization Tool is to use the Comments area at its location in VMware Flings site.
For a Horizon Cloud Imported VM with a Microsoft Windows Client Operating System — Customize the VM for Your Organization's Needs

After the virtual machine (VM) built on a Microsoft Windows client-type operating system is imported and you have paired it to Horizon Cloud, but before converting it into a published image, you customize the guest Windows operating system (OS) to install and configure all of the things you want to have in your end users' VDI desktops. At this time, you install all of the third-party applications you want available in the VDI desktops. Also at this time, you perform any other customizations in the Windows guest operating system, such as installing special drivers required by your organization's needs, applying wallpaper, setting default colors and fonts, configuring taskbar settings, and other such OS-level items. The VM prior to customization is sometimes referred to as an image or base image. After customization, the VM is sometimes referred to as a golden image.

After the Imported VMs page indicates that your imported VM has its agent-related status as active, you connect to it using your RDP software and install the applications into the underlying operating system.

Prerequisites

Verify the Imported VMs page indicates the agent-related status is active for the VM. To get that status for a VM created in a pod at manifest 1600 and higher, use the Imported VMs page's Reset Agent Pairing action on the VM. That action is located in the More drop-down list.

Obtain the VM's IP address as displayed on the Imported VMs page.

Note When using the Microsoft Remote Desktop Client as your RDP software to connect to the VM, ensure it is the most up-to-date version. For example, the default RDP software in the Windows 7 operating system is not at a high enough version. The version must be version 8 or higher.

Verify you have at least one of the following credentials (user name and password) to log in to the VM's guest Windows operating system, according to how the VM was created.
### When the VM was created | How the VM was created | Credentials to use to log in
--- | --- | ---
Prior to the December 2019 service release going live in production | Import Virtual Machine wizard, from the Imported VMs page. | Prior to the December 2019 service release date, the Import Virtual Machine wizard created VMs that were always automatically joined to the Active Directory domain that was specified in the wizard. To log in to such a VM, you can use one of the following:
- The credentials for the local administrator account that were specified in the wizard.
- The credentials for a domain account in that Active Directory domain.

After the December 2019 service release went live in production | Import Virtual Machine wizard, from the Imported VMs page. | Starting with the December 2019 service release date, the Import Virtual Machine wizard provides the option of either having the wizard-created VM joined to a specified Active Directory domain or not having the VM joined to the domain at the end of the creation process.
- If the VM was created with the wizard’s **Domain Join** toggle enabled, you can use either the credentials for a domain account in the specified Active Directory domain or use the local administrator account that was specified in the wizard.
- If the VM was created with the wizard’s **Domain Join** toggle turned off, you must use the local administrator account that was specified in the wizard. In this case, because the VM is not joined to the domain, the local administrator account is the only account that has access to log in.

In any service release | Manual preparation steps in [Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud](#). | Typically you do not need to join the VM to your Active Directory domain when you manually build the VM. To log in to that VM, use one of the following:
- The credentials for the local administrator account that was specified when the manually built VM was created in the Microsoft Azure portal.
- If you manually joined that VM to an Active Directory domain, the credentials for a domain account in that domain.

---

**Important** Starting with pod manifest 1230 and later, domain accounts can direct connect to domain-joined image VMs that have the agent software installed. Prior to pod manifest 1230, the agent software installed in a domain-joined VM prevented domain accounts from directly connecting to that VM. However, if you have not yet updated your pod to a manifest of 1230 and later, before a domain account can direct connect to a domain-joined image VM that has the agent software installed, you must first perform the steps in [When Your Pod is Not Yet Updated to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image](#).
Procedure

1. Use the VM's IP address in your RDP software to connect to the VM's operating system.
   - If the VM was created with a public IP address, you can use that IP address in your RDP software.
   - If the VM has a private IP address, you must RDP into it by one of these two methods:
     - Using another VM in your Microsoft Azure subscription that does have a public IP address and doing an outbound RDP into the imported VM.
     - Use your VPN and RDP into the VM over your corporate network.

   **Note** To access a VM that is running the agent-related software components, the version of the Remote Desktop Client must be version 8 or later. Otherwise, the connection fails. Using the most up-to-date Remote Desktop Client is recommended.

2. Log in to the Windows operating system using credentials (user name and password) as described in the prerequisites here.

   When using the local administrator account credentials that were specified in the Import Image wizard when the VM was created, enter the username as \username.

   **Note** When the VM is a domain-joined VM, as described in the prerequisites here, and you want to use a domain account instead of the local administrator account, enter the user name as domain\username where domain is the name of the domain.

3. When you are logged in to the operating system, install the third-party applications or drivers that you want available for your end users to run in the VDI desktop environment.

4. In the operating system, install any custom drivers you want in the VDI desktops.

5. Make any customizations or configurations you want to have in the VDI desktops, such as add a custom wallpaper, set default fonts or colors or themes, adjust the taskbar default settings, and so on.

6. When you are done adding your finishing touches to the VM's guest operating system, sign out of the operating system.

What to do next

Optimize the image based on your intended business scenario. See the guidance in Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance from Horizon Cloud Farms and Desktops.

Follow the best practices to optimize the VM to prevent encountering sysprep or other errors during the process to convert the golden image to an assignable image in Horizon Cloud, also known as publishing or sealing the image. See Customize the Imported VM's Windows Operating System.

Convert the golden image to an assignable image, using the steps described in Convert a Configured Image VM to an Assignable Image in Horizon Cloud.
For a Horizon Cloud Imported VM with a Microsoft Windows 10 Enterprise Multi-
Session Operating System — Customize the VM for Your Organization's Needs

After the virtual machine (VM) built on a Microsoft Windows 10 Enterprise multi-session operating system is imported and you have paired it to Horizon Cloud, but before converting it into a published image, you customize the guest operating system (OS) to install and configure all of the things you want to have in the RDSH VMs from which your end users’ remote applications and session-based desktops will be provisioned. At this time, you install all of the third-party applications you want available in the session-based desktops or available for assignment as remote applications. Also at this time, you perform any other customizations in the Windows guest operating system, such as installing special drivers required by your organization's needs, applying wallpaper, setting default colors and fonts, configuring taskbar settings, and other such OS-level items. The VM prior to customization is sometimes referred to as an image or base image. After customization, the VM is sometimes referred to as a golden image.

Tip As described in the Microsoft documentation FAQ, Microsoft Windows 10 Enterprise multi-session is a Remote Desktop Session Host (RDSH) type that allows multiple concurrent interactive sessions, which previously only Microsoft Windows Server operating systems could provide. Because Microsoft Windows 10 Enterprise multi-session is an RDSH type of operating system, it will appear in the Horizon Cloud RDSH-applicable workflows when your Horizon Cloud tenant account configuration provides for its use.

After the Imported VMs page indicates that your imported VM has its agent-related status as active, you connect to it using your RDP software and install the applications into the underlying operating system.

Prerequisites

If the imported VM is running one of the Microsoft Windows 10 Enterprise multi-session systems that includes Office 365 ProPlus by default, as part of customizing the operating system, you might have to configure that Office 365 ProPlus for shared computer activation as described in the Microsoft documentation topic Overview of shared computer activation for Office 365 ProPlus. Read that Microsoft documentation topic to determine how you want to configure Office 365 ProPlus for shared computer activation.

Verify the Imported VMs page indicates the agent-related status is active for the VM. To get that status, use the Imported VMs page's Reset Agent Pairing action on the VM. That action is located in the More drop-down list.

Obtain the VM's IP address as displayed on the Imported VMs page.

Tip When using the Microsoft Remote Desktop Client as your RDP software to connect to the VM, ensure it is the most up-to-date version. The version must be version 8 or higher.

Verify you have at least one of the following credentials (user name and password) to log in to the VM's guest Windows operating system, according to how the VM was created.
## How the VM was created

<table>
<thead>
<tr>
<th>How the VM was created</th>
<th>Credentials to use to log in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Virtual Machine wizard, from the Imported VMs page.</td>
<td>The Import Virtual Machine wizard provides the option of either having the wizard-created VM joined to a specified Active Directory domain or not having the VM joined to the domain at the end of the creation process.</td>
</tr>
<tr>
<td></td>
<td>■ If the VM was created with the wizard's <strong>Domain Join</strong> toggle enabled, you can use either the credentials for a domain account in the specified Active Directory domain or use the local administrator account that was specified in the wizard.</td>
</tr>
<tr>
<td></td>
<td>■ If the VM was created with the wizard's <strong>Domain Join</strong> toggle turned off, you must use the local administrator account that was specified in the wizard. In this case, because the VM is not joined to the domain, the local administrator account is the only account that has access to log in.</td>
</tr>
<tr>
<td>Manual preparation steps in <strong>Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud</strong>.</td>
<td>Typically you do not need to join the VM to your Active Directory domain when you manually build the VM. To log in to that VM, use one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ The credentials for the local administrator account that was specified when the manually built VM was created in the Microsoft Azure portal.</td>
</tr>
<tr>
<td></td>
<td>■ If you manually joined that VM to an Active Directory domain, the credentials for a domain account in that domain.</td>
</tr>
</tbody>
</table>

## Procedure

1. Use the VM’s IP address in your RDP software to connect to the VM’s operating system.
   - If the VM was created with a public IP address, you can use that IP address in your RDP software.
   - If the VM has a private IP address, you must RDP into it by one of these two methods:
     - Using another VM in your Microsoft Azure subscription that does have a public IP address and doing an outbound RDP into the imported VM.
     - Use your VPN and RDP into the VM over your corporate network.

   **Remember** When using the Microsoft Remote Desktop Client as your RDP software to connect to the VM, ensure it is the most up-to-date version. The version must be version 8 or higher.

2. Log in to the Windows operating system using credentials (user name and password) as described in the prerequisites here.

   When using the local administrator account credentials that were specified in the Import Image wizard when the VM was created, enter the username as `\username`.

   **Note** When the VM is a domain-joined VM, as described in the prerequisites here, and you want to use a domain account instead of the local administrator account, enter the user name as `domain\username` where `domain` is the name of the domain.
3. When you are logged in to the operating system, install the third-party applications or drivers that you want available for your end users in the session-based desktops or to run as remote applications.

4. In the operating system, install any custom drivers you want available in the RDSH hosts.

5. Make any customizations or configurations you want to have in the session-based desktops, such as add a custom wallpaper, set default fonts or colors or themes, adjust the taskbar default settings, and so on.

6. When you are done adding your finishing touches to the VM’s guest operating system, sign out of the operating system.

What to do next

If the VM is based on one of the Microsoft Windows 10 Enterprise multi-session choices that includes Office 365 ProPlus by default, additional steps might be required. You might have to configure that Office 365 ProPlus for shared computer activation as described in the Microsoft documentation topic Overview of shared computer activation for Office 365 ProPlus. Read that Microsoft documentation topic to determine how you want to configure Office 365 ProPlus for shared computer activation and use the method appropriate for your situation.

Optimize the image based on your intended business scenario. See the guidance in Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance from Horizon Cloud Farms and Desktops.

Follow the best practices to optimize the VM to prevent encountering sysprep or other errors during the process to convert the golden image to an assignable image in Horizon Cloud, also known as publishing or sealing the image. See Customize the Imported VM’s Windows Operating System.

Convert the golden image to an assignable image, using the steps described in Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

For a Horizon Cloud Imported VM with a Microsoft Windows Server Operating System — Customize the VM for Your Organization’s Needs

After the VM built on a Microsoft Windows Server operating system is imported and you have paired it to Horizon Cloud, but before converting it into a published image in Horizon Cloud, but before converting it into a published image, you customize the guest operating system (OS) to install and configure all of the things you want to have in the RDSH VMs from which your end users’ remote applications and session-based desktops will be provisioned. Also at this time, you perform any other customizations in the Windows guest operating system, such as installing special drivers required by your organization’s needs, applying wallpaper, setting default colors and fonts, configuring taskbar settings, and other such OS-level items. The VM prior to customization is sometimes referred to as an image or base image. After customization, the VM is sometimes referred to as a golden image.
After the Imported VMs page indicates that your imported VM has its agent-related status as active, you connect to it using your RDP software and install the applications into the underlying operating system.

For Microsoft's best practices about installing applications directly on to an RDSH server, see the TechNet Magazine article Learn How to Install Applications on an RD Session Host Server.

**Prerequisites**

Verify the Imported VMs page indicates the agent-related status is active for the VM. To get that status for a VM created in a pod at manifest 1600 and higher, use the Imported VMs page's **Reset Agent Pairing** action on the VM. That action is located in the **More** drop-down list.

Obtain the VM's IP address as displayed on the Imported VMs page.

**Note** When using the Microsoft Remote Desktop Client as your RDP software to connect to the VM, ensure it is the most up-to-date version. For example, the default RDP software in the Windows 7 operating system is not at a high enough version. The version must be version 8 or higher.

Verify you have at least one of the following credentials (user name and password) to log in to the VM's guest Windows operating system, according to how the VM was created.
When the VM was created | How the VM was created | Credentials to use to log in
--- | --- | ---
Prior to the December 2019 service release going live in production | Import Virtual Machine wizard, from the Imported VMs page. | Prior to the December 2019 service release date, the Import Virtual Machine wizard created VMs that were always automatically joined to the Active Directory domain that was specified in the wizard. To log in to such a VM, you can use one of the following:
- The credentials for the local administrator account that were specified in the wizard.
- The credentials for a domain account in that Active Directory domain.

After the December 2019 service release went live in production | Import Virtual Machine wizard, from the Imported VMs page. | Starting with the December 2019 service release date, the Import Virtual Machine wizard provides the option of either having the wizard-created VM joined to a specified Active Directory domain or not having the VM joined to the domain at the end of the creation process.
- If the VM was created with the wizard’s **Domain Join** toggle enabled, you can use either the credentials for a domain account in the specified Active Directory domain or use the local administrator account that was specified in the wizard.
- If the VM was created with the wizard’s **Domain Join** toggle turned off, you must use the local administrator account that was specified in the wizard. In this case, because the VM is not joined to the domain, the local administrator account is the only account that has access to log in.

In any service release | Manual preparation steps in Manualy Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud. | Typically you do not need to join the VM to your Active Directory domain when you manually build the VM. To log in to that VM, use one of the following:
- The credentials for the local administrator account that was specified when the manually built VM was created in the Microsoft Azure portal.
- If you manually joined that VM to an Active Directory domain, the credentials for a domain account in that domain.

**Important** Starting with pod manifest 1230 and later, domain accounts can direct connect to domain-joined image VMs that have the agent software installed. Prior to pod manifest 1230, the agent software installed in a domain-joined VM prevented domain accounts from directly connecting to that VM. However, if you have not yet updated your pod to a manifest of 1230 and later, before a domain account can direct connect to a domain-joined image VM that has the agent software installed, you must first perform the steps in When Your Pod is Not Yet Updated to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image.
Procedure

1. Use the VM's IP address in your RDP software to connect to the VM's operating system.
   - If the VM was created with a public IP address, you can use that IP address in your RDP software.
   - If the VM has a private IP address, you must RDP into it by one of these two methods:
     - Using another VM in your Microsoft Azure subscription that does have a public IP address and doing an outbound RDP into the imported VM.
     - Use your VPN and RDP into the VM over your corporate network.

   **Note** To access a VM that is running the agent-related software components, the version of the Remote Desktop Client must be version 8 or later. Otherwise, the connection fails. Using the most up-to-date Remote Desktop Client is recommended.

2. Log in to the Windows operating system using credentials (user name and password) as described in the prerequisites here.

   When using the local administrator account credentials that were specified in the Import Image wizard when the VM was created, enter the username as \username.

   **Note** When the VM is a domain-joined VM, as described in the prerequisites here, and you want to use a domain account instead of the local administrator account, enter the user name as domain\username where domain is the name of the domain.

3. When you are logged in to the operating system, follow these steps to install the third-party applications or drivers that you want available to run in the multi-user RDS desktop environment.

   a. In the Windows Server operating system, open a command prompt as an administrator by right-clicking the Start and clicking Command Prompt (Admin).

   b. In that command prompt, determine the server's current install mode of the server by issuing the command change user /query.

      The response Application EXECUTE mode is enabled indicates the server is in RD-Execute mode.
In that command prompt, switch the server into RD-Install mode by issuing the command `change user /install`.

As described in the Microsoft best practices document, RD-Install is a special install mode to install applications so they can run in a multi-user environment.

Install the third-party user applications you want to provide to your end users in their RDS desktops or as remote applications.

When you are finished installing the applications, return to the command prompt window and switch the server into RD-Execute mode by issuing the command `change user /execute`.

In the operating system, install any custom drivers you want in the RDS desktops.

Make any customizations or configurations you want to have in the RDS desktops, such as add a custom wallpaper, set default fonts or colors or themes, adjust the taskbar default settings, and so on.

When you are done adding your finishing touches to the VM's guest operating system, sign out of the operating system.

What to do next

Optimize the image based on your intended business scenario. See the guidance in Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance from Horizon Cloud Farms and Desktops.

Follow the best practices to optimize the VM to prevent encountering sysprep or other errors during the process to convert the golden image to an assignable image in Horizon Cloud, also known as publishing or sealing the image. See Customize the Imported VM's Windows Operating System.

Convert the golden image to an assignable image, using the steps described in Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance from Horizon Cloud Farms and Desktops

Different end users have different needs. After you have customized a golden image for use in your Horizon Cloud environment, you'll want to ensure it will result in giving your end users optimal performance when using their assigned desktops and applications that are based on that
image. This topic provides some prescriptive guidance to help you in achieving the optimal performance based on end-user personas.

This topic includes the following sections:

- The Five Key Steps
- Optional: Install a User Experience Monitoring Tool
- Codec Selections and VM Series Sizing Recommendations For Farms Used By Various End User Personas and Workload Types

**Tip** Among other sources, these five key steps are informed by the VMware Digital Workspace Tech Zone's *VMware Blast Extreme Optimization Guide* and *Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop*.

### The Five Key Steps

1. To prepare the image's Microsoft Windows operating system for the optimal remote experience, download the [VMware OS Optimization Tool fling](#) to the golden image VM, run the tool, and follow the tool's on-screen advice.

![VMware OS Optimization Tool](vmware-os-optimization-tool.png)

**Note** The Terms of Use page of the VMware Flings site states that all VMware Flings are provided on an as-is and as-available basis. As of this writing, to get help on the VMware OS Optimization Tool, use the Comments area within its location in the VMware Flings site.
In the golden image's operating system, enable the setting to use the WDDM graphics display driver for Remote Desktop Connections. This setting can be enabled in multiple ways. One way to enable the settings is using the Local Group Policy Editor:

a. In the Local Group Policy Editor, navigate to **Local Computer Policy > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment**. The following screenshot is an illustration of this location.

b. Set the policy named **Use WDDM graphics display driver for Remote Desktop Connections** to **Enabled**.
You must restart the VM after enabling the WDDM graphics display driver for the changes to take effect.

3 In the VM, set a codec that is appropriate for the anticipated end-user workloads.

For VDI desktop assignments, see the Codec Options section of the VMware Blast Extreme Optimization Guide and its table of ideal applications for each codec.

For farms, which use images built on Microsoft Windows 10 Enterprise multi-session or Windows Server operating systems, see the guidelines in the following section Codec Selections and VM Series Sizing Recommendations For Farms Used By Various End User Personas and Workload Types.

**Important** As described in Table 2 of the VMware Blast Extreme Optimization Guide's Enabling Codecs and Codec Options section, some codec options require a corresponding Horizon Client setting. For the Blast codec and H.264 codec, the end users must make an appropriate selection in their Horizon Client.

4 As described in Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it with Horizon Cloud, under Advanced Options, the wizard gives you options to enable Horizon remote experience features in the golden image at the time it is being created. Some of those toggles are enabled by default for installation in the image. In the wizard, you should verify that only those remote experience features that are specifically required by your business needs are enabled before you submit the wizard to create the VM. As a simple example, the client drive redirection toggle is on by default, and unless you have determined your business needs require your end users to have client drive redirection, you would disable that toggle to prevent enabling the client drive redirection.

5 Ensure the VM is set for your desired performance by opening the VM's System Properties > Advanced System Settings > Performance Options and verifying the settings. The optimal setting is Adjust for best performance. The following screenshot illustrates the location of these settings.
Optional: Install a User Experience Monitoring Tool

Installing a user experience monitoring tool helps to measure various performance metrics within the VM's operating system, such as FPS, bandwidth, CPU consumption, codec type, and so on. One such tool is the third-party tool RDAnalyzer.

Codec Selections and VM Series Sizing Recommendations For Farms Used By Various End User Personas and Workload Types

The following VM examples and sizing suggestions are based on typical workloads from farms in Horizon Cloud. Farms provision session-based desktops and remote applications to your end users. Farms are based on images that are running Microsoft Windows 10 Enterprise multi-session or Microsoft Windows Server operating systems. You must determine the optimal sizing that will give you the best results in your individual business scenarios. To help you determine that optimal sizing, VMware recommends you use simulation tools to run tests in your environment, especially as Microsoft debuts newer and faster VM sizes over time. If you need additional guidance, please contact your VMware representative. For more details about setting the codecs listed below, see the VMware Blast Optimization Guide's Enabling Codecs and Codec Options and Configuration Settings for Administrators sections.
<table>
<thead>
<tr>
<th>VM Series in Microsoft Azure</th>
<th>Workload Type</th>
<th>Maximum Users per vCPU/Total Users</th>
<th>Personas</th>
<th>Optimal Codec</th>
<th>Description</th>
<th>Application Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>D2s_v3, F2s_v2</td>
<td>Light</td>
<td>Maximum per vCPU = 6 Total = 12</td>
<td>Task worker</td>
<td>Blast codec</td>
<td>Low CPU and bandwidth usage. Tighter bandwidth and frame rate control for optimal experience.</td>
<td>Database entry applications, command-line interfaces (CLIs)</td>
</tr>
<tr>
<td>D4s_v3, F4s_v2</td>
<td>Medium</td>
<td>Maximum per vCPU = 4 Total = 16</td>
<td>Consultants and market researchers</td>
<td>Blast codec</td>
<td>Low CPU and bandwidth usage. Tighter bandwidth and frame rate control for optimal experience.</td>
<td>Database entry applications, command-line interfaces (CLIs), Microsoft Word, static web pages</td>
</tr>
<tr>
<td>VM Series in Microsoft Azure</td>
<td>Workload Type</td>
<td>Maximum Users per vCPU/Total Users</td>
<td>Personas</td>
<td>Optimal Codec</td>
<td>Description</td>
<td>Application Examples</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>-----------------------------------</td>
<td>----------</td>
<td>---------------</td>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>D4s_v3, F4s_v2</td>
<td>Heavy</td>
<td>Maximum per vCPU = 2 Total = 8</td>
<td>Engineers and content creators</td>
<td>H.264</td>
<td>Moderate CPU and bandwidth usage. Good experience for multimedia.</td>
<td>Database entry applications, command-line interfaces (CLIs), Microsoft Word, static web pages, Microsoft Outlook, Microsoft PowerPoint, dynamic web pages</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D4s_v3, F4s_v2, NV6</td>
<td>Power</td>
<td>Maximum per vCPU = 1 Total = 4</td>
<td>Graphics designers</td>
<td>H.264</td>
<td>Moderate CPU and bandwidth usage. Can deliver exceptional experience for multimedia and 3D graphics applications by changing the frame rate to 60 FPS (frames per second). When using NV6, leverage hardware acceleration for graphics.</td>
<td>Database entry applications, command-line interfaces (CLIs), Microsoft Word, static web pages, Microsoft Outlook, Microsoft PowerPoint, dynamic web pages, Adobe Photoshop, Adobe Illustrator, computer-aided design (CAD), computer-aided manufacturing (CAM)</td>
</tr>
</tbody>
</table>

**Additional Information**

For more information on optimizing VMs for remote experience use cases, see:

- The Microsoft documentation topic [Virtual machine sizing guidelines](#), which includes sizing recommendations for Microsoft Windows 10 Enterprise multi-session when the VM is running on Windows Virtual Desktop (WVD).
- [VMware Blast Extreme Optimization Guide](#) at the VMware Digital Workspace Tech Zone
Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop also at the VMware Digital Workspace Tech Zone

Install NVIDIA Graphics Drivers in a GPU-Enabled VM Imported in Horizon Cloud

If you imported a VM with GPU, you must log into the VM's Microsoft Windows operating system and install the supported NVIDIA graphics drivers to get the GPU capabilities of that VM. You install the drivers after the VM is created and the Imported VMs page shows the agent-related status is active.

Obtain the NVIDIA GRID driver that is appropriate for the VM's Windows operating system. See the Microsoft Azure documentation topic at Set up GPU drivers for N-series VMs running Windows.

Note: In this release, when using a Microsoft Windows Server operating system, GPU is recommended for use only in Microsoft Windows Server 2016, due to an NVIDIA driver limit on the number of user sessions in Microsoft Windows Server 2012 R2. The imported VM must be based on Microsoft Windows Server 2016.

Install the driver following the installation instructions in the Driver installation section of the Microsoft article Set up GPU drivers for N-series VMs running Windows.

Caution: Install the NVIDIA GRID drivers listed on that Microsoft page and not other drivers.

Prerequisites

Verify the Imported VMs page indicates the agent-related status is active for the VM. To get that status for a VM created in a pod at manifest 1600 and higher, use the Imported VMs page's Reset Agent Pairing action on the VM. That action is located in the More drop-down list.

Note: When using the Microsoft Remote Desktop Client as your RDP software to connect to the VM, ensure it is the most up-to-date version. For example, the default RDP software in the Windows 7 operating system is not at a high enough version. The version must be version 8 or higher.

Verify you have at least one of the following credentials (user name and password) to log in to the VM’s guest Windows operating system, according to how the VM was created.
<table>
<thead>
<tr>
<th>When the VM was created</th>
<th>How the VM was created</th>
<th>Credentials to use to log in</th>
</tr>
</thead>
</table>
| Prior to the December 2019 service release going live in production | Import Virtual Machine wizard, from the Imported VMs page. | Prior to the December 2019 service release date, the Import Virtual Machine wizard created VMs that were always automatically joined to the Active Directory domain that was specified in the wizard. To log in to such a VM, you can use one of the following:  
  - The credentials for the local administrator account that were specified in the wizard.  
  - The credentials for a domain account in that Active Directory domain. |
| After the December 2019 service release went live in production | Import Virtual Machine wizard, from the Imported VMs page. | Starting with the December 2019 service release date, the Import Virtual Machine wizard provides the option of either having the wizard-created VM joined to a specified Active Directory domain or not having the VM joined to the domain at the end of the creation process.  
  - If the VM was created with the wizard's Domain Join toggle enabled, you can use either the credentials for a domain account in the specified Active Directory domain or use the local administrator account that was specified in the wizard.  
  - If the VM was created with the wizard's Domain Join toggle turned off, you must use the local administrator account that was specified in the wizard. In this case, because the VM is not joined to the domain, the local administrator account is the only account that has access to log in. |
| In any service release | Manual preparation steps in Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud. | Typically you do not need to join the VM to your Active Directory domain when you manually build the VM. To log in to that VM, use one of the following:  
  - The credentials for the local administrator account that was specified when the manually built VM was created in the Microsoft Azure portal.  
  - If you manually joined that VM to an Active Directory domain, the credentials for a domain account in that domain. |

**Important** Starting with pod manifest 1230 and later, domain accounts can direct connect to domain-joined image VMs that have the agent software installed. Prior to pod manifest 1230, the agent software installed in a domain-joined VM prevented domain accounts from directly connecting to that VM. However, if you have not yet updated your pod to a manifest of 1230 and later, before a domain account can direct connect to a domain-joined image VM that has the agent software installed, you must first perform the steps in **When Your Pod is Not Yet Updated to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image.**
Procedure

1. Use the VM's IP address in your RDP software to connect to the VM's Windows operating system.
   - If the VM was created with a public IP address, you can use that IP address in your RDP software.
   - If the VM has a private IP address, you must RDP into it by one of these two methods:
     - Using another VM in your Microsoft Azure subscription that does have a public IP address and doing an outbound RDP into the imported VM.
     - Use your VPN and RDP into the VM over your corporate network.

   **Note** To access a VM that is running the agent-related software components, the version of the Remote Desktop Client must be version 8 or later. Otherwise, the connection fails. Using the most up-to-date Remote Desktop Client is recommended.

2. Log in to the Windows operating system using credentials (user name and password) as described in the prerequisites here.

   When using the local administrator account credentials that were specified in the Import Image wizard when the VM was created, enter the username as \username.

   **Note** When the VM is a domain-joined VM, as described in the prerequisites here, and you want to use a domain account instead of the local administrator account, enter the user name as domain\username where domain is the name of the domain.

3. Install the drivers as described in the Driver installation section of the Microsoft article Set up GPU drivers for N-series VMs running Windows.

4. When the drivers are installed, restart the VM.

5. Reconnect to the VM, log in, and verify that the NVIDIA driver is installed and working in the VM.

   In the VM, open the Device Manager, expand Display Adapters, and verify the proper installation of the NVIDIA driver.

6. Sign out of the VM's Windows operating system.

**Convert a Configured Image VM to an Assignable Image in Horizon Cloud**

After you have customized the imported VM to where it matches your business needs for the desktops and remote applications that you want provisioned to your end users, that VM is now your golden image. To turn that golden image into an assignable image, use the New Image...
workflow on the Image page of the Horizon Cloud Administration Console. An image must display the Published status on the Images page before the system can use it for assignments.

**Warning**  After you publish the image and it is in its sealed state in Horizon Cloud, do not use the Microsoft Azure Portal to perform actions on that image VM. Using the Microsoft Azure Portal to perform direct actions on a VM that is in the published state in Horizon Cloud is unsupported and will cause unexpected behavior. Always use the Horizon Cloud Administration Console to perform actions on sealed images.

**Important**  If your pod in Microsoft Azure is configured to use a proxy, you are responsible for providing a way for the farm VMs or VDI desktop VMs that are created using this image to be configured with the proxy.

**Prerequisites**
Verify that a configured image is available in the pod in which you want to create the assignable image.

Verify that the Imported VMs page indicates that the VM is powered on (green status) and its agent-related status is active, as illustrated in the following screenshot.

![Screenshot of Import VMs page](image-url)

Verify you have the credentials of an enabled local administrator account in the image VM. The system uses the local administrator account in the image sealing process, which converts a golden image into the published state. Typically, the VM’s only enabled local administrator account is the one that you named when you created the image VM, as described in *Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure* and its subtopics.

**Important**  Unless you manually added additional local administrator accounts to the image VM, the VM’s only local administrator account is the one you specified when you ran the Import VM wizard, or when you manually created the VM for the golden image.

**Procedure**
1. In the console, click **Inventory > Images** and then click **New**.
2 Enter the required information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Select the location associated with the pod where you have the configured image. This field filters the set of pods that will appear for selection in the Pod list.</td>
</tr>
<tr>
<td>Pod</td>
<td>Select the pod that has the configured image.</td>
</tr>
<tr>
<td>Tip</td>
<td>If you do not see any pods to select, verify that the Location list is not displaying a location without pods. The Location field works on the Pod list to filter out pods that are not associated with the selected location. If you previously had a pod at a location and then deleted that pod or moved it to a different location, so that the displayed location no longer has any pods, the Pod list will display no entries. Because the locations are listed alphabetically, when the screen opens, it automatically selects the one that is first in the alphabet. If that location no longer has any pods associated with it, you must switch the location to a different entry.</td>
</tr>
<tr>
<td>Desktop</td>
<td>This field lists the VMs located on the selected pod that the system can convert to an assignable image. Select the one you want. After you make a selection, information about the selected VM is displayed, such as its status.</td>
</tr>
<tr>
<td>Image Name</td>
<td>This field is auto-populated with the image name associated with the Desktop selection.</td>
</tr>
<tr>
<td>Company Name</td>
<td>Type an identifying name. This name will appear in the virtual desktops that get created based on this image. The publishing process sets the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \RegisteredOwner to this value. The name will appear in the About Windows dialog in those virtual desktops as the registered organization and owner.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Retain the default.</td>
</tr>
<tr>
<td>Admin credentials for the desktop</td>
<td>Enter the credentials for the local administrator account that is enabled in the image VM. Usually the only enabled local administrator account is the one that was named when the image VM was created.</td>
</tr>
</tbody>
</table>

Note The publishing process includes running the Microsoft Windows Sysprep process. When the VM has a Microsoft Windows server operating system, the Sysprep process will reset the built-in administrator account password to this password that you type here. This password reset is done to secure the built-in administrator account after the Sysprep process has completed. The built-in administrator password is reset to the password you type here whether you specify the built-in administrator account or another local administrator account in this step.

3 Click **Publish**.

The publishing process takes several minutes to complete. The page displays the **In Transition** status during this process. You can use the refresh icon to see the latest status.
Results

If the process is successful, the image's status changes to Published.

**Note** When the image is in Published status, it is considered sealed in Horizon Cloud. Sealed images are those VMs that the system can use in RDSH farms for delivering session-based desktops and remote applications (in the case of RDSH-capable Windows operating systems) or use in VDI desktop assignments (in the case of Windows client operating systems).

If you find you need to change something in a sealed VM's guest Windows operating system, use the steps in the following topics, as appropriate for the situation:

- To update a sealed image with an RDSH type of operating system, such as Microsoft Windows Server or Windows 10 Enterprise multi-session operating system, see [Change Images Used for Farms in Horizon Cloud](#).
- To update a sealed image with a Microsoft Windows client operating system, see [Change Images Used for VDI Desktop Assignments](#).

Images in Published status are not listed on the Imported VMs page. They are removed from the Imported VMs page when they reach Published state. At that point, those sealed VMs are available on the Images page.

If the publish operation fails, select Monitor > Activity and locate the failed job. Correct the problem, then retry the publish operation by selecting the check box next to the image, clicking More > Convert to Desktop. Then click New, enter the required information, and click Publish to publish the image.

**Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud**

These steps are part of the alternative manual method for importing a VM for use as a golden image in a pod in Microsoft Azure. Manually building a virtual machine (VM) that conforms to the environment's requirements for importing into Horizon Cloud is a multi-step process. You perform most of these steps in the Microsoft Azure portal. You first create and configure a base VM, then install agent-related software components into that base VM, and then configure specific properties for those agent-related components.
Use these steps only if you do not want to use the automated wizard and instead want to manually build the VM using the Microsoft Azure portal or if you have already manually built a VM using the Microsoft Azure portal and you want to use that VM as the basis of a golden image in Horizon Cloud. The recommended automated way to build a golden image for a pod in Microsoft Azure is to use the wizard. For details about using the automated wizard, see Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it with Horizon Cloud.

**Important** If you have a VM in Microsoft Azure that you want to import into Horizon Cloud for a golden image, you must ensure it conforms to the same criteria as when a VM is built and imported using the manual steps documented in Create the Virtual Machine Manually in Your Pod in Microsoft Azure. If the VM does not conform to the same criteria, Horizon Cloud cannot consume it to display in its console and use in the Convert to Image workflow. The following criteria are critical:

- Before installing the agent-related software, the base VM must have the **Storage - Use managed disk** setting set to Yes. If the base VM does not adhere to this setting, Horizon Cloud cannot consume this VM.
- The base VM must be in the same Microsoft Azure location as the pod where you want to use that base VM.
- The base VM must be put into a specific resource group in your Microsoft Azure subscription. This resource group is one that belongs to the pod where you plan to use that base VM. The resource group is named `vmw-hcs-podID-base-vms`, where `podID` is the pod’s UUID identifier.
- The base VM must be connected to the same virtual network to which the pod is connected.
- The base VM must be connected to the pod’s subnet named `vmw-hcs-podID-net-tenant`.
- The base VM must use an operating system currently supported for use in this Horizon Cloud release. Links to knowledge base articles about the supported operating systems can be found in the documentation topic Horizon Cloud — Environments, Operating Systems, and Compatibility.
- Do not configure the base VM to use IPv6 IP addresses. Horizon Cloud will report an IP abnormal alert in the Desktop Health tab for VMs that are based on a VM that uses IPv6 IP addresses.

To verify your base VM meets that criteria before you start to configure it further, log in to Horizon Cloud, navigate to the Inventory VMs page, and verify your base VM is listed on that page. If it is listed, then that base VM meets the above criteria and you can safely proceed with the remaining configuration steps starting with the topics listed in Prepare the Manually Created VM Prior to Installing the Agents.

**Procedure**

1. Create the Virtual Machine Manually in Your Pod in Microsoft Azure
2 Prepare the Manually Created VM Prior to Installing the Agents

When manually building and importing a virtual machine (VM) for your pod in Microsoft Azure, you must perform several additional tasks to further prepare the base VM before installing the agent-related software components. You perform these steps using the Microsoft Azure portal and connecting into the new VM.

3 Install the Agents and Pair the Manually Created Base Virtual Machine with Horizon Cloud

Starting with the September 2019 service release, the steps to pair the manually created base VM with the cloud plane have changed. Use one set of steps when your pod is at manifest version 1600 and higher and use the other set of steps when your pod is at a version lower than 1600.

Create the Virtual Machine Manually in Your Pod in Microsoft Azure

In the Microsoft Azure portal, you create a virtual machine (VM) with the Windows guest operating system that you want to use for the VDI client-based desktops, RDS-based session desktops, or RDS-based remote applications. You create this VM using the same subscription that you used for the Horizon Cloud pod.

This VM must be created on the same Microsoft Azure VNet (virtual network) to which the pod is connected. Also, this VM must be created in the resource group named `vmw-hcs-podID-base-vms`, where `podID` is the pod's UUID identifier. Horizon Cloud automatically detects VMs located in that resource group. Horizon Cloud will list those VMs on the Inventory screen in the console if they have Storage-Use managed disk set to Yes.
For your imported VMs, you can use Microsoft Windows VMs that are available in the Microsoft Azure portal’s VM catalog and which match the operating systems currently supported for use in this release of Horizon Cloud. Links to knowledge base articles about the supported operating systems can be found in this release’s Environments, Operating Systems, and Compatibility section of the release notes.

**Note** The Import VM from Marketplace automated method of importing a VM uses the following specific VM families when it creates a VM. Typically you would choose to use these same patterns when you manually create a VM for importing into Horizon Cloud. Because you will later choose the VM types for the actual RDS-based VMs and VDI client-based desktops when you create the farms and VDI desktop assignments, there are few reasons to use VM sizes for the imported VM that are larger than the ones that the Import VM from Marketplace automated process uses. Potentially, you might want to try a larger size if you are going to load applications into the VM and test them out before sealing the golden image based on that VM.

- Non-GPU RDS-based operating systems: D2 V3 Standard type
- Non-GPU client-based operating systems: D4 V3 Standard type
- GPU-backed RDS-based operating systems: NV6 Standard type
- GPU-backed client-based operating systems: NV6 Standard type

If the Microsoft Azure region in which the pod is deployed does not include the D2 V3 or D4 V3 Standard types, the automated Import VM from Marketplace process will fall back to use the D2 V2 Standard (for RDS-based OSes) and D3 V2 Standard (for client-based OSes).

For details about the Microsoft Azure VM types and sizes for Horizon Cloud, see [VMware Knowledge Base article 77120](https://kb.vmware.com/kb/77120). For VM size details in the Microsoft Azure documentation, see [Sizes for Windows virtual machines in Azure](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/size-options).

**Note** The Microsoft VM types that support GPU acceleration, the NV-series types, are only available in some Microsoft Azure regions. To have GPU-based desktops or remote applications available from the pod, the pod must be in a Microsoft Azure region in which the specific NV-series VM types are available. See [Microsoft Azure Products by region](https://azure.microsoft.com/en-us/services/) for details.

**Prerequisites**

Obtain the following information about the pod for which you are creating the VM. To see this information, open the pod’s details in the Horizon Cloud administrative console by navigating to **Settings > Capacity** and clicking the pod’s name. Obtain from the pod's Summary tab:

- The name of the virtual network to which your pod is connected. You must select the same virtual network when creating the VM.
- The pod’s ID for the pod for which you are creating the VM. The pod’s ID is an identifier in UUID form. You need this UUID to identify that pod’s resource groups in the Microsoft Azure portal, so that you know in which resource group to locate the VM.
If the pod was deployed with a manually created subnet, obtain the name of the desktop (tenant) subnet. You must select that same subnet when creating the VM.

**Procedure**

1. Log in to the Microsoft Azure portal using the Microsoft Azure account associated with the subscription used to deploy the pod.
2. Navigate into the pod's `vmw-hcs-podID-base-vms` resource group by clicking **Resource Groups** in the portal's left navigation, locating that specific resource group, and then clicking its name.
   
   To list only the resource groups for a particular pod, on the **Resource groups** screen, type that pod's ID into the **Filter by name** field.
3. In the screen for that `vmw-hcs-podID-base-vms` resource group, click **Add**.
4. Locate the Microsoft Windows operating system that you want to use.
   
   Choose the operating system based on whether you want to provision VDI client-based desktops or RDS-based desktops or remote applications using this base VM. Links to knowledge base articles about the operating systems supported by Horizon Cloud can be found in the documentation topic **Horizon Cloud — Environments, Operating Systems, and Compatibility**.

   **Important** If you want to have GPU-based RDS-based desktops, avoid Microsoft Windows Server 2012 R2. An NVIDIA driver limitation will limit the number of end-user sessions you can have accessing each Windows Server 2012 R2 farm VM to a maximum of 20 sessions on each.

   Do not select Microsoft Windows 7 if you want to have GPU-based desktops. Using Windows 7 with GPU is not supported in Horizon Cloud.
5. Click the one you want for the base VM.
6. In the new pane, verify it says **Deploy with Resource Manager** under the **Create** button, and then click **Create**.
   
   The portal displays the wizard steps for creating the virtual machine, open to the **Basics** step.

   The following screenshot is an illustration of the displayed wizard steps when Windows 10 Pro N, Version 1809 was selected.
Create a virtual machine

<table>
<thead>
<tr>
<th>Basics</th>
<th>Disks</th>
<th>Networking</th>
<th>Management</th>
<th>Guest config</th>
<th>Tags</th>
<th>Review + create</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Looking for elastic VMs? Create VM from Azure Marketplace</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PROJECT DETAILS**
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

<table>
<thead>
<tr>
<th>Subscription</th>
<th>HCS-XXXXX</th>
</tr>
</thead>
</table>

7 In the **Basics** step, complete the required fields and then click **Next: Disks** to save your values and go to the next step.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription</td>
<td>Keep the default setting of your subscription selected.</td>
</tr>
<tr>
<td>Resource group</td>
<td>Select the base-vms resource group for the pod from which you want to serve the virtual desktops and applications (vmw-hcs-podID-base-vms).</td>
</tr>
<tr>
<td>Virtual machine name</td>
<td>Give this VM a name of up to 15 alphanumeric characters.</td>
</tr>
<tr>
<td>Region</td>
<td>Select the region that matches the Microsoft Azure region in which your pod is deployed.</td>
</tr>
<tr>
<td>Note</td>
<td>If you want to have a GPU-based VM, the pod's Microsoft Azure region must have the NV-series VM types available. The NV-series types are not available in all Microsoft Azure regions.</td>
</tr>
<tr>
<td>Availability options</td>
<td>Keep the default (No infrastructure redundancy).</td>
</tr>
<tr>
<td>Image</td>
<td>Verify the selection matches the Windows operating system you want.</td>
</tr>
<tr>
<td>Size</td>
<td>Choose a size for the VM. If you want to choose according to the ones used by the system's automated Import VM from Marketplace wizard, those are: Non-GPU RDS-based operating systems: D2 V3 Standard type Non-GPU client-based operating systems: D4 V3 Standard type GPU-backed RDS-based operating systems: NV6 Standard type GPU-backed client-based operating systems: NV6 Standard type</td>
</tr>
<tr>
<td>Note</td>
<td>Horizon Cloud does not support using GPU NV series with Microsoft Windows 7.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter a name for the VM's default administrator account.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password for the default administrator account, and confirm it. The password must adhere to the password complexity rules that Microsoft Azure defines for the VM. Typically the password must be at least 12 characters long have three of the following: one lower case character, one upper case character, one number, and one special character that is not backslash () or hyphen (-).</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
<tr>
<td>Public inbound ports</td>
<td>If you want to be able to install the agents by connecting to the VM over the Internet using RDP, select <strong>Allow selected ports</strong> and select <strong>RDP</strong> (port 3389).</td>
</tr>
<tr>
<td>SAVE MONEY section</td>
<td>Follow the on-screen instructions. Select the choices appropriate for the valid licensing that your organization has for use with the Microsoft operating system that you selected.</td>
</tr>
</tbody>
</table>
The following screenshot illustrates some of the settings when Microsoft Windows 10 ProN, Version 1809 is the selected VM type.

8 In the Disks step, select either Standard SSD or Standard HDD for the OS disk type. If this VM will be used for GPU-based virtual desktops or applications, select Standard HDD for the disk type. Otherwise, you can either keep the default SSD setting or select HDD, according to your needs.

9 (Optional) In the Disks step, if you want the virtual desktops or RDSH instances that will be based on this base image to have data disks, use the DATA DISKS section to create and attach data disks to this base VM.

In the Create a new disk window, for the Source type, select None (empty disk). For the other choices, you can keep the defaults or change them. You can customize the name of the data disk. When you have specified the required settings, click OK.

The following screenshot is an illustration of the Create a new disk window with its fields filled out.
When the disk is listed on the Disks step, you can optionally select a Host caching setting for the data disk. Typically you choose a setting according to what you think will work best for your intended use of the data disk.

In the Disks step, expand the ADVANCED section and confirm that the Use managed disks toggle is set to Yes.

**Caution** You must keep Use managed disk set to Yes. If the VM does not have Use managed disk set to Yes before you run the installer that installs the agent-related software components, Horizon Cloud cannot use this VM and you have to create another one.

The following screenshot is an illustration with one data disk specified.
11 Click Next: Networking to move to the next step.

12 In the Networking step, configure the virtual network and subnet settings as described below, and then click Review + create to save your entries and go to the review step.

Keep the default values for the other settings.

Attention
- As described in the prerequisites section above, you must set the Virtual network to the same VNet that the pod uses.
- Do not alter the defaults for the other options in the Networking screen (such as no extensions). Keep the defaults for those options. Do not make changes other than what is mentioned in the following table.
Virtual network | Click **Virtual network** and select the same virtual network (VNet) to which the pod is connected.

Subnet | Click **Subnet** and select the one that is your pod's desktop (tenant) subnet. If the pod deployer automatically created the subnets when the pod was deployed, this subnet is named `vmw-hcs-podID-net-tenant`.

---

**Create a virtual machine**

**Basics** | **Disks** | **Networking** | **Management** | **Guest config** | **Tags** | **Review + create**
---

**NETWORK INTERFACE**
When creating a virtual machine, a network interface will be created for you.

**CONFIGURE VIRTUAL NETWORKS**

- **Virtual network**
  - vmw-hcs-<tenant>
  - Create new

- **Subnet**
  - Manage subnet configuration

- **Public IP**
  - (new) a45manualwin10-ip
  - Create new

- **NIC network security group**
  - None
  - Basic
  - Advanced

- **Public inbound ports**
  - None
  - Allow selected ports

- **Select Inbound ports**
  - RDP

- **Accelerated networking**
  - On
  - Off

  The selected image does not support accelerated networking.

**LOAD BALANCING**

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution?
- Yes
- No

---

After you click **Review + create**, a validation runs. When it passes, the wizard moves to the final step.
13 In the final step, review the summary and verify the settings, especially the resource group, virtual network, subnet, and **Use managed disks** is set to **Yes**.

The resource group and subnet names contain the pod’s UUID (**podID**).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource group</td>
<td><code>vmw-hcs-podID-base-vms</code></td>
</tr>
<tr>
<td>Use managed disks</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual network</td>
<td>The pod’s virtual network.</td>
</tr>
<tr>
<td>Subnet</td>
<td><code>vmw-hcs-podID-net-tenant</code></td>
</tr>
</tbody>
</table>

Start deploying the VM by clicking the **Create** button at the bottom of the pane.

**Results**

Microsoft Azure starts deploying the new VM into the resource group. When the VM is deployed successfully in Microsoft Azure, the Horizon Cloud console’s Imported VMs page lists the VM. The
page shows the VM’s agent state as Not Paired, because you have not installed the agent-related components yet.

![Imported VMs](image)

**Note** If you have adhered to the conditions such as creating the VM with managed disks, attaching it to the pod’s primary tenant subnet, and locating it in the pod’s base-vms resource group — and yet you are not seeing the VM listed on the page — that could be due to a rare issue where the pod is not recognizing VMs that do not have tags on them. To work around this issue, in the Microsoft Azure portal, manually add a tag to the VM. The tag can be any value. In the Microsoft Azure portal, on the VM’s Overview page, where it says Tags (change), click change and add a tag. Then refresh the Imported VMs page.

**What to do next**

Fully deploying the VM can take several minutes. When the portal’s dashboard indicates that the VM is created and ready, make a remote desktop connection to the VM’s public IP address and continue configuring the base VM. Complete the steps in **Prepare the Manually Created VM Prior to Installing the Agents**.

**Prepare the Manually Created VM Prior to Installing the Agents**

When manually building and importing a virtual machine (VM) for your pod in Microsoft Azure, you must perform several additional tasks to further prepare the base VM before installing the agent-related software components. You perform these steps using the Microsoft Azure portal and connecting into the new VM.

Follow the steps in the topics below according to type of Microsoft Windows operating system that is installed in the VM.

**Prepare the Server VM for Agent Installation Needed by Horizon Cloud**

Use the following steps to prepare a manually created server VM, that you plan to use for your pod’s RDSH farms. You perform these steps before you install the Horizon Cloud agent-related software. Use the Microsoft Azure portal and connect into the new VM.

At a high level, the steps to prepare the VM prior to actually installing the agents are:

1. Enable the RDS role.
2 Set the VM’s local administrator account properties to **Password never expires**. By default, the created VM’s local security policy has accounts set to a maximum password age of 42 days. Preventing this local administrator account’s password from expiring prevents the possibility of being locked out from using this local account later. The Horizon Cloud image publishing workflow uses the VM’s local administrator account and removes the resulting sealed VM from the domain. If you allow the account’s password to expire, at a future point in time you might find you cannot log in to the VM using that account.

3 Download the Horizon Agents Installer to the VM.

**Prerequisites**

Complete the steps in *Create the Virtual Machine Manually in Your Pod in Microsoft Azure*. If you are using a base VM that you created in Microsoft Azure outside of those documented steps, ensure that your base VM meets the criteria as listed in *Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud*.

**Caution** Ensure that the VM was created with **Storage - Use managed disk** set to **Yes** and with the correct virtual network and subnet, as described in *Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud*. Otherwise, this VM will be unusable in Horizon Cloud even after you configure it and install the agent-related components, and then you will have to recreate it from scratch.

To verify that the VM meets that criteria before you spend time configuring it, log in to Horizon Cloud and navigate to the **Inventory VMs** page to see if the VM is listed. If it is listed, then the VM meets the required criteria and you can safely proceed with further configuration.

**Procedure**

1 In the portal’s dashboard, click the icon for the VM to open its overview page.

2 Click **Connect**.

   ![WSvr2012R2](image)

   Depending on your browser settings, your browser downloads an RDP file or prompts you to save or run it.

3 Use this RDP file to open a remote desktop connection to the VM.

   Use the default user name and password that you specified in the VM creation wizard. To log in without a domain, include a backslash (\) in front of the user name.
4. Click **Yes** to the certificate warning in the Remote Desktop Connection screen.

Because this login is the first login to the operating system, Windows displays a Networks prompt question on the right-hand side. The prompt asks about automatically finding PCs, devices, and other items on the network.

The Server Manager automatically opens to its first-time configuration wizard.

5. Close the Networks prompt on the right-hand side of the screen by clicking **No**.

6. Enable the RDS role in the VM using the following steps.

   Enabling the RDS role allows using this server VM in RDSH farms for providing session-based desktops and remote applications.
   a. In Microsoft Azure portal, connect to the powered-on VM as described in **Step 2**.
   b. In the Server Manager dashboard, click **Add roles and features**.
   c. Go through the wizard, selecting **Role-based or feature-based installation**.
   d. On the **Server Selection** step, retain the defaults and click **Next**.
   e. On the **Server Roles** step, select **Remote Desktop Services** and click **Next**.
   f. On the **Features** step, retain the defaults and click **Next**.
   g. Click to the **Role Services** step and select **Remote Desktop Session Host**.
   h. Optionally keep the setting for the prompt about Remote Desktop Licensing Diagnoser Tools.
Start the process.

The wizard starts installing the RDS role. When the screen indicates that a restart is pending, close the wizard and close your RDP session.

In the Microsoft Azure portal, click **Stop** on the VM to power it off completely.

When the portal reflects the VM is completely stopped, click **Start** to power it on again.

Reconnect to the powered-on VM as described previously.

When the wizard displays the Completion step and you see the success messages, click **Close** to close the wizard.

In the VM, set the VM's local administrator account password to **Password never expires**.

One way to set the local administrator account password is to open Local Users and Groups by running `lusrmgr.msc` and updating the account properties.

To enable Internet Explorer temporarily to download the Horizon Agents Installer software, turn off the **IE Enhanced Security Configuration** for both administrators and users.

### What to do next

To install the agent-related software components, complete the steps described in the topic that applies to your pod manifest version:

- **For Pods at Manifest 1600 and Higher, Install the Agent-Related Software Components in the Base Virtual Machine and Pair it with Horizon Cloud**
- **For Pods at Manifests Lower Than 1600, Install the Agent-Related Software Components in the Base Virtual Machine**

**Note** If you want to enable logging in to the VM using a domain account, you can optionally join the VM to your Active Directory domain. Otherwise you use the local administrator account to log in to the VM when installing the agent software and customizing the VM.

Prepare the **Microsoft Windows 10 Enterprise Multi-Session VM for Agent Installation Needed by Horizon Cloud**

The following steps are for manually preparing a VM that has a Microsoft Windows 10 Enterprise multi-session operating system, prior to installing the agents. You perform these steps using the Microsoft Azure portal and connecting into the new VM.

**Remember** As described in the [Microsoft documentation FAQ](https://docs.microsoft.com/en-us/windows/how-to/), Microsoft Windows 10 Enterprise multi-session is a Remote Desktop Session Host (RDSH) type that allows multiple concurrent interactive sessions, which previously only Microsoft Windows Server operating systems could provide. When your Horizon Cloud tenant account configuration allows for its use, you can make use of Microsoft Windows 10 Enterprise multi-session in your Horizon Cloud environment.
At a high-level, the steps to prepare the VM prior to actually installing the agents are:

1. Set the VM’s local administrator account properties to **Password never expires**. By default, the created VM's local security policy has accounts set to a maximum password age of 42 days. Preventing this local administrator account's password from expiring prevents the possibility of not being able to use this local account at a later time. The Horizon Cloud image publishing workflow uses the VM’s local administrator account and removes the resulting sealed VM from the domain. If you allow the account's password to expire, at a future point in time you might encounter issues when publishing the image.

2. Download the Horizon Agents Installer to the VM.

**Prerequisites**

Complete the steps in Create the Virtual Machine Manually in Your Pod in Microsoft Azure. If you are using a base VM that you created in Microsoft Azure outside of those documented steps, ensure your base VM meets the criteria as listed in Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud.

**Caution** Ensure that the VM was created with **Storage - Use managed disk** set to **Yes** and with the correct virtual network and subnet, as described in Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud. Otherwise, this VM will be unusable in Horizon Cloud even after you configure it and install the agent-related components, and then you will have to recreate it from scratch.

To verify the VM meets that criteria before you spend time configuring it, log in to Horizon Cloud and navigate to the Inventory VMs page to see if the VM is listed. If it is listed, then the VM meets the above criteria and you can safely proceed with further configuration.

**Procedure**

1. In the portal's dashboard, click the icon for the VM to open its overview page.

2. Click **Connect**.

   ![Connect button](image)

   Depending on your browser settings, your browser downloads an RDP file or prompts you to save or run it.
3 Use that RDP file to open a remote desktop connection to the VM.

Use the default user name and password that you specified in the VM creation wizard. Include a backslash (\) in front of the user name to log in without a domain.

![Windows Security: Enter your credentials]

4 Click Yes to the certificate warning in the Remote Desktop Connection screen.

Because this is the first login to the operating system, Windows might display a Networks prompt question on the right hand side. The prompt asks about automatically finding PCs, devices, and other items on the network. If the Networks prompt is displayed, dismiss it by clicking No.

5 In the VM, set the VM’s local administrator account password to Password never expires.

One way to set the local administrator account password is to open Local Users and Groups by running lusrmgr.msc and updating the account properties.

What to do next

To install the agent-related software components, complete the steps described in the topic that applies to your pod manifest version:

- For Pods at Manifest 1600 and Higher, Install the Agent-Related Software Components in the Base Virtual Machine and Pair it with Horizon Cloud
- For Pods at Manifests Lower Than 1600, Install the Agent-Related Software Components in the Base Virtual Machine

**Note** If you want to be able to log in to the VM using a domain account, you can optionally join the VM to your Active Directory domain. Otherwise you use the local administrator account to log in to the VM when installing the agent software and customizing the VM.

Prepare the VDI Desktop VM for Agent Installation Needed by Horizon Cloud

The following steps are for manually preparing a VM that has a Microsoft Windows client operating system, prior to installing the agents. You perform these steps using the Microsoft Azure portal and connecting into the new VM.
At a high-level, the steps to prepare the VM prior to actually installing the agents are:

1. Set the VM’s local administrator account properties to **Password never expires**. By default, the created VM’s local security policy has accounts set to a maximum password age of 42 days. Preventing this local administrator account’s password from expiring prevents the possibility of not being able to use this local account at a later time. The Horizon Cloud image publishing workflow uses the VM’s local administrator account and removes the resulting sealed VM from the domain. If you allow the account’s password to expire, at a future point in time you might encounter issues when publishing the image.

2. Download the Horizon Agents Installer to the VM.

**Prerequisites**

Complete the steps in Create the Virtual Machine Manually in Your Pod in Microsoft Azure. If you are using a base VM that you created in Microsoft Azure outside of those documented steps, ensure your base VM meets the criteria as listed in Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud.

**Caution** Ensure that the VM was created with **Storage - Use managed disk** set to **Yes** and with the correct virtual network and subnet, as described in Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud. Otherwise, this VM will be unusable in Horizon Cloud even after you configure it and install the agent-related components, and then you will have to recreate it from scratch.

To verify the VM meets that criteria before you spend time configuring it, log in to Horizon Cloud and navigate to the Inventory VMs page to see if the VM is listed. If it is listed, then the VM meets the above criteria and you can safely proceed with further configuration.

**Procedure**

1. In the portal’s dashboard, click the icon for the VM to open its overview page.

2. Click **Connect**.

   ![Connect button](image)

   Depending on your browser settings, your browser downloads an RDP file or prompts you to save or run it.
Use that RDP file to open a remote desktop connection to the VM.

Use the default user name and password that you specified in the VM creation wizard. Include a backslash (\) in front of the user name to log in without a domain.

![Windows Security - Enter your credentials](image)

Click **Yes** to the certificate warning in the Remote Desktop Connection screen.

Because this is the first login to the operating system, Windows might display a Networks prompt question on the right hand side. The prompt asks about automatically finding PCs, devices, and other items on the network. If the Networks prompt is displayed, dismiss it by clicking **No**.

In the VM, set the VM's local administrator account password to **Password never expires**.

One way to set the local administrator account password is to open Local Users and Groups by running `lusrmgr.msc` and updating the account properties.

**What to do next**

To install the agent-related software components, complete the steps described in the topic that applies to your pod manifest version:

- **For Pods at Manifest 1600 and Higher, Install the Agent-Related Software Components in the Base Virtual Machine and Pair it with Horizon Cloud**
- **For Pods at Manifests Lower Than 1600, Install the Agent-Related Software Components in the Base Virtual Machine**

**Note** If you want to be able to log in to the VM using a domain account, you can optionally join the VM to your Active Directory domain. Otherwise you use the local administrator account to log in to the VM when installing the agent software and customizing the VM.

**Install the Agents and Pair the Manually Created Base Virtual Machine with Horizon Cloud**

Starting with the September 2019 service release, the steps to pair the manually created base VM with the cloud plane have changed. Use one set of steps when your pod is at manifest version 1600 and higher and use the other set of steps when your pod is at a version lower than 1600.
Follow the steps in the topics below according to the pod manifest version of the pod in which you manually created the VM. You can see the pod's manifest version by navigating to the pod's details page from the Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types.

**Caution** You must install the agent-related software using a version of Horizon Agents Installer that is appropriate for the pod's manifest level. This point is especially important when your pod is of manifest 1600 and lower. If you try to use a version of the Horizon Agent Installer that was made available for use with a later pod manifest, the version-specific steps to subsequently pair the VM with the cloud will not work for you. As an example, when your pod has a manifest version between 1493 and 1600, install Horizon Agents Installer 19.2 into the base VM. When the manifest version is between 1273 and 1493, install Horizon Agents Installer 19.1 into the base VM.

For Pods at Manifest 1600 and Higher, Install the Agent-Related Software Components in the Base Virtual Machine and Pair it with Horizon Cloud

For a pod at a manifest higher than 1600, follow the steps described here to install the agent-related components that are required and appropriate for Horizon Cloud and pair it with the cloud plane. In the base virtual machine's Windows operating system, you run the Horizon Agents Installer. After rebooting the VM, you pair the VM with the cloud plane using the Horizon Cloud administrative console.

Keep the following points in mind as you perform this task:

- The steps in this documentation topic are specifically for pods that are at manifest version 1600 and higher. Those manifest versions were first made available in the service's September 2019 release. If the pod is at a manifest version lower than 1600, use the steps in the following documentation topic instead: For Pods at Manifests Lower Than 1600, Install the Agent-Related Software Components in the Base Virtual Machine. You can check your pod’s manifest version on the pod’s details page from the Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types.

  **Caution** When your pod is of manifest lower than 1600, do not attempt to use these steps. The pairing mechanism changed for pod manifest 1600 and higher. If you attempt to use these steps for a manually created base VM located in a pod of manifest lower than 1600, the final pairing process will fail and you will have to uninstall the agent software and re-install it using a Horizon Agents Installer version that aligns with your pod manifest level.

- Installing a version of the Horizon Agents Installer into a Windows VM that is four or more versions older than the version that aligns with your pod's manifest version can cause downstream issues when you create farms and VDI desktop assignments based on the image VM. As an example, if you create a farm based on an image VM in which you installed an older version of Horizon Agents Installer, the system might allow you to select HTML Access (Blast) as a protocol. However, this selection will not be applied to the farm's RDS VMs even though it appears to have been applied successfully. For the Horizon Agents Installer version
that aligns with your pod manifest version, locate the Release Notes document from the VMware Horizon Cloud Service documentation page and find the What's New section that cites your pod manifest version. The corresponding Horizon Agents Installer version will be listed nearby.

- The Help Desk Plugin option is installed by default. If you choose not to install this option, performance-related metrics from user sessions in the desktop instances or farm RDSH instances based on this image are not collected. As a result, some data will not be available in the user card for such sessions. For details, see About the User Card Feature in Your Horizon Cloud Environment.

- The vRealize Operations Desktop Agent option is installed by default. If you choose not to install this option, activity-related data from user sessions in the desktop instance or farm RDSH instances based on this image is not reported to Horizon Cloud. As a result, data from end-user activity and other types of desktop activity will not be displayed in reports in the console.

- The App Volumes Agent option is not enabled by default. Selecting that option installs the App Volumes Agent, which enables use of this VM to add App Volumes applications into your inventory and leverage the App Volumes features in your Horizon Cloud environment. See App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites.

- The Dynamic Environment Manager option is not enabled by default. Selecting that option installs the VMware Dynamic Environment Manager client component, known as the FlexEngine. Selecting that option installs FlexEngine using its typical mode. The typical mode requires a post-installation configuration step to configure the VMware Dynamic Environment Manager Group Policy. For VMware Dynamic Environment Manager usage information, see the Dynamic Environment Manager product documentation. VMware Dynamic Environment Manager provides various options for achieving the persistence of end-user data, settings, and profiles of desktops provisioned by your pod.

Note When the Dynamic Environment Manager option is selected for installation, its resulting installation path is C:\Program Files\VMware\Horizon Agents\User Environment Manager.

Prerequisites

Verify that the virtual machine (VM) is created and configured as described in Create the Virtual Machine Manually in Your Pod in Microsoft Azure and Prepare the Manually Created VM Prior to Installing the Agents.

Verify that the pod in which this VM is created has a manifest version higher than 1600. The pairing steps in the following procedure apply when the pod has a manifest version of 1600 or higher. You can check your pod's manifest version on the pod's details page from the Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types.
Procedure

1. Navigate to where you downloaded the installer and start it.

   **Important** If you want to use the URL redirection option with the desktops or RDS-based remote applications resulting from this base VM, you must use the command line to start the installer, adding the `VDM_URL_FILTERING_ENABLED=1` parameter to the command.

   For example,

   ```
   VMware-Horizon-Agents-Installer-x.y.z-build-x64.exe VDM_URL_FILTERING_ENABLED=1
   ```

   Where `x.y.z` and `build` match the numbers in the file name.

   After a few minutes, the installation wizard displays its Welcome screen. The installer detects whether it is running on a client operating system or on a Remote Desktop Session Host (RDSH) type of operating system and displays the appropriate Welcome screen. The RDSH types of operating systems include Microsoft Windows server operating systems that have the RDS role enabled and the Microsoft Windows 10 Enterprise multi-session operating systems.

   - For a VM running a Microsoft Windows client operating system, the Horizon Cloud Endpoint Desktop image is displayed.

   ![VMware Horizon® Agents Installer v20.2.0](image)

   By installing you agree to the License Terms.

   Cancel

   - For a VM running a Remote Desktop Session Host (RDSH) type of operating system, the Horizon Cloud RDSH App image is displayed.
2 Click **Configure**.

The wizard's next step displays. The following screenshot is an example of this step when running on a VM with an RDSH-type of operating system.
Note For Windows 7 Enterprise VMs, only those agent options that are supported for use in Windows 7 Enterprise operating systems are available for selection.

3 Scroll down to see the feature options.

The following screenshot is an example of this step when running on a VM with an RDSH-type of operating system.
Select the check boxes for the features you want to install and click the arrow to move to the next step.

If the VM is a GPU-backed Windows RDSH-type operating system VM, select the 3DRDSH option.

**Note**  If you do not install the Help Desk Plugin option, performance-related metrics from user sessions in the desktop instances or farm RDSH instances based on this image are not collected. As a result, some data will not be available in the user card for such sessions. For details, see About the User Card Feature in Your Horizon Cloud Environment.

If prompted with a message about using USB redirection securely, click **OK**.

The final wizard step displays.

**Click Proceed with installation.**

The installer begins installing the components.

**Note**  If a message displays asking for confirmation to install the VMware display adapters, click **Install**.

When all the components are installed, the wizard displays Finish. The following screenshot is an illustration of the list of installed components when running the installer on an RDSH-capable image and only selecting default options. The specific entries might vary depending on the operating system and options you select.
7 When the wizard signals it is finished, click **Finish**.

8 Click **Restart Now** to reboot the VM and have the configuration changes take effect.
9  When the VM is powered back on, use the **Reset Agent Pairing** action in Horizon Cloud to pair it with your Horizon Cloud environment.

   a  Navigate to **Inventory > Imported VMs** and make sure that the VM has a green dot next to it that indicates the VM is powered on.

   Even though the agent software is installed on the VM, the VM is not yet paired with Horizon Cloud. The VM’s Agent Status column will display **Not Paired**, as illustrated in the following screenshot.

   ![Imported VMs](image)

   b  Select the VM, and select **More > Reset Agent Pairing** to pair the VM with Horizon Cloud.

   **Note**  The pairing process can take several minutes to complete. During the pairing process, the VM is restarted and its agent status changes from **Not Paired** to **Unknown** to **Active**. Use the circular arrow icon to refresh the Imported VMs page to see the VM’s current status.

**Results**

The VM pairing process is completed when the Agent Status column displays **Active** and an agent version, such as **20.2.0**. The following screenshot illustrates a VM after the pairing process is completed. At this point, the base VM conforms to the Horizon Cloud environment's requirements to create an assignable image, also referred to as a sealed image.

![Imported VMs](image)

**What to do next**

If you joined the VM to your Active Directory domain, you can use domain accounts to connect to the VM to customize the image. If you did not join the VM to your Active Directory domain, you can use the local administrator account to connect to the VM to customize the image.
Customize the image's Windows operating system, including configuring things like wallpapers and installing the applications you want this VM to provide to your end users. If you enabled a public IP address for the VM, you can connect to the created VM by using the IP address displayed on the Imported VMs page in an RDP client like Microsoft Remote Desktop Connection. For details, see Customize the Imported VM’s Windows Operating System and its subtopics:

- For Microsoft Windows Server operating systems: For a Horizon Cloud Imported VM with a Microsoft Windows Server Operating System — Customize the VM for Your Organization's Needs
- For Microsoft Windows 10 Enterprise multi-session operating systems: For a Horizon Cloud Imported VM with a Microsoft Windows 10 Enterprise Multi-Session Operating System — Customize the VM for Your Organization's Needs
- For Microsoft Windows client-type operating systems: For a Horizon Cloud Imported VM with a Microsoft Windows Client Operating System — Customize the VM for Your Organization's Needs

**Important** It is recommended that you optimize the image VM as described in Customize the Imported VM's Windows Operating System, Deciding to Optimize the Windows Image When Using the Import Virtual Machine from Marketplace Wizard, and Using the Remove Windows Store Apps Option When Using the Import Desktop Wizard.

**Tip** To further tune the image VM to provide an improved configuration for using VMware Blast Extreme, a best practice is to follow the guidance in Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance from Horizon Cloud Farms and Desktops. Another best practice is to read the VMware Blast Extreme Optimization Guide and perform additional tuning for codec options in the image according to that guide's recommendations for codec options.

If you selected to install the App Volumes Agent, continue with the subtopics described in App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites to add App Volumes applications to your inventory.

If you selected to install the Dynamic Environment Manager option, configure a separate file server in your Microsoft Azure subscription that has at least SMB 2 enabled. Then configure VMware Dynamic Environment Manager using that file server. Also configure the GPO settings. See the VMware Dynamic Environment Manager documentation topics in the Dynamic Environment Manager product documentation.

For improved security regarding the use of the Horizon Agent, configure your Active Directory server domain policy GPO (Group Policy Object) to disable weak ciphers in SSL and TLS protocols. For information about disabling weak ciphers when communicating using the SSL/TLS protocol, see the appropriate agent-related information in the VMware Horizon® documentation set, such as Disable Weak Ciphers in SSL/TLS.
If you selected a NV-series VM type, you must log into the VM’s operating system and install the supported NVIDIA graphics drivers to get the GPU capabilities of the GPU-enabled NV-series VM. You install the drivers after the VM is created and the Imported VMs page shows the agent state is active for the VM. See Install NVIDIA Graphics Drivers in a GPU-Enabled VM Imported in Horizon Cloud.

After you are finished customizing the image, use the New Image workflow to convert the image to an assignable image. See Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

**For Pods at Manifests Lower Than 1600, Install the Agent-Related Software Components in the Base Virtual Machine**

For a pod at a manifest lower than 1600, you first install the agent-related components that are required and appropriate for Horizon Cloud. You do this install by running the Horizon Agents Installer in the base virtual machine’s Windows operating system. After rebooting the VM, then you must manually pair the VM with the cloud plane.

Keep the following points in mind as you perform this task:

- The steps in this documentation topic are specifically for pods that are at manifest version lower than 1600. The manifest versions 1600 and higher were first made available in the service's September 2019 release. If the pod has a manifest version of 1600 or higher, use the steps in the following documentation topic instead: For Pods at Manifest 1600 and Higher, Install the Agent-Related Software Components in the Base Virtual Machine and Pair it with Horizon Cloud. You can check your pod's manifest version on the pod's details page from the Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types.

- For a Windows Server VM, installing a version of the Horizon Agents Installer that is older than the one suitable for your pod's manifest can cause problems subsequently when you create RDS pools based on the image VM. In this situation, when you create a new RDS pool, the system can allow you to select HTML Access (Blast) as a protocol, but this selection will not be applied to the pool even though it appears to have been applied successfully.

- The Help Desk Plugin option is installed by default. If you choose not to install this option, performance-related metrics from user sessions in the desktop instances or farm server instances based on this image are not collected. As a result, some data will not be available in the user card for such sessions. For details, see About the User Card Feature in Your Horizon Cloud Environment.

- The vRealize Operations Desktop Agent option is installed by default. If you choose not to install this option, activity-related data from user sessions in the desktop instance or farm server instances based on this image is not reported to Horizon Cloud. As a result, data from end-user activity and other types of desktop activity will not be displayed in reports in the Horizon Cloud administrative console.
The Dynamic Environment Manager option is not enabled by default. Selecting that option installs the VMware Dynamic Environment Manager client component, known as the FlexEngine. Selecting that option installs FlexEngine using its typical mode. The typical mode requires a post-installation configuration step to configure the VMware Dynamic Environment Manager Group Policy. For VMware Dynamic Environment Manager usage information, see the Dynamic Environment Manager product documentation. VMware Dynamic Environment Manager provides various options for achieving the persistence of end-user data, settings, and profiles of desktops provisioned by your pod.

**Note** When the Dynamic Environment Manager option is selected for installation, its resulting installation path is C:\Program Files\VMware\Horizon Agents\User Environment Manager.

Prerequisites

Verify that the virtual machine (VM) is created and configured as described in Create the Virtual Machine Manually in Your Pod in Microsoft Azure and Prepare the Manually Created VM Prior to Installing the Agents.

Verify that the pod in which this VM is created has a manifest version lower than 1600 and that you know what that version is. The following steps do not apply when the pod has a manifest version of 1600 or higher. You can check your pod's manifest version on the pod's details page from the Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types.

**Caution** When your pod is of manifest 1600 and lower, you must install the agent-related software using a version of Horizon Agents Installer that corresponds to your pod level. Otherwise the version-specific steps to subsequently pair the VM with the cloud will not work for you. As an example, when your pod has a manifest version between 1493 and 1600, install Horizon Agents Installer 19.2 into the base VM. When the manifest version is between 1273 and 1493, install Horizon Agents Installer 19.1 into the base VM.

Procedure

1. Download the Horizon Agent Installer software that aligns with your pod's manifest version to the VM from www.vmware.com by logging in using your My VMware account and navigating to the product's software downloads page.

   One method to download the installer is to point the VM's Internet Explorer browser to the My VMware location in vmware.com. Log in using your My VMware account. Navigate to the VMware Horizon Cloud Service on Microsoft Azure downloads page by clicking View & Download Products, navigating to the VMware Horizon Cloud Service download components page, and selecting Go to Downloads for the VMware Horizon Cloud Service on Microsoft Azure choice.
2 Navigate to where you downloaded the installer and start it.

**Important** If you want to use the URL redirection option with the desktops or RDS-based remote applications resulting from this base VM, you must use the command line to start the installer, adding the `VDM_URL_FILTERING_ENABLED=1` parameter to the command.

For example,

```bash
VMware-Horizon-Agents-Installer-x.y.z-build-x64.exe VDM_URL_FILTERING_ENABLED=1
```

Where `x.y.z` and `build` match the numbers in the file name.

After a few minutes, the installation wizard displays its Welcome screen.

- For a VDI desktop image, the Horizon Cloud Endpoint Desktop image is displayed.

- For a server image, the Horizon Cloud RDSH App image is displayed.
3 Click **Configure**.

The wizard's next step displays. The following screenshot is an example of this step when running on a server image.
4 Scroll down to see the feature options.

The following screenshot is an example of this step when running on a server image.
5 Select the check boxes for the features you want to install and click the arrow to move to the next step.

If the VM is a GPU-backed Windows Server operating system VM, select the 3DRDSH option.

**Note** If you do not install the Help Desk Plugin option, performance-related metrics from user sessions in the desktop instances or farm server instances based on this image are not collected. As a result, some data will not be available in the user card for such sessions. For details, see About the User Card Feature in Your Horizon Cloud Environment.

6 If prompted with a message about using USB redirection securely, click **OK**.

The final wizard step displays.

7 Click **Proceed with installation**.

The installer begins installing the components.

**Note** If a message displays asking for confirmation to install the VMware display adapters, click **Install**.

When all the components are installed, the wizard displays **Finish**. The following screenshot is an illustration of the list of installed components when running the installer on a server image and only selecting default options. The specific entries might vary depending on the operating system and options you select.

![VMware Horizon® Agents Installer v19.2.0](image)

**Installation list**

- Microsoft Visual C++ 2017 Redistributable - x86
- Microsoft Visual C++ 2017 Redistributable - x64
- VMware Horizon Cloud Components
- VMware Horizon Agent Components

8 When the wizard signals it is finished, click **Finish**.
9 Click **Restart Now** to reboot the VM and have the configuration changes take effect.

**What to do next**

Pair the configured VM with the cloud plane by following the steps in Manually Pair the Configured Virtual Machine with Horizon Cloud For Pods with Manifests Lower Than 1600

**Manually Pair the Configured Virtual Machine with Horizon Cloud For Pods with Manifests Lower Than 1600**

When manually creating a base VM in a pod with manifest lower than 1600, after running the Horizon Agents Installer, you must configure some DaaS agent properties in the VM to explicitly pair the VM with the pod before Horizon Cloud can convert the VM into an assignable image that can be used in Horizon Cloud.

**Prerequisites**

- From the pod's details page in the Horizon Cloud administrative console, obtain the IP address that is needed for this pairing process when the VM resides in a pod with manifest lower than 1600.

  **Note** Prior to the July 2020 quarterly service release, this IP address had the label **Tenant appliance IP address** on the pod's details page. The current label is **Pod Manager LoadBalancer IP**. Pods of recent manifests include a Microsoft Azure load balancer deployed for the pod manager instance by default, and the current label reflects that pod architecture. Even though pods of manifests lower than 1600 do not have a Microsoft Azure load balancer deployed for their pod manager VM, the IP address you need to use for this pairing task is the IP displayed next to that label in the pod's details page.

To obtain the IP address appropriate to use for this pairing process for pods of manifests lower than 1600, navigate to **Settings > Capacity** and click on the pod's name. On the Summary page, locate the **Pod Manager Load Balancer IP** property and note down that IP address.
Verify that the agent-related components were installed in the base VM as described in For Pods at Manifests Lower Than 1600, Install the Agent-Related Software Components in the Base Virtual Machine.

**Important** When your pod is of manifest 1600 and lower, you must use a version of Horizon Agents Installer that aligns with your pod level. Otherwise these steps to pair the VM with the cloud will not work and the VM will fail to pair with the cloud. As an example, when your pod has a manifest version between 1493 and 1600, install Horizon Agents Installer 19.2 into the base VM. When the manifest version is between 1273 and 1493, install Horizon Agents Installer 19.1 into the base VM.

In the base VM’s Windows operating system, confirm that you can access the Keytool.exe file in `C:\Program Files (x86)\VMware\Horizon Agents\Horizon DaaS Agent\service`. Open a command prompt as administrator, navigate to `C:\Program Files (x86)\VMware\Horizon Agents \Horizon DaaS Agent\service`, and issue the command `Keytool.exe -h`. If the command returns information about running Keytool to import the bootstrap credentials, you have the required access.

**Procedure**

1. In the Microsoft Azure portal, connect to the base VM and log in to the VM’s Windows operating system if you are not already connected.
2  Download the DaaS SSL bootstrap file from Horizon Cloud.
   This file is used in the bootstrap process that allows the VM's operating system and the pod to pair with each other securely.
   a  Point the VM's browser to https://cloud.horizon.vmware.com and log in with your credentials.
   b  Click **Inventory > Images**.
   c  On the Images page, select ... > **Download Bootstrap**.
   d  In the download window, select the appropriate location, the corresponding pod, and enter and re-enter a password of 8-20 ASCII characters containing at least one each of the following: lowercase letter, uppercase letter, number, and symbol (!@#$%^&*).
      Do not use non-ASCII characters in the password. Make a note of this password for future use.
   e  Click **OK** to save the bootstrap file to a location in the VM.
      The downloaded file is named image_bootstrap.7z by default. This file is used as input to the keytool.exe utility.

3  Verify the setting of the DaaS agent's EnableBootstrap registry key is set to 1 (one), and not 0 (zero).
   a  Run regedit.
   b  In the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware DaaS Agent entry.
   c  Verify the value of the EnableBootstrap key is set to 1 (one).
      If EnableBootstrap key is not set to 1 (one), then modify the key to set it to 1 (one).

4  Create a registry key for the desktop manager address.
   a  In the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware DaaS Agent entry.
   b  Add a new string value key named DesktopMgrAddresses.
   c  Set the new key's value to that IP value that you obtained from the pod's details page, as described in this documentation topic's Prerequisites section.
5  Restart the DaaS agent service.

   The DaaS agent waits for the bootstrap credentials to be imported in the next step.

6  Import the DaaS SSL bootstrap credentials.

   a  Open a command prompt as administrator and navigate to C:\Program Files (x86)\VMware\Horizon Agents\Horizon DaaS Agent\service.

   b  Run Keytool.exe using the downloaded DaaS SSL bootstrap file (image_bootstrap.7z) as an argument.

      Keytool.exe -f absolute-path-to-bootstrap-file/image_bootstrap.7z

   When prompted, enter the encryption password that you set when you downloaded the DaaS SSL bootstrap file.

      Note  Ensure that step 2 to add the registry key is completed before you run the Keytool utility. If the registry key does not exist, the Keytool command might fail with the message Cannot find the file specified.

      The Keytool utility performs the bootstrap and moves the certificate to the cert folder. If you see a message that the file is successfully decrypted, this step is complete.

7  Close your RDP connection.

8  In the Microsoft Azure portal, click Stop on the VM.

9  When the portal indicates the VM is completely stopped, click Start on the VM.

What to do next

At this point, the base VM conforms to the Horizon Cloud environment's requirements to create an assignable image, also referred to as a sealed image. To confirm that this VM can be converted into a sealed image, in the Horizon Cloud administrative console, navigate to Inventory > Imported VMs and check that an ACTIVE status is displayed in the Agent Version column for this VM.

If you joined the VM to your Active Directory domain, you can use domain accounts to connect to the VM to customize the image. If you did not join the VM to your Active Directory domain, you can use the local administrator account to connect to the VM to customize the image.

Customize the image’s Windows operating system, including configuring things like wallpapers and installing the applications you want this VM to provide to your end users. If you enabled a public IP address for the VM, you can connect to the created VM by using the IP address displayed on the Imported VMs page in an RDP client like Microsoft Remote Desktop Connection. For details, see Customize the Imported VM’s Windows Operating System and its subtopics:

   ■  For server operating systems: For a Horizon Cloud Imported VM with a Microsoft Windows Server Operating System — Customize the VM for Your Organization’s Needs
For Windows 10 operating systems: For a Horizon Cloud Imported VM with a Microsoft Windows Client Operating System — Customize the VM for Your Organization’s Needs

**Important** It is strongly recommended that you optimize the image VM, including removing AppX packages from Window 10 images, as described in Customize the Imported VM’s Windows Operating System, Deciding to Optimize the Windows Image When Using the Import Virtual Machine from Marketplace Wizard, and Using the Remove Windows Store Apps Option When Using the Import Desktop Wizard.

**Tip** To further tune the image VM to provide an improved configuration for using VMware Blast Extreme, a best practice is to follow the guidance in Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance from Horizon Cloud Farms and Desktops. Another best practice is to read the VMware Blast Extreme Optimization Guide and perform additional tuning for codec options in the image according to that guide’s recommendations for codec options.

If you selected a NV-series VM type, you must log into the VM’s operating system and install the supported NVIDIA graphics drivers to get the GPU capabilities of the GPU-enabled NV-series VM. You install the drivers after the VM is created and the Imported VMs page shows the agent state is active for the VM. See Install NVIDIA Graphics Drivers in a GPU-Enabled VM Imported in Horizon Cloud.

If you selected to install the Dynamic Environment Manager option when installing the agent, configure a separate file server in your Microsoft Azure subscription that has at least SMB 2 enabled. Then configure VMware Dynamic Environment Manager using that file server. Also configure the GPO settings. See the VMware Dynamic Environment Manager documentation topics in the Dynamic Environment Manager product documentation.

For improved security regarding the use of the Horizon Agent, configure your Active Directory server domain policy GPO (Group Policy Object) to disable weak ciphers in SSL and TLS protocols. For information about disabling weak ciphers when communicating using the SSL/TLS protocol, see the appropriate agent-related information in the VMware Horizon® documentation set, such as Disable Weak Ciphers in SSL/TLS.

After you are finished customizing the image, use the New Image workflow to convert the image to an assignable image. See Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

**Tech Preview - How To Configure a Microsoft Windows 10 Multi-Session Image for Use with App Volumes Features in Horizon Cloud Pods in Microsoft Azure**

Use of App Volumes with Microsoft Windows 10 Enterprise multi-session operating system is currently in tech preview. During the tech preview, when you are creating an image in your pods in Microsoft Azure that uses Microsoft Windows 10 Enterprise multi-session and you plan to use App Volumes with that image, you must follow a slightly different sequence of steps to get to a published image than the standard creation steps. This topic describes those steps at a high-
level, points out what you must do differently from the standard steps for this use case, and provides links to the topics with the standard steps.

Creating an assignable image is a multi-step process: a base virtual machine (VM) must be created and paired with the cloud plane, then customized according to your organization's needs, and then converted into an assignable desktop image. The standard process is described in Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure.

The topic App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites has a section with the high-level sequence for adding an App Volumes application using a Microsoft Windows 10 Enterprise multi-session VM. This topic here is the first step in that high-level sequence.

**Important**

- For this tech preview feature, you can create the base VM using either the automated Import VM wizard or manually. Using the automated wizard ensures the VM is connected to the appropriate subnet in the pod. However, for a Microsoft Windows 10 Enterprise multi-session VM, even though the wizard will install the Horizon agent software into the VM, the wizard is not able to install the App Volumes Agent at this time. As a result, when you want to use the automated wizard, you must perform the sequence of steps described below.

- Whichever method you use, ensure that the base VM is joined to an Active Directory domain registered with Horizon Cloud. App Volumes requires a domain-joined base VM.

**Prerequisite for Both Methods: Obtain the IP Address Needed for the App Volumes Agent to Communicate with the App Volumes Manager in the Pod**

For both of the methods below, running the Horizon Agents Installer in the VM and selecting the App Volumes Agent option will require you to provide the IP address to use for the agent to communicate with the App Volumes Manager running in the pod. The IP address to use is the one next to the label **Pod Manager Load Balancer IP** in the pod detail's page.

In the console, navigate to Settings > Capacity and click on the pod's name. On the Summary page, locate the **Pod Manager Load Balancer IP** property and note down that IP address.
Method One: Steps From Create the Base VM Using the Import VM From Azure Marketplace Wizard to the Published Image State

First read through Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it with Horizon Cloud to understand the flow. The wizard’s process will install the agent software, except for the App Volumes Agent. Because this tech preview use case needs the App Volumes Agent installed, when you use the wizard to create the VM, you will have to log in to the VM, uninstall the agent software, download the Horizon Agents Installer, and re-install the agent software with all of the options you want, including with the App Volumes Agent option.

Follow this sequence.

1. For using App Volumes with a Microsoft Windows Enterprise 10 multi-session system, when you run the wizard, in addition to the items that the wizard and the standard documented steps indicate are required, for this tech preview use case, ensure the following criteria are met.
   - For **OS**, select one of the Microsoft Windows 10 Enterprise multi-session types
   - Select **Domain Join**. This is an App Volumes requirement.
After the VM is created, you will need to connect and log in to the VM. In the wizard, you can select **Enable Public IP Address** to give the VM a public IP address. If not enabled, then you will later need to RDP into the resulting VM as described in For a Horizon Cloud Imported VM with a Microsoft Windows 10 Enterprise Multi-Session Operating System — Customize the VM for Your Organization’s Needs.

In the wizard’s Advanced Options section, because you will be subsequently uninstalling the agent software after the VM is created, those toggle settings do not matter. You can leave all the toggles as the defaults, or you can also disable all of the toggles in the Advanced Options.

2 Run the Import VM wizard from the Imported VMs page by clicking **Import**, ensure the above criteria, and click **Import** in the wizard to start the creation tasks.

3 After the VM is created and you see it says Import Successful on the Imported VMs page, use your RDP software to connect to the VM and log in to it using the admin user name and password that you specified in the wizard.

4 Uninstall the Horizon Agent Installer software from the VM. Follow the on-screen prompts. Restart the VM when prompted.

5 Log back in to the VM.

6 Download the Horizon Agents Installer software package from my.vmware.com's Downloads area for Horizon Service. Log in to my.vmware.com, navigate to **Download VMware Horizon Service**, look for the VMware Horizon Cloud Service on Microsoft Azure row and click its **Go To Downloads**. Download the Horizon Agents Installer 20.2 file to the VM. That is the latest version to use.

7 Start running the Horizon Agents Installer on the VM. Because the multi-session operating system is an RDSH type of system, the start screen label says RDSH.
Click **Configure** to proceed.

8 In the options, ensure you select **App Volumes Agent**. At this point, you can follow the same steps that are described in For Pods at Manifest 1600 and Higher, Install the Agent-Related Software Components in the Base Virtual Machine and Pair it with Horizon Cloud. Select the other agent options you want.

9 After selecting the agent options and proceeding to the next step, the Specify the App Volumes Manager IP step is displayed. In this step, provide the IP address that is the pod manager’s Azure load balancer IP address. This address is displayed in the pod's details page, next to the label **Pod Manager Load Balancer IP**. The steps to locate that address are described in the preceding section.

10 After completion of the agent installation and you've restarted the VM, when the VM is powered back on, use the **Reset Agent Pairing** action in Horizon Cloud to pair it with your Horizon Cloud environment.

11 Customize the VM as described in For a Horizon Cloud Imported VM with a Microsoft Windows 10 Enterprise Multi-Session Operating System — Customize the VM for Your Organization's Needs and Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance from Horizon Cloud Farms and Desktops.

12 Publish the image as described in Convert a Configured Image VM to an Assignable Image in Horizon Cloud.
Return to App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites and follow the next step in the section about adding App Volumes applications to your inventory when using a Windows 10 Enterprise multi-session VM.

Method Two: Steps From Create the Base VM Manually to the Published Image State

Perform the steps described in the following topics, ensuring the following items:

- Before installing the agent software, you join the VM to the pod’s Active Directory domain. This is an App Volumes requirement.
- When installing the agent software, ensure you select App Volumes Agent

Follow the steps in the linked topics according to this sequence:

1. Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud
2. Create the Virtual Machine Manually in Your Pod in Microsoft Azure
3. Prepare the Microsoft Windows 10 Enterprise Multi-Session VM for Agent Installation Needed by Horizon Cloud
4. For Pods at Manifest 1600 and Higher, Install the Agent-Related Software Components in the Base Virtual Machine and Pair it with Horizon Cloud

**Note** After selecting the agent options and proceeding to the next step, the Specify the App Volumes Manager IP step is displayed. In this step, provide the IP address that is the pod manager's Azure load balancer IP address. This address is displayed in the pod's details page, next to the label Pod Manager Load Balancer IP. The steps to locate that address are described in the preceding Prerequisite section.

5. After completion of the agent installation and you've restarted the VM, when the VM is powered back on, use the Reset Agent Pairing action in Horizon Cloud to pair it with your Horizon Cloud environment.

6. After paring the VM App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites and follow the next step in the section about adding an App Volumes application using a Windows 10 Enterprise multi-session VM.

7. Customize the VM as described in For a Horizon Cloud Imported VM with a Microsoft Windows 10 Enterprise Multi-Session Operating System — Customize the VM for Your Organization's Needs.

8. Publish the image as described in Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

9. Return to App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites and follow the next step in the section about adding App Volumes applications to your inventory when using a Windows 10 Enterprise multi-session VM.
Using Microsoft Azure Disk Encryption with Your Farms and VDI Desktops in Your Horizon Cloud Environment

When you create an RDSH farm or a VDI desktop assignment in your Horizon Cloud pod in Microsoft Azure, you can decide to whether to enable disk encryption. When you enable disk encryption for a farm or VDI desktop assignment, all disks for all of the virtual machines (VMs) in that farm or VDI desktop assignment are encrypted. You specify disk encryption when you create the farm or VDI desktop assignment, and you cannot change the encryption state after the farm or assignment is created.

The workflows to create a farm and a VDI desktop assignment include a toggle for enabling disk encryption. For details of those workflows, see:

- Create a Farm
- Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure
- Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure

Note

- This release does not support having disk encryption for floating VDI assignments that use image VMs with attached data disks.

Performance Impact of Disk Encryption

The disk encryption feature is provided by the Microsoft Azure cloud’s Azure Disk Encryption (ADE) capability. ADE uses the BitLocker feature of Microsoft Windows to provide encryption for the OS and data disks of the VMs in Microsoft Azure. In general, BitLocker imposes a single-digit performance overhead, so the encrypted VMs might have a noticeable performance impact. The downsides of VM encryption are that it might increase data, network, or compute resource usage, which can result in additional license or subscription costs. Instead of simply reading data from the disk and writing data to an unencrypted disk, the VM must unencrypt the data to read it, then encrypt the data to write it back to the encrypted disk. In this process, keys are read from the key vault in Azure, which increases the network usage, and CPU cycles are spent on performing the encryption. See Azure Disk Encryption FAQ and BitLocker Deployment and Administration FAQ in the Microsoft documentation.

The Encryption Key Vault

The key vault used for the pod’s encrypted farms and VDI desktop assignments is created in the same Microsoft Azure resource group that contains the pod’s manager VM. A single key vault is used for all of the pod’s encrypted farms and desktop assignments. The system creates this encryption key vault when the first encrypted VM is created as a result of creating the associated farm or VDI desktop assignment. Until that first encrypted VM is created, you will not see this key vault in your pod’s resource groups.
The system generates the key vault's name using the pod's ID, which is an identifier in UUID form. To adhere to Microsoft Azure naming rules, the system sets the key vault name by:

1. Taking the pod's ID.
2. Appending the letters `kv` to the beginning.
3. Removing any non-alphanumeric characters.
4. Truncating characters as needed to keep to a maximum length of 24.

The following screenshot illustrates the items in the pod's manager VM's resource group when that pod has an encrypted farm. The screenshot shows two key vaults: one is the key vault for the pod itself, created during pod deployment, and one is the key vault created when the first encrypted VM is created as a result of creating a disk-encryption-enabled farm or VDI desktop assignment. In the screenshot, you can see that:

- The pod's ID is `e1c80e74-7f6f-434f-bd79-c1e3772f6c5a`, in the pod's manager VM's name.
- The encryption key vault's name is `kve1c80e747f6f434fbd79c1`, determined by taking that UUID, adding `kv` to the beginning, removing the hyphens, and truncating the name to 24 characters.

**Caution** Do not delete any key vaults you see in the pod's manager VM's resource group. The encrypted VMs will not power on if the encryption key vault is deleted. The pod's manager VM will not power on if the pod's own key vault is deleted.

### Creating and Deleting Encrypted VMs

An encryption secret is used for each encrypted VM. As a VM instance is created in an encrypted farm or VDI desktop assignment, a secret is created in the key vault. When a VM instance is deleted from an encrypted farm or VDI desktop assignment, the secret is removed from the key vault.
When you use the Horizon Cloud administrative console to delete an encrypted farm or VDI desktop assignment, the system deletes the associated secrets from the key vault. When you delete the pod itself, the key vault for the encrypted VMs is also deleted.

**Note** Creation of an encrypted farm VM or desktop VM takes approximately twice as long as creating a non-encrypted VM. As a result, the end-to-end time to complete creating a farm or VDI desktop assignment that has disk encryption enabled is approximately twice as long as creating that farm or VDI desktop assignment without disk encryption enabled.

Also, when an image VM has a data disk, additional time is needed for creating an encrypted farm VM or desktop VM based on that image VM. Generally speaking, times for disk encryption of VMs with data disks that are running Windows Server operating systems are shorter times than for Windows 10 VMs with data disks. The longest times occur for Windows 10 operating systems with data disks of larger, terabyte sizes.

### When Scheduling Power Management for Farms and VDI Desktop Assignments That Have Large Numbers of Encrypted VMs

The time to power on an encrypted VM and have the VM become ready to accept an end-user connection takes longer than for non-encrypted VMs. When the VM has a small number of cores, like the A1 size, the time can take approximately 12 minutes. With a larger number of cores, the time is shorter, approximately 6 minutes.

When you are using the system's power management scheduling feature to have large numbers of VMs powered on it time to meet a predicted end-user demand, if the VMs are encrypted, you must consider the additional time it will take to have those VMs ready. The system powers on a maximum of 125 VMs concurrently. If your VDI desktop assignment or farm has more than 125 VMs, when a power management schedule says to power on the assignment or farm at 8 AM, the system starts powering on the VMs at 8 AM in batches of 125 at a time. When the VMs are of the smallest A1 size and are encrypted, this combination of 125 VMs per batch and the 12 minutes to be ready for connections gives an approximate time line that looks like:

- By 8:12 AM, 125 VMs are ready
- By 8:24 AM, 250 VMs are ready
- By 8:36 AM, 375 VMs are ready

As a result, if your VDI desktop assignment has 2,000 encrypted VMs of the small A1 size, the time it takes for having 100% of them powered-on and ready for end-user connections will be approximately 3.5 hours. If your goal is to have 100% of those encrypted A1 size desktops ready at 8 AM, you should consider setting the power management schedule to start at 4:30 AM.

For larger-sized VMs, the time to be ready is about half as long. So instead of 3.5 hours, an encrypted VDI desktop assignment of 2,000 encrypted VMs of a larger size like A4 would take 75 minutes to have 100% of them ready to accept end-user connections.
Similarly, an encrypted VDI desktop assignment that has less desktops will be ready faster than the large 2,000 pool size. For a pool of 500 encrypted desktops of the small A1 size, 100% of the pool will be ready in approximately 48 minutes. 500 VMs divided by 125 per batch makes 4 batches, then multiplied by 12 minutes per batch gives 48.

Using Data Disks with Virtual Desktops from a Horizon Cloud Pod in Microsoft Azure

With a data disk, you can provide data, applications, or extra storage for your end users. You can use data disks both with image VMs automatically created by the Import Virtual Machine from Marketplace wizard or image VMs that you have manually created and paired with your Horizon Cloud environment. The system supports using data disks with session-based desktops and remote applications from RDSH farms, floating VDI desktop assignments, and dedicated VDI desktop assignments. However, because of the different nature of the assignment types, the use cases vary for each type.

Data Disks and Dedicated VDI Desktop Assignments

The dedicated VDI desktop assignment is the most common use case for data disks. Initially, each desktop VM in the assignment’s pool of VMs has the same data disk configuration and contents as for the original image VM on which the assignment is based. You might provide data and applications on the initial data disk that you want to give to all of the entitled end users. Each end user in a dedicated VDI desktop assignment is assigned a specific virtual desktop. The assigned end user returns to the same virtual desktop each time they launch the desktop and log in. Because the data disk persists with that virtual desktop, the assigned end user can make changes to the data on the data disk and all of the user’s changes are preserved between sessions.

Data Disks and Floating VDI Desktop Assignments

In a floating VDI desktop assignment, each virtual desktop VM is reverted to the initial state of the original image VM when an end user logs out of the desktop. Like in the dedicated case, initially each desktop VM in the assignment’s pool of VMs has the same data disk configuration and contents as for the original image VM on which the assignment is based. Also as in the dedicated case, you might provide data and applications on the initial data disk that you want to give to all of the entitled end users. Each time an end user connects to a desktop from the pool, that end user is connected to a desktop with any data disks in their initial state.

Unlike the dedicated case, when the end user logs out of the desktop, the virtual desktop’s data disks are reverted to the initial data disk configuration and contents. Any files the end user might have saved to those disks are lost when the user logs out.
Data Disks and RDSH-Based Desktop and Application Assignments

The main use case for using data disks with RDSH VMs is to provide shared, read-only data or applications to all of the end users that you will entitle to use session-based desktops and remote applications provisioned from the RDSH farm. Any data disk that is attached to an RDSH VM is available to all end users that connect to that VM for their session-based desktops and remote applications. Also, because an end user might get connected to different VM instances each time the end user logs in to use their entitled desktop or application, there is no guarantee a particular end user would be able to access data they saved to the data disk during previous sessions. As a result, using data disks for personal data in this scenario is typically avoided.

Getting Started

To have data disks available to the pod-provisioned virtual desktops and remote applications, you use the Microsoft Azure portal to create the disks and attach them to a golden image VM before publishing the image. At a high level, you:

1. Attach the created data disks to the VM.
2. Initialize those data disks according to the steps in the Microsoft Azure documentation topic [Attach a managed data disk to a Windows VM by using the Azure portal](#). Those steps include initializing the disks, defining volumes, and formatting partitions as appropriate for your needs.
3. Add any initial contents you want on the data disks.

You must perform those steps before you convert the golden image to a published image. The system's image publishing process captures that initial state of the data disks as it seals the image. After publishing the image, you cannot add data disks to that sealed image. To update a sealed image for any reason, including adding a data disk, you update the image according to the information in [Managing Published Images for Horizon Cloud Pods in Microsoft Azure](#) and its subtopics.

For the detailed steps of preparing a data disk for an image VM used in Horizon Cloud, see [Setting Up a Data Disk for an Image VM in Horizon Cloud](#).

Number of Data Disks per VM

The current recommendation on the number of data disks supported in Horizon Cloud on an image VM is up to five (5) data disks. Additional factors might restrict the number of data disks you can attach to a VM, such as Microsoft Azure policies about how many data disks can be attached to a particular VM size and the Microsoft Azure region into which your pod is deployed. See the Microsoft Azure documentation topic [Sizes for Windows virtual machines in Azure](#) and the pages for the various VM types for the charts that show the maximum numbers for each Microsoft Azure VM size.
Life Cycle of Data Disks

When you use the Horizon Cloud administrative console to delete a VM, the system looks for all of the resources associated with the VM and deletes those resources. Even though you manually created the data disks in the Microsoft Azure portal, when the data disks are attached to a VM in Horizon Cloud, the system will delete those data disks when it deletes the VM.

When farm RDSH instances and VDI desktop instances are created from images with attached data disks, the data disks for those instances are created and deleted automatically when the RDSH and desktop VMs are created and deleted, according to the system’s standard behavior.

Setting Up a Data Disk for an Image VM in Horizon Cloud

To provide a data disk in your pod-provisioned virtual desktops and remote applications, you create a managed data disk using the Microsoft Azure portal and add that data disk to the image VM. Then you initialize the data disk and format it. After formatting the disk, you can optionally load it with any content you want in the disk’s initial configuration. You must perform those steps before you convert the image to a published image.

In Horizon Cloud, you can use data disks both with image VMs automatically created by the Import Virtual Machine from Marketplace wizard or image VMs that you have manually created and paired with your environment. For information about using data disks in your Horizon Cloud environment, see Using Data Disks with Virtual Desktops from a Horizon Cloud Pod in Microsoft Azure.

This topic describes the best practice workflow in the context of your Horizon Cloud pod, when the VM already exists in a state where it is paired with Horizon Cloud and the VM does not already have a data disk attached to it. The system’s automated Import wizard creates a VM without a data disk. If you manually created a base VM and attached a data disk at creation time, you must log in to the VM and initialize the data disk before publishing the image. To initialize a VM’s data disk, follow the steps described in the Microsoft Azure documentation topic Initialize a new data disk.

The general steps for adding a data disk to a VM and initializing it are available in the Microsoft Azure documentation topic Attach a managed data disk to a Windows VM by using the Azure portal. An overview of the process is:

- In the Microsoft Azure portal, you locate the image VM and add a data disk to it.
- You log in to the VM and initialize that data disk.

Prerequisites

Verify the Imported VMs page indicates the agent-related status is active for the VM. To get that status for a VM created in a pod at manifest 1600 and higher, use the Imported VMs page’s Reset Agent Pairing action on the VM. That action is located in the More drop-down list.
Obtain the VM's name and IP address as displayed on the Imported VMs page. You use the name to locate the VM in the pod's resource groups in the Microsoft Azure portal so you can attach the data disk to the VM. You use the IP address to log in to the VM to initialize the data disk after it is attached.

**Note**  When using the Microsoft Remote Desktop Client as your RDP software to connect to the VM, ensure it is the most up-to-date version. For example, the default RDP software in the Windows 7 operating system is not at a high enough version. The version must be version 8 or higher.

Verify you have at least one of the following credentials (user name and password) to log in to the VM's guest Windows operating system, according to how the VM was created.
<table>
<thead>
<tr>
<th>When the VM was created</th>
<th>How the VM was created</th>
<th>Credentials to use to log in</th>
</tr>
</thead>
</table>
| Prior to the December 2019 service release going live in production | Import Virtual Machine wizard, from the Imported VMs page. | Prior to the December 2019 service release date, the Import Virtual Machine wizard created VMs that were always automatically joined to the Active Directory domain that was specified in the wizard. To log in to such a VM, you can use one of the following:  
  - The credentials for the local administrator account that were specified in the wizard.  
  - The credentials for a domain account in that Active Directory domain. |
| After the December 2019 service release went live in production | Import Virtual Machine wizard, from the Imported VMs page. | Starting with the December 2019 service release date, the Import Virtual Machine wizard provides the option of either having the wizard-created VM joined to a specified Active Directory domain or not having the VM joined to the domain at the end of the creation process.  
  - If the VM was created with the wizard’s Domain Join toggle enabled, you can use either the credentials for a domain account in the specified Active Directory domain or use the local administrator account that was specified in the wizard.  
  - If the VM was created with the wizard’s Domain Join toggle turned off, you must use the local administrator account that was specified in the wizard. In this case, because the VM is not joined to the domain, the local administrator account is the only account that has access to log in. |
| In any service release | Manual preparation steps in Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud. | Typically you do not need to join the VM to your Active Directory domain when you manually build the VM. To log in to that VM, use one of the following:  
  - The credentials for the local administrator account that was specified when the manually built VM was created in the Microsoft Azure portal.  
  - If you manually joined that VM to an Active Directory domain, the credentials for a domain account in that domain. |

**Important** Starting with pod manifest 1230 and later, domain accounts can direct connect to domain-joined image VMs that have the agent software installed. Prior to pod manifest 1230, the agent software installed in a domain-joined VM prevented domain accounts from directly connecting to that VM. However, if you have not yet updated your pod to a manifest of 1230 and later, before a domain account can direct connect to a domain-joined image VM that has the agent software installed, you must first perform the steps in *When Your Pod is Not Yet Updated to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image*.
Procedure

1. In the Microsoft Azure portal, locate the image VM.
   a. Use the portal's search bar to search for the VM's name.
      The following screenshot is an illustration of searching for a VM named la48win-1. The first result is the virtual machine.

![Image of Azure portal search results for la48win-1]

   b. Display the VM's page in the portal by clicking the virtual machine in the search results list.
   c. Make note of the VM's resource group to use it in the Create Managed Disk page.
      Image VMs used in Horizon Cloud are located in a resource group with a name in the pattern `vmw-hcs-podID-base-vms` where `podID` is the pod's identifier. In the Horizon Cloud administrative console, the pod ID is listed in the pod's details page from the Capacity page.

2. Add a new data disk to the VM.
   a. Open the VM's Disks page by clicking Disks under Settings.
   b. Click Add data disk.
      A data disk row displays.
   c. Use the drop-down to click Create disk.
      The disk creation page opens.
In the disk creation page, specify the required values.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Type a name for the data disk.</td>
</tr>
<tr>
<td><strong>Resource Group</strong></td>
<td>Select a resource group in which to locate the data disk. Typically you would select the same resource group in which the VM is located (vmw-hcs-podID-base-vms).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can locate the data disk in a resource group other than the pod's resource groups.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Displays the Microsoft Azure region in which the VM is located.</td>
</tr>
<tr>
<td><strong>Account type</strong></td>
<td>Select the type you want.</td>
</tr>
<tr>
<td><strong>Source type</strong></td>
<td>Select <strong>None (empty disk)</strong>.</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>Specify the size of the disk.</td>
</tr>
</tbody>
</table>

The following screenshot is an example of the fields filled out.

![Dashboard > la48win-1 - Disks > Create managed disk](image)
e  Click **Create**.

After a little time during which the system creates the disk, the portal re-displays the VM's Disks page with the new data disk listed.

**Note**  The new data disk is added with **Host Caching** set to **None** by default. You can choose a setting that is appropriate for your intended use of the data disk.

The following screenshot illustrates the VM's Disks page and its listed data disk.

f  At the top of the VM's Disks page, click **Save** to complete attaching the new data disk to the VM.

At this point, the data disk is attached but uninitialized.
3 Log in to the VM.
   a Use the VM’s IP address in your RDP software to connect to the Windows operating system.
      ■ If the VM was created with a public IP address, you can use that IP address in your RDP software
      ■ If the VM has a private IP address, you must RDP into it by one of these two methods:
         ■ Using another VM in your Microsoft Azure subscription that does have a public IP address and doing an outbound RDP into the image VM.
         ■ Use your VPN and RDP into the image VM over your corporate network

   Note  To access a VM that is running the agent-related software components, the version of the Remote Desktop Client must be version 8 or later. Otherwise, the connection fails. Using the most up-to-date Remote Desktop Client is recommended.

   b Log in to the Windows operating system using credentials (user name and password) as described in the prerequisites here.

   When using the local administrator account credentials that were specified in the Import Image wizard when the VM was created, enter the username as \username.

   Note  When the VM is a domain-joined VM, as described in the prerequisites here, and you want to use a domain account instead of the local administrator account, enter the user name as domain\username where domain is the name of the domain.

4 In the VM, perform the steps to initialize and format the data disk, as described in the Microsoft Azure documentation topic Initialize a new data disk.

Results

At this point, the image VM has a formatted, empty data disk. If you want to load the data disk with any content you want to provide to your end users in the disk's initial configuration, you can add the content at any time until you publish the image.

VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure

When the Microsoft Azure VNet that is used by your pods is configured for NSX Cloud, you are able to leverage the features of NSX-T Data Center network virtualization with those pods’ farms and VDI desktop assignments. You can use the micro-segmentation features of NSX Cloud to restrict access between farm RDSH instances and VDI desktops even when those virtual machines are in the same tenant subnet.
For the specific version of NSX-T Data Center that is supported for this integration, see the documentation topic Horizon Cloud — Environments, Operating Systems, and Compatibility.

**Note** When you have updated an existing pod from manifest versions prior to 1101 to a later manifest version, those farms and VDI desktop assignments that existed in the pod prior to updating the pod cannot be edited after the update to enable them for NSX Cloud management.

NSX Cloud integrates the NSX-T Data Center core components, NSX Manager and NSX Controllers, with your Microsoft Azure cloud environment. For an overview of the NSX Cloud architecture and components, see NSX Cloud Architecture and Components in the VMware NSX-T Data Center documentation. The core NSX Cloud components are:

- NSX Manager
- NSX Controller
- Cloud Service Manager (CSM)
- NSX Public Cloud Gateway (PCG)
- NSX Agent

**Note** This integration of NSX Cloud and Horizon Cloud pods in Microsoft Azure supports non-quarantine mode only.

One requirement of using NSX Cloud with your Microsoft Azure environment is you must establish a connection between your Microsoft Azure VNet and your on-premises NSX-T Data Center appliances. Because Microsoft Azure does not allow you to modify a VNet's CIDR block after a VNet is peered or after attaching a VPN Gateway, ensure you have checked all of the values you want to use before you attach the VNet to the VPN Gateway. For a workflow of the high-level steps for connecting NSX Cloud to your public cloud, see Day-0 Workflow for Connecting NSX Cloud with Your Public Cloud.

The following table is a high-level summary of the end-to-end steps to enable using the NSX Cloud features with your pod’s RDSH VMs and VDI desktop VMs. Some of the links in the Details column open the relevant NSX-T Data Center version 2.4 documentation topics. If you are using NSX-T Data Center 2.3 instead, when you take one of the links below to the 2.4 version topic, you can use the upper blue menu to switch to the 2.3 version of the same documentation topic. The following screenshot illustrates the position of that blue menu for the Deploy or Link NSX Public Cloud Gateways topic.
<table>
<thead>
<tr>
<th>High-Level Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install CSM in your on-premises NSX-T environment and connect it with NSX</td>
<td>Refer to the NSX-T Data Center documentation topic here.</td>
</tr>
<tr>
<td>Manager.</td>
<td></td>
</tr>
<tr>
<td>Enable the ports and protocols that are required for hybrid connectivity.</td>
<td>Refer to the NSX-T Data Center documentation topic here.</td>
</tr>
<tr>
<td>Peer your Microsoft Azure VNet with your on-premises NSX-T Data Center</td>
<td>Refer to the NSX-T Data Center documentation topic here.</td>
</tr>
<tr>
<td>environment.</td>
<td></td>
</tr>
<tr>
<td>Enable CSM to access your Microsoft Azure inventory.</td>
<td>Refer to the NSX-T Data Center documentation topic here.</td>
</tr>
<tr>
<td>Deploy the NSX Cloud PCG on the configured Microsoft Azure VNet.</td>
<td>Refer to the NSX-T Data Center documentation topics:</td>
</tr>
<tr>
<td></td>
<td>• Deploy PCG prerequisites</td>
</tr>
<tr>
<td></td>
<td>• Deploy PCG in a Microsoft Azure VNet</td>
</tr>
<tr>
<td>Create a VM and import it into Horizon Cloud using the Import Virtual Machine</td>
<td>See Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it</td>
</tr>
<tr>
<td>from Marketplace wizard.</td>
<td>with Horizon Cloud.</td>
</tr>
<tr>
<td></td>
<td>To make it easy to install the required NSX agent, a best practice is to select the option for</td>
</tr>
<tr>
<td></td>
<td>a public IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When importing the VM, select the options for optimizing the VM and, for Windows 10,</td>
</tr>
<tr>
<td></td>
<td>removing Windows Store Apps. Using those options helps prevent sysprep issues when subsequently</td>
</tr>
<tr>
<td></td>
<td>sealing the image.</td>
</tr>
<tr>
<td>Connect to the imported VM and install the required NSX agent.</td>
<td>Install the NSX Agent in the Horizon Cloud Imported Image VM</td>
</tr>
<tr>
<td>Publish the image.</td>
<td>Convert a Configured Image VM to an Assignable Image in Horizon Cloud</td>
</tr>
<tr>
<td>Create farms and VDI desktop assignments using that image and the setting to</td>
<td>• Create a Farm</td>
</tr>
<tr>
<td>enable NSX Cloud management for that farm or assignment.</td>
<td>• Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure</td>
</tr>
<tr>
<td>When the RDSH VMs and VDI desktop VMs are created, they appear in your NSX</td>
<td>• Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure</td>
</tr>
<tr>
<td>Cloud inventory.</td>
<td></td>
</tr>
<tr>
<td>Enable the distributed firewall rules in NSX Manager that will allow</td>
<td>Because NSX Cloud will block these communications by default, you must enable some distributed</td>
</tr>
<tr>
<td>communication with the RDSH VMs and VDI desktop VMs</td>
<td>firewall rules in NSX Manager to allow communication with the NSX-managed VMs that are provisioned</td>
</tr>
<tr>
<td></td>
<td>from the pod. See Firewall Rules Required in NSX Manager for Pod-Provisioned VMs.</td>
</tr>
<tr>
<td></td>
<td>If you are using NSX-T Data Center 2.4, in addition to enabling the firewall rules, you must</td>
</tr>
<tr>
<td></td>
<td>also add a forwarding policy to route the traffic pertaining to the NSX-managed VMs over the</td>
</tr>
<tr>
<td></td>
<td>Microsoft Azure cloud's network (underlay). See Add the Required Forwarding Policy in NSX</td>
</tr>
<tr>
<td></td>
<td>Manager for the Pod-Provisioned VMs.</td>
</tr>
<tr>
<td>Use NSX Cloud features with the RDSH VMs and VDI desktop VMs in your NSX</td>
<td>See this NSX Cloud topic and its subtopics in the NSX-T Data Center Administration Guide.</td>
</tr>
<tr>
<td>Cloud inventory.</td>
<td></td>
</tr>
</tbody>
</table>
Horizon Cloud Workflows and NSX Cloud

When you create an RDSH farm or a VDI desktop assignment in your Horizon Cloud pod using a golden image VM that you configured with the NSX agent, you can decide to whether to enable NSX Cloud management on that farm or VDI desktop assignment. When you enable NSX Cloud management for a farm or VDI desktop assignment, all of the virtual machines (VMs) in that farm or VDI desktop assignment are tagged for use in NSX Cloud. You specify NSX Cloud management when you create the farm or VDI desktop assignment, and you cannot change that state after the farm or assignment is created. The Horizon Cloud workflows to create a farm and a VDI desktop assignment include a toggle for enabling use of NSX Cloud with the farm’s RDSH instances or the VDI desktop assignment’s virtual desktops. For details of those workflows, see:

- Create a Farm
- Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure
- Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure

Setting the **NSX Cloud Managed** toggle to **Yes** when creating a farm or VDI desktop assignment gives the resulting farm’s RDSH VMs or VDI desktop VMs with a custom tag named `nsx.network=default`. The NSX Cloud PCG manages all VMs that have that tag. NSX Cloud automatically discovers the VMs in your configured Microsoft Azure VNet that have this tag and includes these VMs in your public cloud inventory. You can then manage and secure those VMs using the CSM component of NSX-T Data Center. For details, see this NSX Cloud topic and its subtopics in the NSX-T Data Center Administration Guide.

Some limitations apply when using the NSX Cloud management feature with your pods in Horizon Cloud:

- You cannot edit the name of a farm or VDI desktop assignment that has NSX Cloud management enabled.
- To use both disk encryption and the NSX Cloud management features for a floating VDI desktop assignment, you must install the latest version of the NSX agent. That combination is not supported with previous NSX agent versions.

Install the NSX Agent in the Horizon Cloud Imported Image VM

When you want to create a farm or VDI desktop assignment that is enabled for NSX Cloud management, the NSX agent must be installed in published image you use for that farm or assignment. You must install the NSX agent into the image VM before you publish it. You install the NSX agent after the VM is created and the Imported VMs page shows the status of the VM’s agent-related software is active.

Installing the NSX agent involves downloading a PowerShell install script file from the download location identified in your NSX Cloud environment’s Cloud Service Manager (CSM). In the image VM, you run that install script to download the NSX agent install binaries and install the agent. Many of the details about installing the NSX agent on Windows VMs are located in the NSX-T Data Center documentation. For further information, see the **Install NSX Agent** topic and its subtopics in the NSX-T Data Center Administration Guide.
Prerequisites

Verify the Imported VMs page indicates the agent-related status is active for the VM. To get that status for a VM created in a pod at manifest 1600 and higher, use the Imported VMs page's Reset Agent Pairing action on the VM. That action is located in the More drop-down list.

**Note** When using the Microsoft Remote Desktop Client as your RDP software to connect to the VM, ensure it is the most up-to-date version. For example, the default RDP software in the Windows 7 operating system is not at a high enough version. The version must be version 8 or higher.

Verify you have at least one of the following credentials (user name and password) to log in to the VM's guest Windows operating system, according to how the VM was created.
<table>
<thead>
<tr>
<th>When the VM was created</th>
<th>How the VM was created</th>
<th>Credentials to use to log in</th>
</tr>
</thead>
</table>
| Prior to the December 2019 service release going live in production | Import Virtual Machine wizard, from the Imported VMs page. | Prior to the December 2019 service release date, the Import Virtual Machine wizard created VMs that were always automatically joined to the Active Directory domain that was specified in the wizard. To log in to such a VM, you can use one of the following:  
  - The credentials for the local administrator account that were specified in the wizard.  
  - The credentials for a domain account in that Active Directory domain. |
| After the December 2019 service release went live in production | Import Virtual Machine wizard, from the Imported VMs page. | Starting with the December 2019 service release date, the Import Virtual Machine wizard provides the option of either having the wizard-created VM joined to a specified Active Directory domain or not having the VM joined to the domain at the end of the creation process.  
  - If the VM was created with the wizard's Domain Join toggle enabled, you can use either the credentials for a domain account in the specified Active Directory domain or use the local administrator account that was specified in the wizard.  
  - If the VM was created with the wizard's Domain Join toggle turned off, you must use the local administrator account that was specified in the wizard. In this case, because the VM is not joined to the domain, the local administrator account is the only account that has access to log in. |
| In any service release | Manual preparation steps in Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud. | Typically you do not need to join the VM to your Active Directory domain when you manually build the VM. To log in to that VM, use one of the following:  
  - The credentials for the local administrator account that was specified when the manually built VM was created in the Microsoft Azure portal.  
  - If you manually joined that VM to an Active Directory domain, the credentials for a domain account in that domain. |

**Important** Starting with pod manifest 1230 and later, domain accounts can direct connect to domain-joined image VMs that have the agent software installed. Prior to pod manifest 1230, the agent software installed in a domain-joined VM prevented domain accounts from directly connecting to that VM. However, if you have not yet updated your pod to a manifest of 1230 and later, before a domain account can direct connect to a domain-joined image VM that has the agent software installed, you must first perform the steps in When Your Pod is Not Yet Updated to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image.
Verify you have the credentials to log in to the portal for your NSX Cloud environment’s CSM. You use the CSM to identify the location for downloading the PowerShell install script to install the NSX agent. CSM is a component of NSX Cloud and provides a single-pane-of-glass management endpoint for your public cloud inventory. For more details, see the Cloud Service Manager topic and related topics in the NSX-T Data Center Administration Guide.

Procedure

1. Use the VM’s IP address in your RDP software to connect to the VM’s Windows operating system.
   - If the VM was created with a public IP address, you can use that IP address in your RDP software.
   - If the VM has a private IP address, you must RDP into it by one of these two methods:
     - Using another VM in your Microsoft Azure subscription that does have a public IP address and doing an outbound RDP into the image VM.
     - Use your VPN and RDP into the image VM over your corporate network.

   **Note** To access a VM that is running the agent-related software components, the version of the Remote Desktop Client must be version 8 or later. Otherwise, the connection fails. Using the most up-to-date Remote Desktop Client is recommended.

2. Log in to the Windows operating system using credentials (user name and password) as described in the prerequisites here.

   When using the local administrator account credentials that were specified in the Import Image wizard when the VM was created, enter the username as \username.

   **Note** When the VM is a domain-joined VM, as described in the prerequisites here, and you want to use a domain account instead of the local administrator account, enter the user name as domain\username where domain is the name of the domain.

3. From the Windows VM, log in to CSM and navigate to Clouds > Azure > VNets.

4. On the Overview tab, expand the Agent Download & Installation area if it is not already expanded.

   In that area, locate the displayed Windows install script download location. Under the download location is also a simple basic installation command.

   - The displayed download location has the pattern http://filepath/nsx_install.ps1, where nsx_install.ps1 is the PowerShell script file and filepath is the path from which to download the file.
The displayed basic installation command includes a portion –dnsSuffix DNS-suffix, where DNS-suffix is a dynamically generated value related to the DNS settings you chose when you deployed the PCG on your Microsoft Azure VNet as part of configuring NSX Cloud.

**Important** When you run the script to install the NSX agent for an image VM in Horizon Cloud, you must specify:

- The same DNS-suffix that you see displayed in CSM for your Microsoft Azure VNet. The DNS-suffix is unique to your configured environment.
- The startOnDemand true option. That option optimizes the NSX agent for the Horizon Cloud publishing workflow.

5 Copy the displayed DNS-suffix so that you have it when you run the install script in the next steps.

6 Use the download location to download the nsx_install.ps1 file to a location on the VM.

7 Open a PowerShell prompt, navigate to where you downloaded the nsx_install.ps1 file, and install the agent by running the installation command using your value for DNS-suffix and the option –startOnDemand true.

**Important** The option -startOnDemand true is required.

The following code block is an example of the command in a PowerShell prompt with an example DNS-suffix of xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.xx.internal.cloudapp.net.

```
powershell -file 'nsx_install.ps1' -operation install -dnsSuffix xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.xx.internal.cloudapp.net -startOnDemand true
```

When the script finishes running, a message appears indicating whether the NSX agent is installed successfully.

8 Close the PowerShell command prompt.

9 Verify that the agent's bootstrap status is ready by opening a regular command prompt and running the following command.

```
schtasks /query /tn nsx_bootstrap
```

Running that command should show the nsx_bootstrap task in Ready status. The following shows an example.

<table>
<thead>
<tr>
<th>TaskName</th>
<th>Next Run Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsx_bootstrap</td>
<td>N/A</td>
<td>Ready</td>
</tr>
</tbody>
</table>

10 Sign out of the VM's Windows operating system.
What to do next

With the NSX agent installed and the `nsx_bootstrap` task showing as Ready, you can publish the image if you have no further customizations to make. See Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

Firewall Rules Required in NSX Manager for Pod-Provisioned VMs

When using NSX Cloud features with your pod in Microsoft Azure, you must enable some distributed firewall rules in NSX Manager to allow communication with the NSX-managed VMs that are provisioned from the pod. If these rules are not enabled, end users will not be able to launch and log in to their desktops or remote applications.

In NSX Manager, enable these rules to allow the traffic as indicated. In the table, the phrase desktop pool refers to the RDSH farm or VDI desktop assignment.

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Source</th>
<th>Destination</th>
<th>Service/Protocol/Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon HTML Access (Blast) traffic</td>
<td>The pod's Unified Access Gateway VMs</td>
<td>Desktop pool</td>
<td>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</td>
</tr>
<tr>
<td>Desktop pool to pod manager traffic</td>
<td>Desktop pool</td>
<td>Pod's manager VM</td>
<td>VMware-View5.x-JMS/TCP/4001 Desktop-Messaging Server/TCP/3099 VMware-View7-JMS/TCP/4002</td>
</tr>
<tr>
<td>Desktop pool to Active Directory domain server traffic</td>
<td>Desktop pool</td>
<td>Pod's manager VM</td>
<td>ANY</td>
</tr>
</tbody>
</table>

Add the Required Forwarding Policy in NSX Manager for the Pod-Provisioned VMs

When you are using NSX-T Data Center 2.4 with a pod in Microsoft Azure, in addition to enabling the firewall rules, you must also add a forwarding policy to route the traffic pertaining to the pod's NSX-managed VMs over the Microsoft Azure cloud's network (underlay). Forwarding policies were introduced in NSX-T Data Center 2.4.

You perform these steps in your NSX-T Data Center 2.4 environment.
Procedure

1. Log in to your environment's NSX Manager.
3. On that Forwarding Policies page, expand the section that represents the VNet on which the NSX Public Cloud Gateway (PCG) is deployed for your pod's use.
4. In the expanded section, make a copy of the last rule listed in that section, the one named CloudDefaultRoute, by right-clicking and selecting Copy rule.
5. Set the action of the new copy to Route to Underlay.
6. Click Publish.

Managing VM Types and Sizes for Farms and Assignments

On the VM Types and Sizes page (Settings > VM Types and Sizes), you can manage the types and sizes of VMs you want to be available for creating farms and assignments.

For pods in Microsoft Azure, you can select the VMs that appear in the Model drop-down menu in the farm and desktop assignment creation wizards. You can also add custom tags, which can be used to filter VMs in the Model drop-down menu. For details about how this list can be filtered, see one of the following topics: Create a Farm, Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure, or Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure. The filter option functions identically in all three cases, so the information describing the option is the same in these three topics.

Important For production environments, ensure the VM models used for your farms and desktop assignments have a minimum of two (2) CPUs. VMware scale testing has shown that using 2 CPUs or more avoids unexpected end-user connection issues. Even though the system does not prevent you from choosing a VM model with a single CPU, you should use such VM models for tests or proof-of-concepts only.

The VM Types and Sizes page (Settings > VM Types and Sizes) displays a list of all VMs available in Azure across all regions, refreshed weekly to include new VMs as they are added. You can use the drop-down menu above the VM list to filter by region.

Note While the filter is being applied, you might see a message indicating that VM Types and Sizes is not supported for the selected region. If the message only appears briefly and then disappears, you can ignore the message.

You can use the Add Tag and Remove Tag buttons to manage custom tags for VMs. See the description of the Tag field in the following table for more information.

There are a few VMs that VMware has removed from the list because they do not work with Horizon Cloud, and might be some that Microsoft has not made available for other reasons. If there is an Azure VM you want to use but do not see listed, contact your VMware representative.
The information displayed for each VM is shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visibility</td>
<td>Indicates whether a VM is displayed in the <strong>Model</strong> drop-down menu in the farm and desktop assignment creation wizards. By default, this option is selected for all VMs.</td>
</tr>
<tr>
<td>VM Name</td>
<td>Name of the VM.</td>
</tr>
<tr>
<td>Tag</td>
<td>There are two types of tags that can be applied to VMs.</td>
</tr>
<tr>
<td></td>
<td>- System tags - These tags are hard-coded and are not editable. Currently the only system-level tag is VMware Recommended, which is applied to VM configurations recommended by VMware. These recommended VM sizes are ones that VMware has determined optimize the price-to-performance ratio for typical Horizon Cloud RDS farm and VDI workloads. However, your business needs might require VM sizes that are not in this VMware recommended list. Even if a VM size is not in this recommended list, ensure that you select a VM size that meets your use case and requirements.</td>
</tr>
<tr>
<td></td>
<td>- Custom tags - These are your own tags, which you create and apply to VMs. You can filter by these tags when selecting a model in the farm and desktop assignment creation wizards.</td>
</tr>
<tr>
<td></td>
<td>To add custom tags to VMs:</td>
</tr>
<tr>
<td></td>
<td>a Select the check boxes for the VMs.</td>
</tr>
<tr>
<td></td>
<td>b Click <strong>Add Tag</strong>.</td>
</tr>
<tr>
<td></td>
<td>c Enter tags, separated by commas, and click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>To remove custom tags from VMs:</td>
</tr>
<tr>
<td></td>
<td>a Select the check boxes for the VMs.</td>
</tr>
<tr>
<td></td>
<td>b Click <strong>Remove Tag</strong>.</td>
</tr>
<tr>
<td></td>
<td>c Select tags to be removed, and click <strong>Save</strong>.</td>
</tr>
<tr>
<td>vCPU</td>
<td>Number of vCPU in the VM.</td>
</tr>
<tr>
<td>RAM</td>
<td>Size of the RAM for the VM.</td>
</tr>
<tr>
<td>Data Disk</td>
<td>Number of data disks in the VM.</td>
</tr>
</tbody>
</table>

**Farms in Horizon Cloud**

A farm is a collection of Microsoft Remote Desktop Services (RDS) hosts that provide multiple users with session-based desktops and applications. Farms simplify the management of the RDS hosts. You can create farms to serve groups of users that vary in size or have different desktop or application requirements.

Before you can assign session-based desktops or remote applications to end users, you must create the farms to serve those desktops and applications. A farm can provide either session-based desktops or remote applications.

Use the Farms page to manage your farms. In your tenant environment, navigate to the Farms page by selecting **Inventory > Farms**.
Create a Farm

You create farms using the Farms page.

A farm is a collection of Remote Desktop Services hosts (RDSHs). Each of those Remote Desktop Services (RDS) hosts is a VM that is instantiated based on the specific RDSH-capable image which you select to use for the farm. The RDSH-capable image is sometimes also called an RDS-enabled image, an RDSH image, or an RDSH-capable image.

By default, Horizon Cloud farms are configured with rolling maintenance. For an example of how rolling maintenance works for a farm, see Example of Farm Rolling Maintenance.

**Note**  Tech Preview feature: When you want to provision desktops running a Microsoft Windows 10 multi-session operating system and have use of App Volumes applications in those desktops, you create a farm of desktop type. Specify the sealed multi-session Microsoft Windows 10 image in which you installed the App Volumes agent.

**Prerequisites**

- Verify that you have at least one image listed on the Images page, that image has an RDSH-capable Windows operating system, the Images page shows that image is in Published state, and that image is located in the pod in which you want to create the farm. You cannot create a farm in a pod without such an image available in that pod.

- Decide if you want this farm's VMs to be connected to a VM subnet that is different from the pod's primary VM subnet (also known as the tenant subnet). If your pod is running manifest 2298 or later and you have edited the pod to add additional VM subnets, you can specify use
of those subnets for this farm. For this use case, you must verify that the VM subnet you want to use is listed on the pod's details page's Networking section in a Ready state so that the subnet will available for you to select in the workflow steps. For details, see Overview of Using Multiple Tenant Subnets with Your Horizon Cloud Pod for Your Farms and VDI Desktop Assignments.

- Decide whether this farm will serve session-based desktops or remote applications. In this release, the same farm cannot serve both.

**Note**  Tech Preview feature: To have your end users use App Volumes applications from a Microsoft Windows 10 multi-session operating system, you must entitle those users to both an App Volumes applications assignment and to a session-based desktops assignment. For this scenario, create a desktops farm to provide those session-based desktops based on that farm. When creating that desktops farm, select the published image that you created by following the steps in Tech Preview - How To Configure a Microsoft Windows 10 Multi-Session Image for Use with App Volumes Features in Horizon Cloud Pods in Microsoft Azure.

- Decide whether you want the farm's RDSH VMs to have encrypted disks. You must specify disk encryption when creating the farm. You cannot later add disk encryption after the farm is created. For a description of the disk capability, see Using Microsoft Azure Disk Encryption with Your Farms and VDI Desktops in Your Horizon Cloud Environment.

- Decide whether you want the ability to use NSX Cloud features with the farm's RDSH VMs. You must enable NSX Cloud management when creating the farm. You cannot later enable the farm for NSX Cloud management after the farm is created. The published image you choose for this farm must have the NSX agent installed in it. You must have installed the NSX agent prior to publishing the image. See VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure and its subtopics.

- If the image's operating system contains Universal Windows Platform (UWP) applications, decide on the method you want to use to ensure that your end users can use those UWP applications from the farm's RDSH VMs. An example is when the image has the Microsoft Windows 10 Enterprise multi-session operating system. The method you choose to enable use of those UWP applications might determine which Active Directory OU you use for the farm. For more information, see Enable a Horizon Agent Policy to Allow Running Universal Windows Platform (UWP) Applications from Microsoft Windows 10 Enterprise Multi-Session RDSH VMs in Horizon Cloud.

Procedure

1. In the administrative console, navigate to **Inventory > Farms**.
2. Click **New**.

   The New Farm wizard opens.
3 In the wizard's Definition step, complete the fields and make your selections as appropriate and then click **Next**.

**Note** You might have to use the scroll bar to see all the required fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for this farm.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter an optional description.</td>
</tr>
<tr>
<td><strong>VM Names</strong></td>
<td>Base name for all of the RDSH VMs created for this farm. The VM names will have numbers appended to this base name, for example, win2016-1, win2016-2, etc. The name must start with a letter and can contain only letters, dashes, and numbers.</td>
</tr>
<tr>
<td><strong>Farm Type</strong></td>
<td>Specify the type of asset this farm provides to end users:</td>
</tr>
<tr>
<td></td>
<td>■ Select <a href="#">Desktops</a> to use this farm to provide session-based desktops.</td>
</tr>
<tr>
<td></td>
<td>■ Select <a href="#">Applications</a> to use this farm to provide access to remote applications. After an applications farm is created, you can use the New Application workflow's <strong>Auto-scan from Farm</strong> option to import applications from the farm's VMs' operating system into your application inventory.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Select the location associated with the pod that has the RDSH image. This selection filters the choices in the Pod field to only the pods in the selected location.</td>
</tr>
<tr>
<td><strong>Pod</strong></td>
<td>Select the pod.</td>
</tr>
</tbody>
</table>

**Tip** If you do not see any pods to select, verify that the Location list is not displaying a location without pods. The Location field works on the Pod list to filter out pods that are not associated with the selected location. If you previously had a pod at a location and then deleted that pod or moved it to a different location, so that the displayed location no longer has any pods, the Pod list will display no entries. Because the locations are listed alphabetically, when the screen opens, it automatically selects the one that is first in the alphabet. If that location no longer has any pods associated with it, you must switch the location to a different entry.

| **Specify VM Subnet(s)** | Enable this toggle to select one or more specific subnets to which the farm's VMs will be connected. After enabling the toggle, you can select the specific subnets from the displayed list. When this toggle is disabled, the farm's VMs will be connected to the pod's primary VM subnet by default. |

Administration of Your Horizon Cloud Tenant Environment and Your Fleet of Onboarded Pods
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Models</td>
<td>Set one or more filters to control the models available in the Models drop-down menu. You can filter models by type, series, number of CPUs, memory, and tags. For more information about selecting models, see Managing VM Types and Sizes for Farms and Assignments, which describes the options on the VM Types &amp; Sizes page (Settings &gt; VM Types &amp; Sizes).</td>
</tr>
</tbody>
</table>

To set a filter, you first select the criterion in the drop-down menu and then enter the desired value(s). By default, there is a single filter with the criterion 'Tag' the value 'VMware Recommended'. You can edit this first filter and add more filters connected by And and Or operators.

The following are the criteria you can use for filters and descriptions of the values you can enter for each.

- **Type**

  When you select this option, there is only value available in the second drop-down menu:

  - **GPU and High Performance** - Models with GPU.

    **Note** If you choose a GPU model (for example, Standard_NV6), then the list of images shown will contain only images that were created with the Include GPU flag selected, so you need at least one such image in order to create a farm or pool using a GPU model. If you choose a non-GPU model, then the list of images shown will contain only images that were created without the Include GPU flag.

- **Series**

  When you select this option, you can then select a series of models from a second drop-down menu. You can also filter this list by entering text in the Filter text box at the top of the list.

- **CPUs**

  When you select this option, you can then enter a CPU range.

  **Important** For production environments, to avoid unexpected end-user connection issues, use VM models that have a minimum of two (2) CPUs.

- **Memory**
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Memory</td>
<td>When you select this option, you can then enter a range of memory in GBs.</td>
</tr>
</tbody>
</table>
| Tag | When you select this option, you can then select a tag from a second drop-down menu. You can also filter this list by entering text in the Filter text box at the top of the list. Tags available in the drop-down menu are both hard-coded system tags and custom tags that you created on the VM Types & Sizes page (Settings > VM Types & Sizes). You can set additional filters by performing the following steps for each filter:  
  a. Click the Add link.  
  b. Select either And or Or as the operator between the previous filter and the new one you are creating.  
  c. Set the new filter by selecting a criterion and entering value(s). |
| **Model** | The choices here are filtered by your selections in Filter Models. Select the VM model to use for the farm's RDSH VMs. This selection defines the set of underlying resources that will be used when the farm's RDSH VMs are created, in terms of capacity (compute, storage, and so on). The available choices map to standard VM sizes that are available in Microsoft Azure.  
  **Important** For production environments, select a VM model that has a minimum of two (2) CPUs. VMware scale testing has shown that using 2 CPUs or more avoids unexpected end-user connection issues. Even though the system does not prevent you from choosing a VM model with a single CPU, you should use such models for tests or proof-of-concepts only. |
| **Disk Type** | Select a supported disk type from the available options. Disk type options are based on the model selected, and your Azure subscription and region. The following are some commonly available disk types.  
  a. Standard HDD - Default disk type.  
  b. Standard SSD  
  c. Premium SSD - Option only appears if you selected a model that supports premium IO. You can edit your selection later if desired. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Size</td>
<td>Enter the OS disk size in GiB for the farm's VMs.</td>
</tr>
<tr>
<td></td>
<td>- The default value is the base image OS disk size (typically 127 GiB).</td>
</tr>
<tr>
<td></td>
<td>- If you edit the size, the value you enter must be greater than the base image OS disk size, and cannot exceed the largest size (typically 1024 GiB) supported by the selected model.</td>
</tr>
<tr>
<td></td>
<td>- You can also edit this value later if desired.</td>
</tr>
<tr>
<td>Important</td>
<td>If you edit the disk size, there are additional actions you must take to ensure that the VMs are created as expected. For more information, see <a href="#">Required Administrator Actions When the Disk Size for a Farm or VDI Desktop Assignment is Increased</a>.</td>
</tr>
<tr>
<td>Image</td>
<td>Select the RDSH image.</td>
</tr>
<tr>
<td>Important</td>
<td>- If the image's operating system contains Universal Windows Platform (UWP) applications, there are additional actions you must take to ensure that your end users will be able to use those UWP applications from the farm's RDSH VMs. For more information, see <a href="#">Enable a Horizon Agent Policy to Allow Running Universal Windows Platform (UWP) Applications from Microsoft Windows 10 Enterprise Multi-Session RDSH VMs in Horizon Cloud</a>.</td>
</tr>
<tr>
<td></td>
<td>- If you set the <strong>NSX Cloud Managed</strong> toggle to <strong>Yes</strong>, ensure that the image you select here has the NSX agent installed on it. For the NSX Cloud management features to work with the farm's VMs, the image that you select for this farm must have the NSX agent already installed on it. The system does not verify if the selected image has the NSX agent when it creates the farm.</td>
</tr>
<tr>
<td>Preferred Protocol</td>
<td>Select a default display protocol you want the end-user sessions to use. Circumstances might occur that cause another protocol to be used instead of the default protocol. For example, the client device does not support the default protocol or the end user overrides the default protocol selection.</td>
</tr>
<tr>
<td>Preferred Client Type</td>
<td>Select the preferred client type used when end users launch their session-based desktops from Workspace ONE Access, either a Horizon Client or a browser for HTML Access.</td>
</tr>
<tr>
<td>Domain</td>
<td>Select the Active Directory domain registered with your environment.</td>
</tr>
<tr>
<td>Join Domain</td>
<td>Select <strong>Yes</strong> so that the farm's VMs are automatically joined to the domain when they are created.</td>
</tr>
<tr>
<td>Encrypt Disks</td>
<td>Select <strong>Yes</strong> so that the farm's VMs have encrypted disks.</td>
</tr>
<tr>
<td>Important</td>
<td>If you want disk encryption, you must make this selection when creating the farm. You cannot later add disk encryption after the farm is created.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>NSX Cloud Managed</strong></td>
<td>Select <strong>Yes</strong> so that you can use features of NSX Cloud with the farm's VMs. For a description of using NSX Cloud features with your farms in Microsoft Azure, see <a href="https://example.com">VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure</a> and its subtopics.</td>
</tr>
</tbody>
</table>
| **Important**                | - If you want to use NSX Cloud with the farm's VMs, you must make this selection when creating the farm. You cannot later enable NSX Cloud management after the farm is created.  
- For the NSX Cloud management features to work with the VMs, the image that you select for this farm must have the NSX agent already installed on it. When you set this toggle to **Yes**, ensure that the image you select in **Image** has the NSX agent installed on it. The system does not verify if the selected image has the NSX agent when it creates the farm. |
| **Min VMs**                  | Specify the minimum number and maximum number of RDSH VMs you want in this farm. When the farm is first created, the system deploys the number of VMs specified in the **Max VMs** field, and then powers off the VMs except the number specified for **Min VMs**. Only the minimum number of VMs are initially powered on. As end user demand increases, the system powers on additional VMs, up to the **Max VMs** number. Then as end-user demand shrinks, the system powers off the VMs, until it reaches the **Min VMs** number of VMs. A VM must be completely empty of user sessions before the system powers it off. When you specify zero (0) for **Min VMs**, it indicates that you want the system to power off all the farm's RDSH VMs when there is no end-user demand for sessions to the farm. When you enter zero (0) for **Min VMs**, use the **Power Off Protect Time** field to specify the amount of time you want the system to wait after determining the remaining powered-on VM has no user sessions before the system powers off that VM. |
| **Max VMs**                  |                                                                                                                                                                                                           |
| **Power Off Protect Time**   | Specify the number of minutes that you want the system to wait before automatically powering off a powered-on farm VM. You can enter a value from 1 to 60. The default is 30 minutes.  
This protect time is used primarily for the situations where the system would normally power off a farm's VM. You can use this **Power Off Protect Time** setting to tell the system to wait the specified time before starting to power off the VM. The default wait time is 30 minutes. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions per VM</td>
<td>Specify the number of concurrent end-user sessions per VM that this farm will allow. For a pod in Microsoft Azure, based on performance testing of user densities, VMware has some recommended maximums. For details about these recommendations and the analysis behind them, see the <em>VMware Horizon Cloud Service™ on Microsoft Azure RDS Desktop and Application Scalability</em> technical paper located <a href="http://vmware.com">here in vmware.com</a>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Due to a NVIDIA driver limitation, if your GPU-enabled image has Microsoft Windows Server 2012 R2 for its operating system, a farm using that image for its RDSH VMs is limited to 20 sessions maximum per VM. If you have that particular combination (image with GPU, Microsoft Windows Server 2012 R2, NVIDIA drivers, and an NV-series model), do not specify more than 20 here.</td>
</tr>
<tr>
<td>Windows license question</td>
<td>The wizard asks you to confirm you have an eligible license to use the Microsoft Windows operating system that is in the image and which will be in the farm's RDSH VMs. Follow the on-screen instructions.</td>
</tr>
</tbody>
</table>
Optionally configure the advanced properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer OU</strong></td>
<td>Active Directory Organizational Unit where the farm VMs are to be located. Enter the Active Directory Organizational Unit using the distinguished name, for example, <code>OU=RootOrgName,DC=DomainComponent,DC=eng</code>, and so on. The OU and each path in a nested OU can contain any combination of letters, numbers, special characters, and spaces, and can have a maximum of 64 characters. If you need to use nested Organization Units, see Considerations For Using Nested Active Directory Domain Organizational Units.</td>
</tr>
<tr>
<td><strong>Run Once Script</strong></td>
<td>(Optional) Location of a script that you want run in the farm's VMs after the VM creation process.</td>
</tr>
</tbody>
</table>
| **Azure Resource Tags** | (Optional) Create custom tags to be applied to Azure resource groups. Azure resource tags are only applied to the resource groups, and are not inherited by the resources in the groups.  
To create the first tag, enter information in the Name and Value fields. To create an additional tag, click Add and then enter information in the Name and Value fields that appear below the existing ones.  
- You can create a maximum of 10 tags.  
- The tag name is limited to 512 characters, and the tag value is limited to 256 characters. For storage accounts, the tag name is limited to 128 characters, and the tag value is limited to 256 characters.  
- Tag names cannot contain the following characters:  
  `< > % & \ ? /`  
- Tag names cannot contain these case-insensitive strings:  
  ‘azure’, ‘windows’, ‘microsoft’  
After a farm has been created, you can add more Azure resource tags and edit or delete tags for that farm. |

Note: If the Computer OU is set to `CN=Computers`, the system uses the default Active Directory Computers container for VMs. Your Active Directory might have this default container redirected to an organizational unit class container.

Note: The script should end with a reboot step to reboot the VM. A sample reboot line as a Windows command is:

```
shutdown /r /t 0
```
4 In the wizard's Management step, complete the fields and make your selections as appropriate and then click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rolling Maintenance</td>
<td>Select the maintenance type, either according to a time cadence (Scheduled) or based on user sessions to this farm's VMs (Session). When Scheduled is selected, configure the maintenance cadence, either daily or weekly. If you choose a daily recurrence, specify the hour at which the maintenance will start. If you choose a weekly recurrence, specify both the day of the week and the hour. When Session is selected, specify the number of sessions at which the farm should begin rolling maintenance. <strong>Note</strong> Sessions which are logged off within 15 minutes are not counted for the purposes of the rolling maintenance calculations, to prevent restarting or rebuilding the VMs based on a count of short running sessions. In the Concurrent Quiescing VMs field, specify the number of farm VMs that can be in the quiescing state at the same time. When a VM is in quiescing state, the VM continues to work for the user sessions already connected to that VM, but it does not accept any new user connections. For a simple example, see Example of Farm Rolling Maintenance.</td>
</tr>
</tbody>
</table>
| VM Action          | Select the action that the system should perform on the VMs undergoing maintenance.  
  ■ With **Restart**, the VMs are restarted.  
  ■ With **Rebuild**, the VMs are first deleted and then reprovisioned based on the farm's associated image. If you choose to have the unused VMs powered off, they will still consume some storage use in your cloud environment. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Power Management  | These power management settings are related to the thresholds at which the system automatically increases and shrinks the number of powered-on farm VMs according to the session usage on the VMs. When the usage increases above an upper bound, the system automatically powers up one of the unused VM. When the usage shrinks below a lower bound, the system drains the VM until it is not being used. Then the system shuts down the VM and deallocates it. The power management selections balance capacity cost with faster availability:  
  - Select **Optimized Performance** when you want the system to power on the next VM sooner rather than later. Even though you are spending more by having the next VM ready to go before the user demand requires it, this setting increases the chance that when users log in, the VM is already powered up to meet that demand.  
  - Select **Optimized Power**, when you want the system to wait the maximum amount of time possible before powering on the next VM. The occupancy of the VMs is higher before the system powers up the next one. Even though this selection minimizes capacity costs by getting higher use of the existing VMs, this setting increases the chance that there might be a delay when new users try to log in because they might have to wait during the time system has to power on the VM.  
  - Select **Balanced** to strike a balance between capacity costs and time-to-availability for users.  
  The low and high thresholds for each selection are:  
  - **Optimized Performance**  
    - Low threshold: 23%  
    - High threshold: 50%  
  - **Optimized Power**  
    - Low threshold: 38%  
    - High threshold: 80%  
  - **Balanced**  
    - Low threshold: 31%  
    - High threshold: 66%  
  For an in-depth description about the power management features of Horizon Cloud and descriptions of how they work in various scenarios, see the [VMware Horizon Cloud Service™ on Microsoft Azure RDS Desktop and Application Scalability](vmware.com) technical paper located here.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout Handling</td>
<td>Configure how you want the system to handle certain types of user sessions.</td>
</tr>
</tbody>
</table>

**Note** The user sessions governed by these settings are the user logins to the Windows operating system session of the RDS session desktop or application. These sessions are not the user logins in Horizon Client, Horizon HTML Access, or Workspace ONE.

The user's session begins when the user authenticates to the Windows operating system that underlies the session-based desktop or the remote application that is served from this farm's RDSH VMs.

- **Empty Session Timeout** - For applications farms, select how the system should handle idle user sessions, whether to never time out idle sessions or to time out after a specified number of minutes. Idle timeouts are based on the activity on the endpoint device, not on the session-based desktop or application. If you specify to time out an idle session, select what happens when the timeout period is up: whether to disconnect the session or log the user off. When a session is disconnected, the session is disconnected from the network and preserved in memory. When a session is logged off, the session is not preserved in memory, and any unsaved documents are lost.

- **Log Off Disconnected Sessions** - Select when the system logs the user off of a disconnected session.

- **Max Session Lifetime** - Specify the maximum number of minutes the system should allow for a single user session.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Timeout Interval</td>
<td>This time interval is the amount of time the end users’ sessions can be idle before the system forces a logoff from the session-based desktops or applications that are served by this farm. This timeout applies to the logged-in session to the underlying Windows operating system. The time you specify here is different from the time out settings that govern the end users’ Horizon Client or HTML Access logged-in session.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> When the system forces the logoff in the underlying Windows operating system session, any unsaved data is lost. To prevent an unintended loss of data, set this interval high enough to accommodate the business needs of your end users.</td>
</tr>
<tr>
<td></td>
<td>The default interval is one day (1440 minutes).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If no user activity occurs before the timeout interval is reached, a message indicates that the user will be logged off if they do not click <strong>OK</strong> in the next 30 seconds. If the logout occurs, any unsaved user data, such as documents or files, is lost.</td>
</tr>
<tr>
<td>Schedule Power Management</td>
<td>To help optimize savings and performance of the farm’s VMs in Microsoft Azure, you can optionally configure schedules to adjust the minimum number of powered-on VMs in this farm on a recurring weekly basis. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ For weekends or night hours when you know that your end users will not be using their desktops or remote applications, you can have a schedule for zero or a low number of powered-on VMs.</td>
</tr>
<tr>
<td></td>
<td>▪ For specific days or specific hourly stretches that you can predict will have increased end-user demand, you can have a schedule that increases the minimum number of powered-on VMs to be available to meet that demand.</td>
</tr>
<tr>
<td></td>
<td>You can specify up to 10 schedules for the farm. If any schedules have overlapping time periods but specify different minimum VM numbers, the system uses the largest value of minimum VMs for the overlapping time period.</td>
</tr>
<tr>
<td></td>
<td>a Click the + icon to add the first row in the Schedule Power Management section.</td>
</tr>
<tr>
<td></td>
<td>b Enter an identifying name for the first schedule.</td>
</tr>
<tr>
<td></td>
<td>c Select the days for the first schedule.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> One day is selected by default when the row is added. If you do not want to include the selected day in this schedule, click the drop-down and deselect that selected day.</td>
</tr>
<tr>
<td></td>
<td>d Specify the applicable hours in the specified days. Either:</td>
</tr>
<tr>
<td></td>
<td>▪ Select the <strong>All Day</strong> check box to have this schedule in effect for all hours of the specified days.</td>
</tr>
<tr>
<td></td>
<td>▪ Specify start and end times for the time period in each day.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Encrypted VMs take longer to power on than non-encrypted VMs. If you have set <strong>Encrypt Disks</strong> to <strong>Yes</strong>, and you want 100% of the encrypted VMs to be ready for end-user connections at a particular time of day, you might have to set an earlier start time here. See [When Scheduling Power Management for Farms and VDI Desktop Assignments That Have Large Numbers of Encrypted VMs](<a href="https://v2.vmware.com/viewer/pdf/1/vmware">https://v2.vmware.com/viewer/pdf/1/vmware</a> Horizon Cloud Whitepaper.pdf).</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>e</td>
<td>Select the time zone. The time zone closest to your end users' location is recommended. As appropriate for the selected time zone, Daylight Savings Time is automatically applied.</td>
</tr>
<tr>
<td>Note</td>
<td>If two schedules have the same time zone setting and have overlapping times, a warning is displayed. However, if two schedules have different time zone settings and overlap, the warning is not displayed. As an example, if you have two all-day Saturday schedules and one has Europe/London time zone selected and the other has America/Toronto selected, the overlap warning does not display.</td>
</tr>
<tr>
<td>f</td>
<td>In the Min VMs field, enter the minimum number of VMs you want powered on during the specified time period. During the specified time period, that number of VMs at a minimum will be powered on to be available to take end-user requests during that time. The number can range from zero (0) up to the number specified for Max VMs for the farm. When this number is zero (0) and there are no active end-user sessions at the schedule's starting time point, the farm's VMs are powered off. In that scenario, if an end user then attempts to connect to a desktop or application served by this farm during the scheduled time period, there will be a delay before the desktop or application is in a usable state because the underlying VM has to power on.</td>
</tr>
</tbody>
</table>

5 In the wizard’s Load Balancing step, enter values for **Login Threshold**. This setting controls the number of logins allowed within a time period before a VM is deprioritized for having new sessions assigned to it. For example, if **Login Threshold** is set to 3 logins per 30 seconds, then whenever there have been 3 logged-in sessions assigned to VM 1 within the previous 30 seconds, the next session is assigned to VM 2, and so on.  

**Note** Load Balancing settings might not appear or might be disabled if you have an older environment or if the agent for the farm is not the latest version.

6 Complete the fields under **Session Host Load balancing settings**.  
   - Horizon Cloud agents use the first five settings (**CPU Usage Threshold**, **Memory Usage Threshold**, **Disk Queue Length Threshold**, **Disk Read Latency Threshold**, and **Disk Write Latency Threshold**) to calculate the Agent Load Index, a value between 0 and 100 that measures a VM's load.  
   - The last setting, **Load Index Threshold**, is the Agent Load Index value at which a VM is considered full.  

**Important** Because of the key role that Agent Load Index plays in power management, it is essential that you select appropriate values for these settings so you can achieve the desired balance of power consumption and performance in your environment.
For more information about how Agent Load Index affects power management, see About Power Management and Load Balancing for Farms in Horizon Cloud.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU Usage Threshold</strong></td>
<td>Threshold value for the CPU usage in percentage. You can set a value from 0 to 100. The recommended value is 90, which is also the default value.</td>
</tr>
<tr>
<td><strong>Memory Usage Threshold</strong></td>
<td>Threshold value for the memory in percentage. You can set a value from 0 to 100. The recommended value is 90, which is also the default value.</td>
</tr>
<tr>
<td><strong>Disk Queue Length Threshold</strong></td>
<td>Threshold of the average number of both read and write requests that were queued for the selected disk during the sample interval. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.</td>
</tr>
<tr>
<td><strong>Disk Read Latency Threshold</strong></td>
<td>Threshold of the average time of read of data from the disk in milliseconds. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.</td>
</tr>
<tr>
<td><strong>Disk Write Latency Threshold</strong></td>
<td>Threshold of the average time of write of data to the disk in milliseconds. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.</td>
</tr>
</tbody>
</table>
| **Load Index Threshold** | Value of the Agent Load Index at which a VM is considered to be full and is not assigned any new sessions. You can enter a value between 0 and 100. The default value is 90.   

**Note**  The system corrects this value if necessary to be greater than the power management high threshold. This ensures effective power management. |

7 Click Next.

8 In the wizard's Summary step, review the settings and then click Submit to begin creating the farm.

Results

The system starts creating the farm. You can monitor the progress using the Activity page. When the farm's status shows a green dot on the Farms page, the farm is ready for use.
Note  Creation of an encrypted farm VM takes approximately twice as long as creating a non-encrypted VM. As a result, the end-to-end time to complete creating a farm that has disk encryption enabled is approximately twice as long as creating that farm without disk encryption enabled.

Also, when an image VM has a data disk, additional time is needed for creating an encrypted farm VM based on that image VM. The longest times occur for data disks of larger, terabyte sizes.

What to do next

If you created a desktops farm, you would next create a session-based desktop assignment for your end users by following the steps in Create an RDSH Session Desktop Assignment.

Note  Tech Preview feature: If you created a desktops farm to have your end users use App Volumes applications in a Microsoft Windows 10 multi-session operating system, you would perform these workflows next:

1 Ensure the App Volumes applications are added into your applications inventory Add an App Volumes Application by Importing an Existing App Package.

2 Entitle those applications to your users by Create an App Volumes Assignment.

3 Entitle a session-based desktop to those users, based on this farm by Create an RDSH Session Desktop Assignment.

If you created an applications farm, you would next scan that farm to load applications into Horizon Cloud and then create an applications assignment so your end users can use the remote applications from that farm.

For more information, see Applications in Your Horizon Cloud Inventory, Remote Applications - Importing from RDSH Farms that are Provisioned by Horizon Cloud Pods in Microsoft Azure, and Remote Applications - Create a Remote Application Assignment for Remote Applications Provisioned By Horizon Cloud Pods in Microsoft Azure.

If the image for this farm has applications that require opening special ports, you might need to modify this farm’s associated Network Security Group (NSG) in Microsoft Azure. For details about the NSG, see About Network Security Groups and Your Farms.
If you specified NSX Cloud management for this farm, you can use your NSX Cloud environment’s Service Manager (CSM) to see that the farm’s VMs are managed in NSX Cloud. Log in to your environment’s CSM and navigate to **Clouds > Azure >Instances**. When that Instances page shows a status of Managed for the farm’s VMs, you can start implementing NSX policies on them.

**Enable a Horizon Agent Policy to Allow Running Universal Windows Platform (UWP) Applications from Microsoft Windows 10 Enterprise Multi-Session RDSH VMs in Horizon Cloud**

When you create a farm based on a Microsoft Windows 10 Enterprise multi-session operating system VM and you want your end users to be able to use Universal Windows Platform (UWP) applications that the operating system provides, you must enable a specific Horizon Agent policy that is disabled by default. The Horizon Agent’s default policy settings do not permit launch of UWP applications. As a result, you must take some steps to enable the Horizon-agent-related Group Policy Setting named *Enable UWP support on RDSH platforms* so that your end users can use those UWP applications.

For a description about the required setting and the Horizon ADMX template that contains it, look for that *Enable UWP support on RDSH platforms* name in this VMware Horizon 7.12 documentation topic [*VMware View Agent Configuration ADMX Template Settings*](#). From that VMware Horizon documentation page, you can see that the corresponding Horizon Agent policy within the farm VMs will be disabled by default. Therefore, you must enable it to permit your end users to use the UWP applications provisioned from those farm VMs — either in session-based desktops or remote applications. Unless that agent policy is enabled, the UWP application status shows as Unavailable to the Horizon Agent installed in the RDSH VM, and as a result, an end user would not be able to access that UWP application.

**Important** After enabling the policy, you must force the GPO setting to the farm’s existing RDSH VMs and you must restart the VMware Horizon View Agent service (wsm.exe) in those RDSH VMs or restart the RDSH VM to make the GPO take effect.

The Horizon Agent Configuration ADMX template file (named *vdm_agent.admx*) contains this policy setting in its *Unity Touch and Hosted Apps* folder (*VMware View Agent Configuration > Unity Touch and Hosted Apps*). One way to configure the required policy setting to the farm’s RDSH VMs is to use that ADMX template file in your Active Directory server to add the *Unity Touch and Hosted Apps* folder to your Active Directory server’s Group Policy Management Editor. When the folder is present there, then you can enable the UWP support for the VMs using a GPO in your Active Directory system on the farm’s target OU by following the sample steps below.
Prerequisites

In your Active Directory server, create a named GPO that you'll use to apply the UWP group policy setting to the RDSH VMs. The Group Policy Management Console (GPMC) is typically launched by Start > Administrative Tools > Group Policy Management. Link the GPO you create to the OU in which those RDSH VMs will exist. This OU is the one specified in the Create Farm page when you create the farm that will have provision those RDSH VMs. If you do not specify an OU in the Create Farm page, the default OU used is the one you specify when you register the Active Directory server with Horizon Cloud, in the Active Directory registration workflow.

Remember  Ultimately, the goal is to ensure that the farm RDSH VMs have the required agent policy enabled if you want your end users to launch the UWP applications. The steps here are an example of one way in which you can enable the required policy on the RDSH VMs. You might choose to adopt a different method that provides you the same result. That would be your choice.

Procedure

1 Download the Horizon 7.11 View GPO Bundle from the VMware Horizon Cloud Service on Microsoft Azure downloads page in https://my.vmware.com.

Tip  Version 7.11 is the version in which the policy setting was introduced into the Horizon View GPO bundle and which is available at the time of this writing. When later versions become available, you can use those also.

From that URL, you must log in with your My VMware account credentials. Navigate to the Horizon Cloud Service on Microsoft Azure downloads location. The following URL might work for you directly to locate the 7.11 version GPO bundle, although sometimes browser caching issues have been reported that result in direct linking to this URL not working: https://my.vmware.com/group/vmware/details?downloadGroup=HCS-MA-220&productId=716&rPId=40176. In that page, you will see a list of downloadable items. Locate the entry named Horizon 7.11.0 View GPO Bundle and download its ZIP file. All of the ADMX files that provide group policy settings for Horizon-related components are in this file. The file itself is named like VMware-Horizon-Extras-Bundle-x.y.z-nnnnnn.zip, where x.y.z-nnnnnn represent the build numbers for this file.

2 Unzip the ZIP file and copy the following files to the indicated locations:

- Copy the vdm_agent.admx file to your Active Directory server, to the %systemroot%\PolicyDefinitions location.

- Copy the vmd_agent.adml language resource file for the locale you want (such as en-US/vmd_agent.adml) file to your Active Directory server, to the %systemroot%\PolicyDefinitions\<locale> location where <locale> matches the locale of the ADML file you are copying.

3 On the Active Directory server, open Group Policy Management and select to edit the GPO that you created for applying the UWP group policy settings.
4 In the Group Policy Management Editor, expand the Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > Unity Touch and Hosted Apps.

5 In that Unity Touch and Hosted Apps folder, locate the Enable UWP support on RDSH platforms and edit it to set it to Enabled.

6 Link that GPO with the OU in which the farm's RDSH VMs are created.

Remember When you link the GPO with the OU in which the farm's VMs are created, the UWP policy that you set in that GPO using the steps above is applied to all of the VMs in that OU. That is standard GPO behavior.

7 Force the GPO setting to the farm's RDSH VMs.

8 Restart the VMware Horizon View Agent service (wsnm.exe) in those RDSH VMs.

Managing Farms in Horizon Cloud

You can perform several actions on the farms listed on the administrative console's Farms page.

Actions You Can Perform on the Farms Page

At a page level, you can select the check box next to an existing farm and click one of the buttons to perform its associated action on the farm.

Edit

Clicking this button launches a wizard in which you can change certain settings, such as the farm's power management settings, the minimum and maximum number of VMs the farm can have, and so on. The wizard is similar to the New Farm wizard, with read-only fields for those settings that cannot be changed for an existing farm. For detailed descriptions of the fields, see Create a Farm.
Alternatively, instead of using the **Edit** button, you can click the farm's name and update the settings from the farm's summary page.

**Note** When you edit the farm and reduce the **Sessions per VM** value, any existing sessions in excess of the new lower value are not automatically logged off. You can either manually log off the excess sessions or wait until the system logs off the sessions according to the values for the farm's **Timeout Handling** settings (**Empty Session Timeout**, **Log Off Disconnected Sessions**, **Max Session Lifetime**) and **Session Timeout Interval**. Because those existing sessions in excess of the new lower value are not automatically logged off, the console might display VM and farm utilization values higher than 100% until the excess active sessions are logged off.

For your farms in Microsoft Azure

- When you change the **Sessions per VM** value, the system might power on or power off the farm's VMs to meet the new load on the farm based on the updated value.

- If the model VM you selected to create the farm has become unavailable, you will not be able to expand the farm. The farm will remain fully functional except for this limitation. To see if a VM type is available, navigate to the VM Types & Sizes page (**Settings > VM Types & Sizes**). For more information about model VMs, see [Managing VM Types and Sizes for Farms and Assignments](#).

**Take Offline**

Clicking this button opens a window in which you can select to take a farm offline for maintenance.

**Bring Online**

Clicking this button opens a window in which you can select to bring an offline farm back online.

**Delete**

You use this button to delete the selected farm. However, before you can delete a farm using this button, you must delete any assignments that are using the farm. You can view the assignments that are using the farm by navigating to the Assignments page and sorting on its **Farms** column.

**Note** Deleting the farm deletes all the farm's underlying RDSH VMs. When a farm is deleted, all of that farm's logged activity is removed from the Activity page.

**Actions You Can Perform Within a Farm's Detailed Pages**

From the Farms page, you can click a farm's name to see its detailed pages. Initially the Summary page is displayed.

The following screenshot is an illustration of a farm's Summary page for a farm in a pod in Microsoft Azure.
Summary page

The Summary page displays the farm's current settings. For each page section, you can click the pencil icon to change those settings that the system allows to be updated for an existing farm. Some settings cannot be changed on a farm after it is created, such as its pod.

Session Hosts page

The Session Hosts page displays the existing RDSH instances in the farm. The actions you can perform on a selected instance are power on or off (depending on the VM's current state), delete, and reset the agent pairing.

Sessions page

The Sessions page displays the farm's existing user sessions. When you select a session, you can disconnect it or log the user off the session. When you click Disconnect, you force the user's session to be disconnected. No message is sent to the user that the session is disconnecting. When you click Log Off, a message is displayed to the user with a grace period in which the user can save documents before the session ends.

System Activity page

The System Activity page displays activity in the farm due to system actions, such as expanding the farm.
You can cancel assignment-related tasks before they complete by selecting the task in the list and clicking **Cancel Tasks**.

- Before attempting to select a task for cancellation, refresh the view to update the status for the tasks displayed.
- If a task is in a state where the system allows you to cancel it, you can select the check box corresponding to that cancelable task.

The following table shows tasks that you can cancel.

<table>
<thead>
<tr>
<th>Task</th>
<th>Cancel When Task is in Queued State</th>
<th>Cancel When Task is in Running State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Farm Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the system has</td>
<td><strong>Note</strong> When the system has</td>
</tr>
<tr>
<td></td>
<td>automatically created an expansion</td>
<td>automatically created an expansion</td>
</tr>
<tr>
<td></td>
<td>task for an RDSH farm, the farm must</td>
<td>task for an RDSH farm, the farm must</td>
</tr>
<tr>
<td></td>
<td>be offline before you can cancel</td>
<td>be offline before you can cancel</td>
</tr>
<tr>
<td></td>
<td>that task.</td>
<td>that task.</td>
</tr>
<tr>
<td>Assignment Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the system has</td>
<td><strong>Note</strong> When the system has</td>
</tr>
<tr>
<td></td>
<td>automatically created an expansion</td>
<td>automatically created an expansion</td>
</tr>
<tr>
<td></td>
<td>task for a VDI desktop assignment,</td>
<td>task for a VDI desktop assignment,</td>
</tr>
<tr>
<td></td>
<td>the assignment must be offline</td>
<td>the assignment must be offline</td>
</tr>
<tr>
<td></td>
<td>before you can cancel that task.</td>
<td>before you can cancel that task.</td>
</tr>
<tr>
<td>Convert VM to Image</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you cancel this task,</td>
<td><strong>Note</strong> If you cancel this task,</td>
</tr>
<tr>
<td></td>
<td>and want to retry it, first confirm</td>
<td>and want to retry it, first confirm</td>
</tr>
<tr>
<td></td>
<td>that the VM is in a state where it</td>
<td>that the VM is in a state where it</td>
</tr>
<tr>
<td></td>
<td>can be converted.  If you are not</td>
<td>can be converted.  If you are not</td>
</tr>
<tr>
<td></td>
<td>sure, power off and then power on</td>
<td>sure, power off and then power on</td>
</tr>
<tr>
<td></td>
<td>the VM.</td>
<td>the VM.</td>
</tr>
</tbody>
</table>

**User Activity page**

The User Activity page displays activity in the farm due to user actions, such as logging on and logging off sessions provided by the farm.
Manage Farm RDSH Session Hosts

You can perform certain actions on the individual RDSH session hosts in a farm.

Procedure

1. Click **Inventory > Farms**.
   The Farms page displays.

2. Click the name of a farm on the list.
   The farm details page displays.

3. Click **Session Hosts** at the top of the page.
   The Session Hosts tab displays, showing a list of the RDSH session host virtual machines (VMs) in the farm. You can filter, refresh, and export the list using the controls to the top right of the page.

   You can perform the following actions by selecting one or more session host VMs and clicking one of the buttons at the top of the page.

   **Note**  The VM status must be green to perform these actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Off</td>
<td>Shuts down the selected VMs.</td>
</tr>
<tr>
<td></td>
<td>- You can select more than one VM at a time.</td>
</tr>
<tr>
<td></td>
<td>- You can only shut down VMs that do not have active user sessions.</td>
</tr>
<tr>
<td>Power On</td>
<td>Starts up the selected powered-off VMs.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected VM. To reduce the size of the farm when the VM is deleted, select <strong>Yes</strong> under 'Reduce farm size' in the dialog box.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Reset Agent Pairing | Repairs the agent pairing state when a pairing failure has occurred.  
  ■ You can select multiple VMs. The action is only applied to those selected VMs that are currently powered on.  
  ■ You can view progress on the Monitor > Activity page or on the System Activity tab of the farm's detail page. |
| User Login Mode     | Controls user logins for maintenance purposes. Settings are described below.  
  **Note** You can only change this setting if the VM has the latest agent.  
  ■ Allow Logins (Active)  
    ■ Allows new connections to the VM.  
    ■ Allows reconnections to the VM.  
    ■ Agent Status is Active.  
  ■ Prevent New Logins and Reconnections (Disabled)  
    ■ Does not send new connection requests to the VM.  
    ■ Routes new connections to other available VMs in the farm.  
    ■ Denies reconnections to the VM.  
    ■ Agent Status is Disabled.  
  **Note** You must log in or reconnect to the VM before selecting this option.  
  ■ Prevent New Logins Only (Drain)  
    ■ Does not send new connection requests to the VM.  
    ■ Routes new connections to other available VMs in the farm.  
    ■ Allows reconnections to the VM.  
    ■ Agent Status is Draining.  
  **Note** You must have an existing session on the VM before selecting this option.  
  ■ Prevent New Logins (Drain) Until Restart  
    ■ Does not send new connection requests to the VM until the VM is restarted.  
    ■ Routes new connections to other available VMs in the farm until the VM is restarted.  
    ■ Allows reconnections to the VM.  
    ■ Agent Status is Draining Until Restart.  
    ■ Reverts to Allow Logins setting after VM restart.  
  **Note** You must have an existing session on the VM before selecting this option. |

**About Network Security Groups and Your Farms**

For every Horizon Cloud pod deployed into your Microsoft Azure cloud, a network security group (NSG) is also created in the pod's resource group to act as a template. You can use this template to ensure you have opened those additional ports that you might need for the remote applications or RDS desktops provided by your farms.

In Microsoft Azure, a network security group (NSG) governs the network traffic to the resources connected to Azure Virtual Networks (VNet). An NSG defines the security rules that allow or deny that network traffic. For more detailed information about how NSGs filter network traffic, see the Microsoft Azure documentation topic [Filter network traffic with network security groups](#).
When a Horizon Cloud pod is deployed into Microsoft Azure, an NSG named `vmw-hcs-podID-nsg-template` is created in the pod's same resource group named `vmw-hcs-podID`, where `podID` is the pod's ID. You can obtain the pod's ID from the pod's details page, navigating from the Capacity page in Horizon Cloud's administrative console.

By default, the pod's template NSG is configured with no outbound security rules and with the following inbound security rules. These default inbound security rules support end-user clients’ access to the RDS session desktops and remote applications for Blast and PCOIP and USB redirection.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Name</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>AllowBlastUdpIn</td>
<td>22443</td>
<td>UDP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>1100</td>
<td>AllowBlastTcpIn</td>
<td>22443</td>
<td>TCP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>1200</td>
<td>AllowPcoipTcpIn</td>
<td>4172</td>
<td>TCP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>1300</td>
<td>AllowPcoipUdpIn</td>
<td>4172</td>
<td>UDP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>1400</td>
<td>AllowTcpSideChannelIn</td>
<td>9427</td>
<td>TCP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>1500</td>
<td>AllowUsbRedirectionIn</td>
<td>32111</td>
<td>TCP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
</tbody>
</table>

In addition to this template NSG, when a farm is created, the system creates an NSG for that farm by copying the template NSG. Every farm has its own NSG that is a copy from the template NSG. A farm's NSG is assigned to the NICs of that farm's virtual machines (VMs). By default, every farm uses the same default security rules as configured in the pod's template NSG.

You can modify both the template NSG and the per-farm NSGs. For example, if you have an application in a farm that you know needs an additional port opened for that application, you would modify that farm's NSG to allow network traffic on that port. If you are planning to create multiple farms that need the same port opened, a simple way to support that scenario is to edit the template NSG prior to creating those farms.

**Important**  When planning to modify the base template, make a copy before modifying it. The copy can be a backup in case you need to revert back to the original default settings.

**Example of Farm Rolling Maintenance**

This example describes how Horizon Cloud provisions a new farm's RDSH virtual machines (VMs) and manages them for rolling maintenance.

In the New Farm wizard, this farm is sized as:

- **Min VMs** = 1
- **Max VMs** = 3
- **Sessions per VM** = 20
In the creation workflow:

1. All three RDSH VMs are fully configured in Microsoft Azure: powered on and joined to the domain.
2. Then VMs 2 and 3 are powered down to save the cost of running them.

VM 1 remains powered up and ready to provide user sessions.

As users log on, they are given sessions on VM 1. When the occupancy of the available VMs, VM 1 here, reaches the power management threshold, then another VM is powered on (VM 2). When two VM are powered on, new user sessions are placed on the least loaded VM so that sessions are load balanced between the two powered-on VMs. When the number of user sessions reaches the next occupancy threshold as calculated across both powered-on VMs, the next VM powers on (VM 3).

As users log off of their sessions:

1. When the occupancy drops below the low threshold, then one of the VMs is marked for quiescing. Typically, the system marks the least loaded VM for quiescing.
2. Once marked, existing sessions stay on that VM, but no new user sessions are accepted for that VM. At that point, any new sessions are only placed on the running VMs.
3. When all of the users with existing sessions on the marked VM have logged off their sessions, Horizon Cloud powers off that VM.

The above steps repeat until the number of running VMs reaches the Min VMs value.

**Rolling Maintenance**

A best practice for virtual machine maintenance is to restart the VMs from time to time, to clear out cached resources or any memory leaks from third-party applications in the VM. The Horizon Cloud rolling maintenance feature provides for restoring normal health across the farm in an automated way. The typical action is to restart the VMs. Horizon Cloud offers an additional option to rebuild the farm’s VMs, by deleting the VMs and reprovisioning them based on the latest published image used for that farm. The rebuild option provides a convenient way to ripple image updates across the farm’s VMs automatically and regularly. The rebuild option avoids needing manual intervention as a part of routine operations.

At any one time, the system only quiesces the number of VMs configured for the farm’s Concurrent Quiescing VMs value. As set by the Maintenance Type configured for the farm’s rolling maintenance, the system goes through each of the VMs and performs the specified maintenance action. The action is not performed on VMs that have active user sessions nor on more than the number set in Concurrent Quiescing VMs.

**About Power Management and Load Balancing for Farms in Horizon Cloud**

This topic describes how Agent Load Index, based on load balancing settings, is used for power management in RDSH farms in Horizon Cloud.
Horizon Cloud agents use five settings (CPU Usage Threshold, Memory Usage Threshold, Disk Queue Length Threshold, Disk Read Latency Threshold, and Disk Write Latency Threshold) to calculate the Agent Load Index, a value between 0 and 100 that measures each VM's load. For more information about these settings, see Create a Farm.

**Important** Because of the key role that Agent Load Index plays in power management, it is essential that you select appropriate values for these settings so you can achieve the desired balance of power consumption and performance in your environment.

Usage of a farm is determined by selecting the higher of the following two percentage values:

- Session occupancy - The number of active sessions within a farm divided by the total number of sessions possible on the powered-on VMs in the farm. The number of sessions possible is calculated by multiplying the number of powered-on VMs in the farm by the Sessions per VM value you set for the farm. For more information on the Sessions per VM setting, see Create a Farm,

- Average load index - The average Agent Load Index of the powered-on VMs in the farm.

For farm expansion, that value is then compared to the high threshold for the Power Management setting you selected for the farm. For more information about the Power Management setting, see Create a Farm.

In both of the following examples, the Power Management setting for the farm is Optimized Performance. The high threshold for the Optimized Performance setting is 50%, meaning that when the usage reaches 50%, the system powers up one of the unused VMs.

**Note** In the examples below, the Max VMs setting for the farm must be greater than 1. Otherwise, the expansion does not occur. For more information about the Max VMs setting, see Create a Farm.

**Example - Farm Expansion Due to Session Occupancy Exceeding the High Threshold**

In this example, settings are as follows:

- Sessions per VM = 20
- High threshold for Power Management = 50%
### Example - Farm Expansion Due to Average Load Index Exceeding the High Threshold

In this example, settings are as follows:

- **Sessions per VM** = 20
- **High threshold for Power Management** = 50%

#### Before Expansion

<table>
<thead>
<tr>
<th>Powered-on VMs</th>
<th>Usage values</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM 1</td>
<td></td>
</tr>
<tr>
<td>Sessions running = 5</td>
<td></td>
</tr>
<tr>
<td>Agent Load Index = 50%</td>
<td></td>
</tr>
<tr>
<td>Average load index = Agent Load Index 50% / 1 VM = 25%</td>
<td></td>
</tr>
</tbody>
</table>

The higher of the two values is 50%, which matches the high threshold for the Optimum Performance setting for Power Management. As a result, the system powers on a second VM.

#### After Expansion

<table>
<thead>
<tr>
<th>Powered-on VMs</th>
<th>Usage values</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM 1</td>
<td></td>
</tr>
<tr>
<td>Sessions running = 5</td>
<td></td>
</tr>
<tr>
<td>Agent Load Index = 50%</td>
<td></td>
</tr>
<tr>
<td>VM 2</td>
<td></td>
</tr>
<tr>
<td>Sessions running = 0</td>
<td></td>
</tr>
<tr>
<td>Agent Load Index = 0%</td>
<td></td>
</tr>
<tr>
<td>Average load index = Agent Load Index 25% / 1 VM = 25%</td>
<td></td>
</tr>
</tbody>
</table>

The higher of the two values is 25%, which is below the high threshold for the Optimum Performance setting for Power Management. As a result, the system takes no action.
inventory. These applications are the ones that you want to provide for your end users to use. In the console, you open the Applications page by clicking **Inventory > Applications**.

The system categorizes the applications in this inventory depending on the application's source.

- **App Volumes applications** contain app packages created using App Volumes. The console provides for adding such applications to your inventory when your Horizon Cloud tenant is configured to use App Volumes features on pods deployed in Microsoft Azure. See **App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites**.

- **Remote applications** are those added into your inventory from the RDSH farms of type Applications (as shown on the console's Farms page). When they are added into the inventory, you can assign these remote applications to your users. See **Remote Applications - Importing from RDSH Farms that are Provisioned by Horizon Cloud Pods in Microsoft Azure**.

In addition to adding new applications into your inventory, the page also provides for editing the applications and removing them from the inventory.

**App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites**

Using App Volumes applications functionality, you can manage the entire life cycle of applications, including packaging, updating, and retiring an application. You can also customize application assignments to deliver specific versions of an application to end users.

**Overview of VMware App Volumes Functionality in Horizon Cloud**

**Overview of the App Volumes Application Process**

**Prerequisites for App Volumes Applications**

**Adding an App Volumes Application Using a Windows 10 Enterprise Multi-Session VM**

**Overview of VMware App Volumes Functionality in Horizon Cloud**

The following table provides an overview of VMware App Volumes functionality in Horizon Cloud.

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment</td>
<td>- Zero-touch deployment. Auto-provisioning of App Volumes infrastructure</td>
</tr>
<tr>
<td></td>
<td>components, such as App Volumes Managers, App Volumes databases, and</td>
</tr>
<tr>
<td></td>
<td>storage.</td>
</tr>
<tr>
<td></td>
<td>- Leverages Microsoft Azure PostgreSQL managed service for database needs.</td>
</tr>
<tr>
<td></td>
<td>No additional database management required.</td>
</tr>
<tr>
<td></td>
<td>- Automatic provisioning of Microsoft Azure File Shares during pod setup to</td>
</tr>
<tr>
<td></td>
<td>store and deliver apps.</td>
</tr>
<tr>
<td>Management Console</td>
<td>- App Volumes console is seamlessly integrated into the Horizon Cloud</td>
</tr>
<tr>
<td></td>
<td>administration console. Manage desktops and apps in the same console.</td>
</tr>
<tr>
<td></td>
<td>- App Volumes Agent installation experience seamlessly integrated into the</td>
</tr>
<tr>
<td></td>
<td>Horizon Cloud image creation workflows.</td>
</tr>
<tr>
<td>App Volumes 4 agent</td>
<td>Unified performance-optimized agent used both for on-premises and Microsoft</td>
</tr>
<tr>
<td></td>
<td>Azure deployments.</td>
</tr>
</tbody>
</table>
## Functional Area | Description
--- | ---
Packaging |  - Supports VHD based packages that are delivered using Microsoft Azure fileshares.  
  - App package creation performed natively within Horizon Cloud. No command-line tools necessary.
Application Lifecycle Management | Supports Simplified Application Management (SAM) capability that is already a part of App Volumes 4 on-prem. Administrators can now manage the entire lifecycle of the application, including packaging, updating, and retiring.
Application Assignment |  - Administrators can customize their application assignments to deliver specific versions of an application to end users.  
  - Supports multi-pod application delivery.
Hybrid Cloud Support | On-prem App Volumes customers can now import their application packages from their on-prem deployments into Horizon Cloud on Microsoft Azure. Reuse on-prem packages. No need to repackage for Microsoft Azure.
Preview features |  - (Preview Only) - Customers can import MSIX app attach VHDs and evaluate delivering this new package format using App Volumes.  
  - (Preview Only) - Customers can evaluate App Volumes native format with Windows 10 Enterprise multi-session.  
  - (Preview Only) - Customers can evaluate MSIX app attach format with Windows 10 Enterprise multi-session.

### Overview of the App Volumes Application Process

Making App Volumes applications available to users is a two-step process:

- **Add an App Volumes application in the administration console.** There are two ways of doing this:
  - Add an App Volumes application by creating and importing a new app package.
    
    If an app package has not yet been created, you can create it with the **Create** option, which uses App Volumes to create the app package and automatically import it. See [Add an App Volumes Application by Creating a New App Package](#).
  
  - Add an App Volumes application by importing an existing app package.
    
    If you have an app package that was previously created with App Volumes, you can import it with the **Import** option. This means you can reuse app packages from on-premises deployments without having to repackage the applications. See [Add an App Volumes Application by Importing an Existing App Package](#).

- Create an App Volumes assignment to assign the App Volumes application to users. See [Create an App Volumes Assignment](#).
Prerequisites for App Volumes Applications

Before you can add App Volumes applications into your inventory, confirm that your environment meets the following prerequisites.

**Important** As described in *Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud*, the cloud-based console is dynamic and reflects the workflows and settings that are appropriate for the up-to-the-moment situation in your Horizon Cloud tenant environment. Access to features varies depending on factors such as the tenant’s regional cloud plane, whether your cloud-connected pods are running the latest level of the pod’s software, and whether features are based on specific licensing. The console dynamically reflects the elements related to such features only when your license or tenant account configuration includes use of such features. When you are expecting to see a feature in the console and do not see it, you have to contact your VMware account representative to verify whether your license and tenant account configuration entitles its usage.

- **New Customers:**
  - Starting on July 9, 2020, all new customers that purchase the Horizon Universal License subscription will have their tenant accounts enabled by default to use App Volumes for Horizon Cloud on Microsoft Azure pods.

- **Existing Customers:**
  - Customers with existing tenant accounts created after March 16, 2020 and before July 9, 2020 can use App Volumes for Horizon Cloud on Microsoft Azure pods after the version 3.1 (manifest version 2298.0) upgrade has been made available and those customers have upgraded all their pods to that version. To request App Volumes capability after successfully upgrading all pods, contact VMware Support as described in [https://kb.vmware.com/s/article/2006985](https://kb.vmware.com/s/article/2006985).
  - Customers with existing tenant accounts created on or before March 16, 2020 are not able to have App Volumes enabled for their Horizon Cloud on Microsoft Azure pods at this time. Those accounts must first be migrated to one of the regional Horizon Cloud control plane instances in Microsoft Azure. The VMware Horizon Service Team will notify such customers by email when this migration is available.

- You must have a pod deployed in Microsoft Azure that has manifest version 2298.0 or later, is configured with Unified Access Gateway instances, and you have completed the Active Directory domain registration workflow as described in *Chapter 2 Getting Started Using Your Horizon Cloud Environment*.

- If you have set the Domain Controller Policy **Domain controller: LDAP server signing requirements** to **Require Signing** after registering the domain using the Horizon Cloud Administration Console, you must do the following:
  a. On the **Settings > Active Directory** page, click the edit (pencil) icon next to **Domain Bind**.
  b. Enter the primary bind account password in the **Bind Password** text box. Do not make any other changes.
c Click Domain Bind.

- In the Horizon Cloud Administration Console, verify that every pod’s details page shows that the pod has its mounted file shares.

- In addition to meeting the Horizon Cloud Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release’s Manifest or Later, you must also open port 445 for TCP protocol traffic. Port 445 is the standard SMB port for accessing an SMB file share on Microsoft Windows. The AppStacks are stored in an SMB file share located in the pod’s resource group in your Microsoft Azure subscription.

- You have completed the Unified Access Gateway’s FQDN-mapping steps, as is required for pods in Microsoft Azure that are configured with Unified Access Gateway instances.

- You have confirmed that the following settings are shown on the pod detail page for your pod. You open the page by navigating to the Capacity page (Settings > Capacity) and clicking the pod:
  - The Fileshares field under Properties has a value of 2 and when you point to the number both fileshares are listed.
  - The Gateway settings at the bottom of the page are filled in, indicating that Unified Access Gateway is configured.

- Your inventory in the console has a published image with App Volumes Agent installed. For the high-level steps of creating an image VM, see Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure and its subtopics.

### Adding an App Volumes Application Using a Windows 10 Enterprise Multi-Session VM

**Note** Support for Windows 10 Enterprise multi-session VMs is a Tech Preview feature in this release.

The following are the required steps to create an App Volumes application with an app package from a Windows 10 Enterprise multi-session VM.

1. Manually build the VM in Microsoft Azure, including manually installing agents. See Tech Preview - How To Configure a Microsoft Windows 10 Multi-Session Image for Use with App Volumes Features in Horizon Cloud Pods in Microsoft Azure.

2. Add the necessary metadata to MSIX app attach VHD file using the App Volumes Packaging Utility, which is available on the VMware Flings page.

3. Add the App Volumes application using the New > Import process on the Applications page of the console. See Add an App Volumes Application by Importing an Existing App Package.
After you have added the application, you can create an App Volumes assignment as you normally do. See [Create an App Volumes Assignment](#).

**Important** If a service requiring administrative privileges is captured in a Windows 10 Enterprise multi-session app package, any user being assigned that app package must also have administrative privileges.

**Add an App Volumes Application by Creating a New App Package**

You can add an App Volumes application by creating a new app package using AppVolumes.

- After using the *Create* option for the first time, the same user should not attempt to use that option a second time until they have completed the steps to capture an app package in the capture desktop VM. If they try to use the *Create* option again before finishing the steps to capture an app package, a message displays stating that a request to create a package is already initiated. A different user in the same tenant, however, can initiate creating a package whether or not the first user has finished.

- The first time you click the *Create* option to initiate the capture process, the system can take up to 20 minutes before the capture desktop VM is ready and the status changes to *Desktop ready for application capture*. For this first time, this 20-minutes time is because the system is creating a desktop assignment and two desktop VMs to support the capturing process. After you have completed capturing your first app package, and then want to initiate a new capturing process, the time between when you click the *Create* option and the status changes to *Desktop ready for application capture* is shorter, around 10 minutes. The times after the first time are shorter because the system does not have to create the capture desktop assignment like it did for the first time. For the second time, the system deletes the previously used capture desktop VM and uses a new one.

**Prerequisites**

Confirm that your environment meets all the prerequisites listed in [App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites](#).

**Important** Before you begin the steps in this topic, you must have an available image with the App Volumes Agent installed. To create such an image you must:

- Import a VM with the App Volumes Agent installed. Follow the import steps in the [Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it with Horizon Cloud](#) topic and select the *App Volumes Agent* toggle under *Advanced Options*.

- Create an image from that imported VM. This is the image you use to create the new app package in the following steps.

**Procedure**

1. In the console, select **Inventory > Applications**.

   The *App Volumes* tab of the *Applications* page displays.
2 Click **New > Create**.

3 Under **Definition** in the **New Application Package** window, enter the values shown below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Select the <strong>New</strong> radio button and enter a unique name for the application. The name must start with a letter [a-Z] and contain only letters [a-Z], dashes [-], and numbers.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description for the application.</td>
</tr>
<tr>
<td>Package</td>
<td>Enter a unique name for the package.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description for the package.</td>
</tr>
</tbody>
</table>

4 Under **Desktop for Application Package** in the **New Application Package** window, enter the values shown below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Select a location to filter the set of pods displayed in the <strong>Pods</strong> drop-down menu.</td>
</tr>
<tr>
<td>Pod</td>
<td>Select a pod to filter the set of pods displayed in the <strong>Image</strong> drop-down menu. The <strong>Pod</strong> drop-down menu displays only pods that have App Volumes enabled, have at least one image with the App Volumes Agent installed, and have Unified Access Gateway enabled.</td>
</tr>
<tr>
<td>Image</td>
<td>Select an image from the <strong>Image</strong> drop-down menu. <strong>Note</strong> The menu displays only images with the App Volumes Agent installed. See Prerequisites above for more information on creating such an image.</td>
</tr>
</tbody>
</table>

5 Click **Save**.

The first time you initiate the capture process, the system takes up to 20 minutes before the capture desktop VM is ready to use for capturing an application. During these 20 minutes, the system is creating one or more capture-process VDI desktop assignments with two desktop VMs in each to be used for the capture desktop VMs. It can take the system up to 20 minutes to create those underlying assignments and VMs.

- The system creates one assignment per user per image per pod. For this reason, it might create one assignment or multiple assignments.
- There are two desktops in each assignment so that you can start a second capture quickly after the first has finished.
- These assignments are named according to the pattern `appcaptureXXX`, where `XXX` is a randomly generated number.
- If you are using Universal Broker, these assignments appear in **Assignments > VDI Desktops & Apps**. If you are using single-pod broker, they appear in **Assignments > RDSH Desktops & Apps**.
If you want to update the image that is used for the packaging process, you must delete these assignments before doing so.

If you are not planning to perform additional capture in the near future, you can delete these assignments so they are not in your environment for no reason. If you delete them, however, the next time you perform a capture the system will take up to 20 minutes to create new ones.

**Note** If a capture fails, you can check under Monitor > Notifications to see any errors that have been reported.

There is now an entry for the application package in the list on the Applications page. If you point to Status for this list entry, it indicates the status of the capture VM. When the status is Desktop ready for application capture, you can proceed with the steps to log into the capture desktop VM and start installing an application for your app package.

**Note** You must begin the following steps within 6 hours of the capture VM being ready for application capture, or the capture VM will no longer be usable for application capture. You must also finish the steps below within 6 hours of performing the first step. If you do not, the system gives a warning and then 30 minutes later cancels the capture process and shuts down the capture VM, changing the app package status to Error. You can retry by removing the app package that is in Error state and clicking New > Create again on the Applications page.

6. On the Application page, click the name of the application.

   The application detail page for the application displays.

7. Select the new application package and then click Start Capture.

   The Horizon HTML Access (Blast) login form opens in a new browser tab.

8. Log in using the same credentials you used to log into the administration console.

9. In the Horizon HTML Access client, launch the capture desktop VM.

   **Warning** The user name used to log in to the capture VM must have local administrator privileges, or the user will not see the Packaging in progress dialog box.

   A VMware App Volumes - Packaging in progress dialog box with the message Packaging... is displayed on the Windows 10 desktop.

   **Important** Do not close this dialog box. If necessary, move it out of the way until you are finished installing the application you want in the application package.
10 Install an application that you want to package in the application package.

**Note** It is a best practice to capture only one application per capture session. Install one application and then finish the capture process. When the application package for that application is visible on the administration console’s **Applications** page, then you can capture another application in a new package. See *Add a New App Package to an Existing App Volumes Application*.

11 Click **OK** in the **VMware App Volumes - Packaging in progress** dialog box. After you are finished installing the application, in the App Volumes – Packaging in progress window click **OK**. The next App Volumes – Packaging in progress window appears.

A **VMware App Volumes - Packaging in progress** dialog box with the message **Installation complete?** is displayed.

12 Click **Yes**.

A **VMware App Volumes - Finalize Package** dialog box displays.

13 Make any desired changes to the name and version, and optionally add a description.

14 Click **Finalize**.

A message displays prompting you to reboot the VM.

15 Click **OK** and let the VM reboot.

As the capture desktop VM is rebooting, your HTML Access client session displays a message that you have been disconnected.

16 After the capture desktop VM is back online, log in again to see the **Packaging successful!** message.

17 Log out of the capture desktop VM.

**Results**

On the application detail page, the new app package appears with status of **Application capture in progress**. The status changes to **Success** when the app package import is complete.

**Add an App Volumes Application by Importing an Existing App Package**

You can create an App Volumes application in Horizon Cloud by importing an app package you already have in your Microsoft Azure storage.

**Prerequisites**

- Confirm that your environment meets all the prerequisites listed in *App Volumes Applications for Horizon Cloud on Microsoft Azure - Overview and Prerequisites*.

- The JSON and VHD files for the app package you plan to import must be in the staging fileshare of your pod under `cloudvolumes/packages`. You can confirm the location of this
fileshare by navigating to the appropriate fileshare in Microsoft Azure Storage Explorer. To identify the staging fileshare for the pod, go to Settings > Capacity and click the name of the pod, then place your pointer on the value for File Share. The tool tip displayed includes the staging file share.

Procedure

1. In the console, select Inventory > Applications.
   The App Volumes tab of the Applications page displays.

2. Click New > Import.
   The Import Native Application dialog box displays.

3. Select a location and pod, and then click Save.

Results

- A message displays indicating that the application import has been initiated.
- When the import is complete, the new App Volumes application is displayed in the list on the Applications page. You might need to refresh the page to see the new application.
- In the Pod column, the pod you selected is displayed, indicating that the application is available for that pod. If you perform the import again for additional pods (after copying/transferring the VHD and JSON file to each pod from which you must import) the application becomes available for multiple pods. In this case, the column displays the number of pods for which the application is available. You can place your pointer on that number to see the names of the pods.

Add a New App Package to an Existing App Volumes Application

You can create an app package and add it to an existing App Volumes application.

Procedure

1. In the console, select Inventory > Applications.
   The App Volumes tab of the Applications page displays.

2. Click New > Create.

3. Under Definition in the New Application Package window, enter the values shown below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Select the Existing radio button and select the application from the drop-down menu.</td>
</tr>
<tr>
<td>Description</td>
<td>This is not editable when Existing is selected above.</td>
</tr>
<tr>
<td>Package</td>
<td>Enter a unique name for the package.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description for the package.</td>
</tr>
</tbody>
</table>
4 Under **Desktop for Application Package** in the **New Application Package** window, enter the values shown below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Select a location to filter the set of pods displayed in the <em>Pods</em> drop-down menu.</td>
</tr>
<tr>
<td>Pod</td>
<td>Select a pod to filter the set of pods displayed in the <em>Image</em> drop-down menu. The <em>Pod</em> drop-down menu displays only pods that have App Volumes enabled, have at least one image with the App Volumes Agent installed, and have Unified Access Gateway enabled.</td>
</tr>
<tr>
<td>Image</td>
<td>Select an image. The <em>Image</em> drop-down menu displays only images with the App Volumes Agent installed.</td>
</tr>
</tbody>
</table>

5 Click **Save**.

The first time you initiate the capture process, the system takes up to 20 minutes before the capture desktop VM is ready to use for capturing an application. During these 20 minutes, the system is creating a capture-process VDI desktop assignment and two desktop VMs to be used for the capture desktop VMs. It can take the system up to 20 minutes to create that underlying assignment and VMs.

- The system creates one assignment per user per image per pod. For this reason, it might create one assignment or multiple assignments.
- There are two desktops in each assignment so that you can start a second capture quickly after the first has finished.
- These assignments are named according to the pattern `appcaptureXXX`, where `XXX` is a randomly generated number.
- If you are using Universal Broker, these assignments appear in **Assignments > VDI Desktops & Apps**. If you are using single-pod broker, they appear in **Assignments > RDSH Desktops & Apps**.
- If you want to update the image that is used for the packaging process, you must delete these assignments before doing so.
- If you are not planning to perform additional capture in the near future, you can delete these assignments so they are not in your environment for no reason. If you delete them, however, the next time you perform a capture the system will take up to 20 minutes to create new ones.

**Note** If a capture fails, you can look under **Monitor > Notifications** to see any errors that have been reported.
There is now an entry for the application package in the list on the Applications page. If you point to Status for this list entry, it indicates the status of the capture VM. When the status is Desktop ready for application capture, you can proceed with the steps to log into the capture desktop VM and start installing an application for your app package.

**Note** You must begin the steps below within 6 hours of the capture VM being ready for application capture, or the capture VM will no longer be usable for application capture. You must also finish the steps below within 6 hours of performing the first step. If you do not, the system gives a warning and then 30 minutes later cancels the capture process and shuts down the capture VM, changing the app package status to Error. You can retry by removing the app package that is in Error state and clicking New > Create again on the Applications page.

6 On the Application page, click the name of the application.
   The application detail page for the application displays.

7 Select the new application package and then click **Start Capture**.
   The Horizon HTML Access (Blast) login form opens in a new browser tab.

8 Log in using the same credentials you used to log into the administration console.

9 In the Horizon HTML Access client, launch the capture desktop VM.

**Note** The user name used to log in to the capture VM must have local administrator privileges to avoid the User Access Control (UAC) prompt.

A **VMware App Volumes - Packaging in progress** dialog box with the message **Packaging...** is displayed on the Windows 10 desktop.

**Important** Do not close this dialog box. If necessary, move it out of the way until you are finished installing the application you want in the application package.

10 Install an application that you want to package in the application package.

**Note** It is a best practice to capture only one application per capture session. Install one application and then finish the capture process. When the application package for that application is visible on the administration console’s Applications page, then you can capture another application in a new package. See Add a New App Package to an Existing App Volumes Application.

11 Click **OK** in the **VMware App Volumes - Packaging in progress** dialog box. After you are finished installing the application, in the App Volumes – Packaging in progress window click OK. The next App Volumes – Packaging in progress window appears.

A **VMware App Volumes - Packaging in progress** dialog box with the message **Installation complete?** is displayed.
12 Click **Yes**.

A **VMware App Volumes - Finalize Package** dialog box displays.

13 Make any desired changes to the name and version, and optionally add a description.

14 Click **Finalize**.

A message displays prompting you to reboot the VM.

15 Click **OK** and let the VM reboot.

As the capture desktop VM is rebooting, your HTML Access client session displays a message that you have been disconnected.

16 After the capture desktop VM is back online, log in again to see the **Packaging successful!** message.

17 Log out of the capture desktop VM.

**Results**

On the application detail page, the new app package appears with status of **Application capture in progress**. The status changes to **Success** when the app package import is complete.

**Managing App Packages in an App Volumes Application**

You can add, remove, and make other changes to app packages on the application detail page for an App Volumes application.

To view the application detail page for an App Volumes application, go to the **App Volumes** tab of the **Applications** page, and click the application in the **Application** column.

The table below describes actions you can perform on the application detail page.
### Action

Add an app package to the application

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Click <strong>New</strong>. The <strong>Add Application Package</strong> dialog box displays. <strong>Application</strong> and <strong>Description</strong> are pre-populated with the information for the current application.</td>
</tr>
</tbody>
</table>
| 2 Under **Definition** in the **New Application Package** window, enter the values shown below.  
  - **Package** - Enter a unique name for the package.  
  - **Description** - (Optional) Enter a description for the package. |
| 3 Under **Desktop for Application Package** in the **New Application Package** window, enter the values shown below.  
  - **Location** - Select a location to filter the set of pods displayed in the **Pods** drop-down menu.  
  - **Pod** - Select a pod to filter the set of pods displayed in the **Image** drop-down menu. The drop-down menu displays only pods that have App Volumes enabled, have at least one image with the App Volumes Agent installed, and have Unified Access Gateway enabled.  
  - **Image** - Select an image. The drop-down menu displays only images with the App Volumes Agent installed. |
| 4 Click **Save**. The new app package is displayed in the list on the application detail page. |

### Change life cycle status for an app package

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you first create a package, the system sets the status to <strong>New</strong>, and when you have finished capturing an application for the package, the system changes the status to <strong>Packaged</strong>. From this point on, you can update the status to <strong>Tested</strong>, <strong>Published</strong>, or <strong>Retired</strong> to help you track your inventory of application packages.</td>
</tr>
<tr>
<td>Action</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>Capture an application for an app package.</td>
</tr>
<tr>
<td>1 Select the new application package and then click <strong>Start Capture</strong>.</td>
</tr>
<tr>
<td>2 Log in using the same credentials you used to log into the administration console.</td>
</tr>
<tr>
<td>3 In the Horizon HTML Access client, start the capture desktop VM.</td>
</tr>
<tr>
<td>4 Log into the Windows 10 operating system using the same credentials you used to log into the administration console.</td>
</tr>
<tr>
<td>5 Install an application that you want to package in the application package.</td>
</tr>
<tr>
<td>6 Click <strong>OK</strong> in the <strong>VMware App Volumes - Packaging in progress</strong> dialog box. After you are finished installing the application, in the App Volumes – Packaging in progress window click <strong>OK</strong>. The next App Volumes – Packaging in progress window appears.</td>
</tr>
<tr>
<td>7 Click <strong>Yes</strong>.</td>
</tr>
<tr>
<td>8 Make any desired changes to the name and version, and optionally add a description. The value shown for <strong>Name</strong> is what appears in the administration console’s <strong>Applications</strong> page.</td>
</tr>
<tr>
<td>9 Click <strong>Finalize</strong>.</td>
</tr>
<tr>
<td>10 Click <strong>OK</strong> and let the VM reboot.</td>
</tr>
<tr>
<td>Action</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>Add a marker to an app package</td>
</tr>
<tr>
<td>Edit the name and description for an app package</td>
</tr>
<tr>
<td>Remove an app package from the application</td>
</tr>
<tr>
<td>Update the image for an app package</td>
</tr>
</tbody>
</table>

Create an App Volumes Assignment

Prerequisites

Before creating an App Volumes assignment, you must first create a floating VDI desktop assignment. Due to the processing needs of Microsoft Windows 10 operating systems, this assignment must have a VMware-recommended desktop model that provides at least 2 vCPU and 4 GB RAM.

Procedure

1. In the console, click Assignments and select the option that includes App Volumes or VDI.
2. On the main assignments page, click New > App Volumes.
3. On the wizard’s Definition step, enter the values shown below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment Name</td>
<td>Enter a unique name for the new assignment.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description for the assignment.</td>
</tr>
<tr>
<td>OS Family</td>
<td>Select the operating system family from the drop-down menu. For example, Windows 10 (64-bit).</td>
</tr>
</tbody>
</table>

4. Click Next.
On the wizard’s Applications step, select the applications you want to provide to users.

- To filter applications displayed, click the filter icon in the header of the Applications column and enter a filter value.
- To display only applications you have selected, click Selected Applications to the top right of the list.

To select an application, first select the check box and then select an application package in the Package column. You can select a package either by a marker (such as Current) or the actual name of the package (such as Notepad++ v7.7.1).

Click Next.

On the Users step, search for users and groups in your registered Active Directory domains, select the ones you want to entitle to use applications from this assignment, and then click Next.

On the wizard’s Summary step, confirm that the information shown is correct and click Finish.

Results

The new assignment displays in the list on the Assignments page.

Known Limitations for App Volumes in Horizon Cloud

This topic describes known limitations for App Volumes functionality in Horizon Cloud.

- If you delete an App Volumes assignment on the Assignments page (Assignments > Desktops & Apps or Assignments > RDSH Desktops & Apps), you must delete any existing application packages that are still in the ‘New’ stage on the application detail page for the application before you can create a new application package using Inventory > Applications > New > Create.

- Application packages available in one pod are not automatically replicated to other pods. You must import them manually into other pods for them to be available in those pods. For instructions, see Add an App Volumes Application by Importing an Existing App Package.

- When using the Power Management feature in Horizon Cloud pods on Microsoft Azure, App Volumes must be used in High Availability (HA) mode only. Power management must be configured so that it powers on VMs in batches of up to 500 instead of all at once. Turning on more than 500 VMs at the same time can impact the communication between App Volumes agent and the App Volumes Manager service. There a Knowledge Base article to be published shortly on this topic.

Remote Applications - Importing from RDSH Farms that are Provisioned by Horizon Cloud Pods in Microsoft Azure

In Horizon Cloud, you make remote applications available for user assignments by importing them from an RDSH applications farm. You perform these steps using the administrative console’s Applications page. If you have multiple applications farms and the applications vary
from farm to farm, you would repeat these steps for each farm that has the set of applications you want to have in your inventory for assigning to end users.

You have two choices for identifying which remote applications you want the system to import into your inventory:

- **Auto-Scan from Farm** — The system scans the Windows operating system of the VM on which the application farm is based and identifies applications that it can automatically import. A list of those applications is displayed for your selection and confirmation.

- **Manually from Farm** — Even though the best practice is to use the automated way where the system scans the farm's VM's Windows operating system, the manual method can be useful for some unique situations, such as for adding applications that are invoked from the command prompt or which cannot be auto-detected in a Windows operating system. With this method, you identify one application at a time and must provide the precise path where the application resides.

**Tip**  When the console's Applications page displays a Remote tab, you perform the following steps on the Remote tab. The console is dynamic and reflects the workflows that are appropriate for the up-to-the-moment situation in your Horizon Cloud tenant environment. When your Horizon Cloud tenant is enabled to have App Volumes applications, the Applications page displays two tabs — **App Volumes** and **Remote**.

**Prerequisites**

Verify that you have at least one applications farm in your inventory by navigating to **Inventory > Farms**.

**Procedure**

1. Click **New** and then choose the method by which you want to identify to the system those applications to import.

   - **Auto-Scan from Farm**
   - **Manually from Farm**
Depending on the selected method, follow the on-screen prompts.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Scan from Farm</td>
<td>Selecting this method starts a wizard for this method.</td>
</tr>
<tr>
<td></td>
<td>a Select the location, pod, and applications farm and click Next to proceed to the next step.</td>
</tr>
<tr>
<td></td>
<td>b The system scans the selected farm for applications and then displays them for you to select. The system displays the applications that the system's auto-scan process found in the Windows operating system that is used in the farm's RDSH VMs.</td>
</tr>
<tr>
<td></td>
<td>c Select the applications that you want to add to your application inventory and click Next.</td>
</tr>
<tr>
<td></td>
<td>d Optionally customize some of the configurable options for the applications you selected, and then click Next.</td>
</tr>
<tr>
<td></td>
<td>e Review the summary and click Finish.</td>
</tr>
<tr>
<td>Manually from Farm</td>
<td>Selecting this method opens a window in which you specify the details to identify the application to import.</td>
</tr>
<tr>
<td></td>
<td>a Specify the following key properties.</td>
</tr>
<tr>
<td></td>
<td>- Name — Provide a name for the application by which it will be listed in your inventory. Providing a name helps you identify this application in the list of applications displayed in the console.</td>
</tr>
<tr>
<td></td>
<td>- Display Name — Name for the application that you want displayed to end users when they see and launch the application from their clients, such as in Horizon Client or Workspace ONE.</td>
</tr>
<tr>
<td></td>
<td>- Location — Select a location to filter the set of pods to display in the Pod drop-down list. Only pods that are associated with this selected location will appear in the following Pod list.</td>
</tr>
<tr>
<td></td>
<td>- Pod — Select a pod to filter the set of farms to display in the Farm list. Only this selected pod's provisioned farms will appear in the following Farm list.</td>
</tr>
<tr>
<td></td>
<td>- Farm — Select the farm that has the RDSH VM from which you want to add the application.</td>
</tr>
<tr>
<td></td>
<td>- Application Path — Specify the path to the application in the RDSH VM's operating system.</td>
</tr>
<tr>
<td></td>
<td>- Icon File — Optionally upload a PNG file (32 x 32 pixels) to use as the application's icon.</td>
</tr>
<tr>
<td></td>
<td>b In the Advanced Properties section, specify these optional settings.</td>
</tr>
<tr>
<td></td>
<td>- Application available on Farm — Select Yes to have the system validate the application path. If the application is not located in the farm's VM at that path, select No so that the system does not attempt to look for the application. For example, if an application is stored in the local directory in the VM, you would select No so that the system does not try to find the application there.</td>
</tr>
<tr>
<td></td>
<td>- Version — Version number of the application</td>
</tr>
<tr>
<td></td>
<td>- Publisher — Publisher of the application</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Start Folder</strong></td>
<td>Specify the location in the RDSH VM’s Windows operating system that you want the remote application to use as its start folder.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you specify a LNK file in the Application Path that specifies its own start directory, the system does not use the location specified here.</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>Specify any command line parameters you want used when the remote application is launched.</td>
</tr>
</tbody>
</table>

Click Submit.

Results

The system adds the specified applications to the application catalog in your inventory.

What to do next

Repeat the steps to import the applications you want from your other farms.

Remote Applications - Create a Remote Application Assignment for Remote Applications Provisioned By Horizon Cloud Pods in Microsoft Azure

In Horizon Cloud, to provide access for your end users to use a remote application that is provisioned from RDSH farms located in your pods in Microsoft Azure, you create a remote applications assignment. In this release, remote applications originate from applications farms that are provisioned by your pods in Microsoft Azure.

Prerequisites

Use the Applications page to verify that the remote applications you want to entitle to end users are available in your inventory. For an example, see Remote Applications - Importing from RDSH Farms that are Provisioned by Horizon Cloud Pods in Microsoft Azure.

Procedure

1. In the administrative console, click **Assignments** and navigate to the page for creating assignments of RDSH-based applications — also called remote applications — provisioned from your pods in Microsoft Azure.

   **Tip** The console is dynamic and reflects the workflows and settings that are appropriate for the up-to-the-moment situation in your Horizon Cloud tenant environment. The labels displayed for the console’s assignment-related pages will vary depending on factors such as the tenant’s configured brokering setting, the types of cloud-connected pods in your fleet, the tenant’s regional cloud plane, and features that are based on specific licensing.

2. On that page, click **New**.
3. From the New Assignment start screen, click the Applications icon.

4. On the wizard's Definition step, select the location and pod, provide a name for this assignment, and then click Next.

5. On the Applications step, select the remote applications and click Next.

   **Note** The displayed applications are all of the ones that were imported into your Horizon Cloud applications catalog from the farms in the same Horizon Cloud pod. You can have applications from different farms in the same pod within the assignment.

6. On the Users step, search for and select the users and groups for this assignment and click Next.

7. On the Summary step, review the information and then click Submit.

**Results**

The system creates the assignment and lists it on the Assignments page.
About Desktop Assignments for Your Horizon Cloud Environment's Pods in Microsoft Azure

In a Horizon Cloud environment, to provision VDI or remote desktops to your end users, you define what are known as desktop assignments. Each desktop assignment associates a published image with a set of entitled users. You use the Horizon Cloud Administration Console to create these desktop assignments.

A Horizon Cloud pod in a Microsoft Azure environment provides for the following types of desktop assignments.

**Session desktop assignment**

In a session desktop assignment, a Remote Desktop Services (RDS) desktop experience is shared across multiple users. These desktops are session-based connections to the RDSH-capable VMs running in a pod's RDSH farms. Before creating an RDSH session desktop assignment, you must have at least one desktops farm that was created based on the published image. See Create a Farm.

**Dedicated VDI desktop assignment**

In a dedicated VDI desktop assignment, each virtual desktop gets mapped to a specific user. Each mapped user returns to the same desktop at every login. When a particular dedicated VDI desktop is mapped to a specific user, that desktop is said to be assigned to that user. A specific dedicated VDI desktop gets mapped to a particular user in one of two ways:

- An administrator explicitly assigns that specific desktop to that particular user, using the Assign action.
- The user is entitled to the assignment (in the Users tab) and makes an initial launch of a desktop from the assignment. At that point, that user has claimed that dedicated VDI desktop from the set of all dedicated VDI desktops defined by that assignment. When the user has claimed a dedicated VDI desktop in this way, the system maps that particular desktop to that specific user and that dedicated VDI desktop gets the Assigned status. That particular dedicated VDI desktop remains in Assigned status until either an administrator explicitly unassigns the desktop (using the Unassign action) or that user's Active Directory account is removed from the assignment's set of entitled users.

Dedicated assignments require a one-to-one desktop-to-user relationship and should be sized based on the total user population. For example, you need an assignment of one hundred desktops for a group of one hundred users. The primary use for such dedicated desktop assignments is to ensure that the host name of the desktop virtual machine for each user remains the same between sessions. Certain software packages might require this use for licensing.

**Floating VDI desktop assignment**

In a floating VDI desktop assignment, a user receives a different virtual machine with a different machine name with each login. With floating desktop assignments, you can create
desktops that shifts of users can use and that should be sized based on the maximum number of concurrent users. For example, three hundred users can use an assignment of one hundred desktops if they work in shifts of one hundred users at a time. With floating desktop assignments, the user might see different host names for each desktop session.

When deciding between dedicated and floating VDI desktop assignments, the floating VDI desktop assignments are a best practice because they provide more flexible pool management capabilities than dedicated VDI desktop assignments and they avoid dedicating virtual machine resources for each user. As a result, floating VDI desktop assignments typically cost less than dedicated VDI desktop assignments.

To create a desktop assignment, you must have at least one image VM in the Published state that the system will use as the underlying configured operating system for the end users’ desktops.

**Note** Neither session-based desktops or floating VDI desktops provide persistence of user data, settings or profiles. When a user logs off from a floating VDI desktop, that floating VDI desktop is reset to the same state it was in before that user logged in. You can provide persistence of user data, settings, and profiles by setting up VMware Dynamic Environment Manager and configuring it for your environment. Images created using the automated Import Desktop wizard have the VMware Dynamic Environment Manager agent installed by default. For information on configuring persistence of those items, see these resources:

- The [VMware User Environment Manager Deployment Considerations](http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-user-environment-manager-deployment-considerations.pdf) document. VMware User Environment Manager™ was the previous name.
- The [Dynamic Environment Manager product documentation](#).

### About Creating These Desktop Assignments

The desktop assignment creation workflows are different depending on which type of broker is configured for your tenant environment. To see which broker type is configured in your environment, navigate to **Settings > Broker** in the console.

#### When your tenant environment is configured for Universal Broker

Follow the workflows described in [Pods in Microsoft Azure - Create a VDI Multi-Cloud Assignment](#).

#### When your tenant environment is configured for single-pod broker

Follow the workflows described in [Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure](#) and [Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure](#).

### Create an RDSH Session Desktop Assignment

You create session desktop assignments using the administrative console’s Assignments area.
For general information about desktop assignments, see About Desktop Assignments for Your Horizon Cloud Environment's Pods in Microsoft Azure.

**Prerequisites**

Verify you have the following items:

- In some deployments, you might see a message displayed on the console's assignment-related pages that states you must set up the broker configuration before you can create assignments involving your pods. If you see that message, follow the on-screen guidance.

- The Farms page lists at least one farm of remote desktops type and that farm is based on the published image that you want to use for the session desktops. Only farms configured to deliver remote desktops can be used for a session desktop assignment.

- The farm is not already used in an assignment. A farm configured to deliver remote desktops cannot be used in more than one session desktop assignment. To verify whether the farm you want to use is already used in a session desktop assignment, on the console page where your session-based desktop assignments are listed, examine the Farms column. If the farm you want to use is listed, then it is already being used in a session desktop assignment and you will have to create a new farm.

**Procedure**

1. Navigate to the assignments-related console page where you see that RDSH desktop assignments are created and start the workflow by clicking **New**.

   **Tip** The console is dynamic and reflects the workflows and settings that are appropriate for the up-to-the-moment situation in your Horizon Cloud tenant environment. The labels displayed for the console's assignment-related pages will vary depending on factors such as the tenant's configured brokering setting, the types of cloud-connected pods in your fleet, the tenant's regional cloud plane, and features that are based on specific licensing.

2. In the displayed screen, click the Desktops icon.

   The New Desktop Assignment window opens to the first wizard step.

3. On the wizard's Definition step, select the **Session** type.
4 Complete the selections on the Definition step and then click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Select the location of the pod from which you want the session desktops to be provided.</td>
</tr>
<tr>
<td>Pod</td>
<td>Select the pod.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>If you do not see any pods to select, verify that the Location list is not displaying a location without pods. The Location field works on the Pod list to filter out pods that are not associated with the selected location. If you previously had a pod at a location and then deleted that pod or moved it to a different location, so that the displayed location no longer has any pods, the Pod list will display no entries. Because the locations are listed alphabetically, when the screen opens, it automatically selects the one that is first in the alphabet. If that location no longer has any pods associated with it, you must switch the location to a different entry.</td>
</tr>
<tr>
<td>Farm</td>
<td>Select the farm that has the configured RDS-enabled image that you want to assign to the end users. Only farms that are in the selected pod and which not already involved in existing session desktop assignments are available for selection.</td>
</tr>
<tr>
<td>Assignment Name</td>
<td>Type a friendly name for this assignment. The end users see this name when they go to access their assigned desktop. For example, when an end user launches Horizon Client to go to an assigned desktop, this name is the one displayed in Horizon Client. The name must contain only letters, hyphens, and numbers. Spaces are not allowed. The name cannot start with a non-alphabetic character.</td>
</tr>
</tbody>
</table>

5 On the Users step, search for users and groups in your registered Active Directory domains, select the ones you want to give this session desktop assignment, and then click Next.

6 On the Summary step, review the configuration and then click Submit.

Results

The system begins the process of configuring the farm's VMs to provide session desktops to the selected users. On the page that lists the assignments, the Status column reflects the current progress.

Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure

In Horizon Cloud, you create desktop assignments to provision virtual desktops to your end users. You create floating VDI desktop assignments using the Assignments area of the Horizon Cloud Administration Console. When your Horizon Cloud tenant is configured to use the single-
pod type of brokering with your pods in Microsoft Azure, you follow the steps here to create a desktop assignment that brokers the virtual desktop from a single pod.

**Note** When your tenant is configured to use the Universal Broker with your pods in Microsoft Azure, instead of following these steps here, you would configure what is called a multi-cloud assignment, which can provision resources from multiple pods within the same assignment. See Chapter 6 Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment.

For general information about desktop assignments, see About Desktop Assignments for Your Horizon Cloud Environment's Pods in Microsoft Azure.

Use these steps to assign a floating VDI desktop to your end users. To assign another type of desktop, see the subtopics listed in About Desktop Assignments for Your Horizon Cloud Environment's Pods in Microsoft Azure.

**Prerequisites**

- In some deployments, you might see a message displayed on the console's assignment-related pages that states you must set up the broker configuration before you can create assignments involving your pods. If you see that message, follow the on-screen guidance.

- Verify that you have at least one published image, with a Microsoft Windows client operating system. You cannot create a VDI desktop assignment without such an image. To verify, navigate to the Images page and make sure it lists an appropriate image. For steps on creating a published image, see Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

- Decide whether you want the desktops to have encrypted disks. You must specify disk encryption when creating the VDI desktop assignment. You cannot later add disk encryption after the assignment is created. For a description of the disk capability, see Using Microsoft Azure Disk Encryption with Your Farms and VDI Desktops in Your Horizon Cloud Environment.

**Important** This release does not support having disk encryption for floating VDI assignments that use image VMs with attached data disks. Make sure the image you plan to use in the assignment does not have data disks.

- Decide whether you want the ability to use NSX Cloud features with the desktop VMs. You must enable NSX Cloud management when creating the VDI desktop assignment. You cannot later enable the assignment for NSX Cloud management after the assignment is created. The published image you choose for this assignment must have the NSX agent installed in it. You must have installed the NSX agent prior to publishing the image. See VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure and its subtopics.

**Important** To use both NSX Cloud features and disk encryption, ensure the image's installed NSX agent is the latest agent version. Using disk encryption with previous versions of the NSX agent is not supported.
- Decide whether you want this assignment’s desktop VMs to be connected to a VM subnet that is different from the pod’s primary VM subnet (also known as the tenant subnet). If your pod is running manifest 2298 or later and you have edited the pod to add additional VM subnets, you can specify use of those subnets for this desktop assignment. For this use case, you must verify that the VM subnet you want to use is listed on the pod’s details page’s Networking section in a Ready state so that the subnet will be available for you to select in the workflow steps. For details, see Overview of Using Multiple Tenant Subnets with Your Horizon Cloud Pod for Your Farms and VDI Desktop Assignments.

Procedure

1. Navigate to the assignments-related console pages, locate the one on which VDI desktop assignments are created and start the new assignment workflow.

   **Tip** The console is dynamic and reflects the workflows and settings that are appropriate for the up-to-the-moment situation in your Horizon Cloud tenant environment. The labels displayed for the console’s assignment-related pages will vary depending on factors such as the tenant’s configured brokering setting, the types of cloud-connected pods in your fleet, the tenant’s regional cloud plane, and features that are based on specific licensing.

2. In the New Assignment start screen, click the Desktops icon.

   ![Desktops](image)

   The New Desktop Assignment window opens to the first wizard step.

3. Select **Floating**.
4 Complete the selections on the Definition step and then click **Next**.

**Note** You might have to use the scroll bar to see everything.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Select the location of the pod from which you want the desktops to be provided.</td>
</tr>
<tr>
<td>Pod</td>
<td>Select the pod.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>If you do not see any pods to select, verify that the <strong>Location</strong> list is not displaying a location without pods. The <strong>Location</strong> field works on the <strong>Pod</strong> list to filter out pods that are not associated with the selected location. If you previously had a pod at a location and then deleted that pod or moved it to a different location, so that the displayed location no longer has any pods, the <strong>Pod</strong> list will display no entries. Because the locations are listed alphabetically, when the screen opens, it automatically selects the one that is first in the alphabet. If that location no longer has any pods associated with it, you must switch the location to a different entry.</td>
</tr>
<tr>
<td>Specify VM Subnet(s)</td>
<td>Enable this toggle to select one or more specific subnets to which the assignment's desktop VMs will be connected. After enabling the toggle, you can select the specific subnets from the displayed list. When this toggle is disabled, the desktop VMs will be connected to the pod's primary VM subnet by default.</td>
</tr>
</tbody>
</table>
### Option | Description
--- | ---
**Filter Models** | Set one or more filters to control the models available in the **Models** drop-down menu. You can filter models by type, series, number of CPUs, memory, and tags. For more information about selecting models, see *Managing VM Types and Sizes for Farms and Assignments*, which describes the options on the VM Types & Sizes page (*Settings > VM Types & Sizes*).

To set a filter, you first select the criterion in the drop-down menu and then enter the desired values. By default, there is a single filter with the criterion ‘Tag’ the value ‘VMware Recommended’. You can edit this first filter and add more filters connected by And and Or operators.

The following are the criteria you can use for filters and descriptions of the values you can enter for each.

**Type**

When you select this option, the second drop-down menu defaults to **GPU and High Performance - Models with GPU**.

**Note** If you choose a GPU model (for example, Standard_NV6), then the list of images shown will contain only images that were created with the Include GPU flag selected, so you need at least one such image in order to create a farm or pool using a GPU model. If you choose a non-GPU model, then the list of images shown will contain only images that were created without the Include GPU flag.

**Series**

When you select this option, you can then select a series of models from a second drop-down menu. You can also filter this list by entering text in the **Filter** text box at the top of the list.

**CPUs**

When you select this option, you can then enter a CPU range.

**Important** For production environments, to avoid unexpected end-user connection issues, use VM models that have a minimum of two (2) CPUs.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>When you select this option, you can then enter a range of memory in GBs.</td>
</tr>
</tbody>
</table>
| Tag    | When you select this option, you can then select a tag from a second drop-down menu. You can also filter this list by entering text in the Filter text box at the top of the list. Tags available in the drop-down menu are both hard-coded system tags and custom tags that you created on the VM Types & Sizes page (Settings > VM Types & Sizes). You can set additional filters by performing the following steps for each filter:  
  a. Click the Add link.  
  b. Select either And or Or as the operator between the previous filter and the new one you are creating.  
  c. Set the new filter by selecting a criterion and entering values. |
| Model  | Select the model to use for the desktop instances. This selection defines the set of underlying resources that will be used when the desktop instances are created, in terms of capacity (compute, storage, and so on). The available choices map to standard VM sizes that are available in Microsoft Azure. **Important** For production environments, select a VM model that has a minimum of two (2) CPUs. VMware scale testing has shown that using 2 CPUs or more avoids unexpected end-user connection issues. Even though the system does not prevent you from choosing a VM model with a single CPU, you should use such models for tests or proof-of-concepts only. |
| Disk Type | Select a supported disk type from the available options. Disk type options are based on the model selected, and your Azure subscription and region. The following are some commonly available disk types.  
  - Standard HDD - Default disk type.  
  - Standard SSD  
  - Premium SSD - Option only appears if you selected a model that supports premium IO.  
You can edit your selection after creating the assignment if desired. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disk Size</strong></td>
<td>Enter the OS disk size in GB for the VMs in this assignment.</td>
</tr>
<tr>
<td></td>
<td>- The default value is the base image OS disk size (typically 128 GB).</td>
</tr>
<tr>
<td></td>
<td>- If you edit the size, the value you enter must be greater than the base image OS disk size, and cannot exceed the largest size (typically 1024 GB) supported by the selected model.</td>
</tr>
<tr>
<td></td>
<td>- You can also edit this value later if desired.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>If you edit the disk size, there are additional actions you must take to ensure that the VMs are created as expected. For more information, see <a href="#">Required Administrator Actions When the Disk Size for a Farm or VDI Desktop Assignment is Increased</a>.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Select the Active Directory domain registered with your environment.</td>
</tr>
<tr>
<td><strong>Join Domain</strong></td>
<td>Select <strong>Yes</strong> so that the desktop instances are automatically joined the domain when they are created.</td>
</tr>
<tr>
<td><strong>Encrypt Disks</strong></td>
<td>Select <strong>Yes</strong> so that the desktop instances have encrypted disks.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>- If you want disk encryption, you must make this selection when creating the VDI desktop assignment. You cannot later add disk encryption after the assignment is created.</td>
</tr>
<tr>
<td></td>
<td>- To use both NSX Cloud features and disk encryption, the image's installed NSX agent must be the latest agent version. Using disk encryption with previous versions of the NSX agent is not supported.</td>
</tr>
<tr>
<td><strong>NSX Cloud Managed</strong></td>
<td>Select <strong>Yes</strong> so that you can use features of NSX Cloud with the assignment's desktop instances. For a description of using NSX Cloud features with your desktops in Microsoft Azure, see <a href="#">VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure</a> and its subtopics.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>- If you want to use NSX Cloud with the desktop instances, you must make this selection when creating the VDI desktop assignment. You cannot later enable NSX Cloud management after the assignment is created.</td>
</tr>
<tr>
<td></td>
<td>- For the NSX Cloud management features to work with the assignment's desktop instances, the image that you select for this assignment must have the NSX agent already installed on it. When you set this toggle to <strong>Yes</strong>, ensure that the image you select in <strong>Image</strong> has the NSX agent installed on it. The system does not verify if the selected image has the NSX agent when it creates the VDI desktop assignment.</td>
</tr>
<tr>
<td></td>
<td>- To use both NSX Cloud features and disk encryption, the image's installed NSX agent must be the latest agent version. Using disk encryption with previous versions of the NSX agent is not supported.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Image</strong></td>
<td>Select an image that you want to assign to the end users. Only those published images in the selected pod that are appropriate for VDI desktops are listed here. A published image, sometimes called a sealed image or an assignable image, is one that was published to the system by converting a base or golden image into a desktop.</td>
</tr>
</tbody>
</table>
| **Important**   | - If you set the Encrypt Disks to Yes, ensure that the image you select here does not have data disks attached to it. Use of disk encryption of VMs with data disks for floating VDI assignments is not supported in this release.  
- If you set the NSX Cloud Managed toggle to Yes, ensure that the image you select here has the NSX agent installed on it. For the NSX Cloud management features to work with the assignment’s desktop instances, the image that you select for this assignment must have the NSX agent already installed on it. The system does not verify if the selected image has the NSX agent when it creates the VDI desktop assignment.                                                                                                                                                                                                                                                                 |
<p>| <strong>Assignment Name</strong> | Type a friendly name for this floating VDI desktop assignment. Entitled end users might see a form of this assignment name in the client they use to access their desktops. The name must contain only letters, hyphens, and numbers. Spaces are not allowed. The name cannot start with a non-alphabetic character.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <strong>VM Names</strong>    | Base name for the desktop VMs created in this assignment. The VM names will have numbers appended to this base name, for example, win10-1, win10-2, etc. The name must start with a letter and can contain only letters, dashes, and numbers. The end users see this name when they go to access a desktop from this assignment. For example, when an end user launches Horizon Client to use one of the desktops, this name is the one displayed in Horizon Client.                                                                                                                                                                                                                                                                                                                                                     |
| <strong>Default Protocol</strong> | Select a default display protocol you want the end-user sessions to use. Circumstances might occur that cause another protocol to be used instead of the default protocol. For example, the client device does not support the default protocol or the end user overrides the default protocol selection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <strong>Note</strong>        | For images with the Microsoft Windows 7 Enterprise operating system, RDP is the only supported choice.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <strong>Preferred Client Type</strong> | Select the preferred client type used when end users launch their desktops from Workspace™ ONE™ Access, either a Horizon Client or a browser for HTML Access.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <strong>Note</strong>        | For images with the Microsoft Windows 7 Enterprise operating system, Horizon Client is the only supported choice.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min Desktops</td>
<td>Specify the minimum number and maximum number of desktops you want in this floating VDI desktop assignment. When the assignment is first created, the system deploys the number of desktops specified in the Max Desktops field, and then powers off the desktops except the number specified for Min Desktops. Only the minimum number of desktop instances is initially powered on. As end-user demand increases, the system powers on additional desktops, up to the Max Desktops number. Then as end-user demand shrinks, the system powers off the desktops, until it reaches the Min Desktops number. A desktop must be free of a logged-in user session before the system will power it off. When you specify zero (0) for Min Desktops, it indicates that you want the system to power off all the assignment's desktops until there is end-user demand for a desktop.</td>
</tr>
<tr>
<td>Max Desktops</td>
<td></td>
</tr>
<tr>
<td>Power Off Protect Time</td>
<td>Specify the number of minutes that you want the system to wait before automatically powering off a powered-on desktop. You can enter a value from 1 to 60. The default is 30 minutes. This protect time is used primarily for the situations where the system will automatically power off a desktop VM. You can use this Power Off Protect Time setting to tell the system to wait the specified time before starting to power off the VM to meet the threshold setting in the Power Management field. The system waits the time specified for the Power Off Protect Time before powering off the VM to match the configured schedule. The default wait time is 30 minutes.</td>
</tr>
<tr>
<td>Windows license question</td>
<td>The wizard asks you to confirm you have an eligible license to use the Microsoft Windows operating system that is in the image and which will be in the desktop VMs. Follow the on-screen instructions. For a client operating system, Horizon Cloud sets the VDI assignment's desktop VMs to use the Windows Client license type by default and you cannot change that setting.</td>
</tr>
</tbody>
</table>
Optionally configure the advanced properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer OU</td>
<td>Active Directory Organizational Unit where the desktop VMs are to be located. Enter the Active Directory Organizational Unit using the distinguished name, for example, <code>OU=RootOrgName,DC=DomainComponent,DC=eng</code>, and so on. The OU and each path in a nested OU can contain any combination of letters, numbers, special characters, and spaces, and can have a maximum of 64 characters. If you need to use nested Organization Units, see <a href="#">Considerations For Using Nested Active Directory Domain Organizational Units</a>. <strong>Note</strong> If the Computer OU is set to <code>CN=Computers</code>, the system uses the default Active Directory Computers container for VMs. Your Active Directory might have this default container redirected to an organizational unit class container.</td>
</tr>
<tr>
<td>Run Once Script</td>
<td>(Optional) Location of a script that you want run in the assignment’s desktop VMs after the VM creation process. <strong>Note</strong> The script must end with a reboot step to reboot the VM. Otherwise, the end user will not be able to log in the desktop until doing a manual restart. A sample reboot line as a Windows command is: <code>shutdown /r /t 0</code>. The reason why the script must end with a reboot step is due to the sequence when the script is run after the sysprep process. When the system creates a desktop VM for the assignment, the VM boots up and completes the sysprep process in the Windows operating system. When the sysprep process completes, the agent in the desktop VM reaches out to do the domain join. At the same time, the agent gets the script path you specify here. The agent sets the Windows RunOnce path (System run once) and then restarts the desktop VM. On the next restart, the system logs in to the Windows operating system using the local administrator account and runs the script. It is only after another subsequent restart, specified in the script, that the desktop VM is ready for a user to log in.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Session Timeout Interval</td>
<td>This time interval is the amount of time the end users’ sessions can be idle before the system forces a log off from the desktops. This time out applies to the logged-in session to the underlying Windows operating system. The time you specify here is different from the time out settings that govern the end users’ Horizon Client or HTML Access logged-in session.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong>   When the system forces the log off in the underlying Windows operating system session, any unsaved data is lost. To prevent an unintended loss of data, set this interval high enough to accommodate the business needs of your end users.</td>
</tr>
<tr>
<td></td>
<td>The default interval is one week (10080 minutes).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>      If no user activity occurs before the timeout interval is reached, a message appears in the desktop that indicates that the user will be logged off if they do not click OK in the next 30 seconds. If the logout occurs, any unsaved user data, such as documents or files, is lost.</td>
</tr>
<tr>
<td>Azure Resource Tags</td>
<td>(Optional) Create custom tags to be applied to Azure resource groups. Azure resource tags are only applied to the resource groups, and are not inherited by the resources in the groups.</td>
</tr>
<tr>
<td></td>
<td>To create the first tag, enter information in the Name and Value fields. To create an additional tag, click Add and then enter information in the Name and Value fields that appear below the existing ones.</td>
</tr>
<tr>
<td></td>
<td>▪ You can create a maximum of 10 tags.</td>
</tr>
<tr>
<td></td>
<td>▪ The tag name is limited to 512 characters, and the tag value is limited to 256 characters. For storage accounts, the tag name is limited to 128 characters, and the tag value is limited to 256 characters.</td>
</tr>
<tr>
<td></td>
<td>▪ Tag names cannot contain the following characters:</td>
</tr>
<tr>
<td></td>
<td><code>&lt; &gt; % &amp; \ ? /</code></td>
</tr>
<tr>
<td></td>
<td>▪ Tag names cannot contain these case-insensitive strings:</td>
</tr>
<tr>
<td></td>
<td>‘azure’, ‘windows’, ‘microsoft’</td>
</tr>
<tr>
<td></td>
<td>After an assignment has been created, you can add more Azure resource tags and edit or delete tags for that assignment.</td>
</tr>
</tbody>
</table>
5 In the wizard's Management step, complete the fields and make your selections as appropriate and then click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Image Updates</strong></td>
<td>The Concurrent Quiescing Desktops setting controls the number of desktops in this floating VDI desktop assignment that can be concurrently quiesced during the time the assignment's image is being updated. For example, when you later edit this floating VDI desktop assignment to use another image, the system will power off at the same time this number of desktops. Then the system performs the required actions to provision the new image to that set of powered-off desktops. Typically this number is a subset of the full maximum number of desktops defined for this assignment. However, you can specify a number here equal to the Max Desktops setting. In that scenario, you would be allowing the system to power off all of the assignment's desktops at the same time when you edit the assignment to use a new image.</td>
</tr>
</tbody>
</table>
| **Power Management**| These power management settings are related to the thresholds at which the system automatically increases and shrinks the number of powered-on desktop instances in the floating VDI desktop assignment according to usage. When the usage increases above an upper bound, the system automatically powers up a new desktop instance. When the usage shrinks below a lower bound, the system shuts down deallocates desktop VMs as end users log off from the desktops. The power management selections balance capacity cost with faster availability:  
- Select **Optimized Performance** when you want the system to power on the next desktop instance sooner rather than later. Even though you are spending more by having the next desktop ready to go before the user demand requires it, this setting increases the chance that when users try to launch a desktop from the assignment, the desktop is already powered up to meet that demand. 
- Select **Optimized Power**, when you want the system to wait as long as possible before powering on the next desktop instance. The occupancy of the assignment's set of desktops is higher before the system powers up the next desktop instance. Even though this selection minimizes capacity costs by having more utilization of the existing desktops, this setting increases the chance that there might be a delay when new users try to log in because they might have to wait during the time system has to power on desktops. 
- Select **Balanced** to strike a balance between capacity costs and time-to-availability for users. 

The low and high thresholds for each selection are:  
- **Optimized Performance**  
  - Low threshold: 23%  
  - High threshold: 50%  
- **Optimized Power**  
  - Low threshold: 38%  
  - High threshold: 80%  
- **Balanced**  
  - Low threshold: 31%  
  - High threshold: 66% |
<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timeout Handling</strong></td>
<td>Configure how you want the system to handle the desktops’ user sessions.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The user sessions governed by these settings are the user logins to the desktops’ Windows operating system. These sessions are not the user logins in Horizon Client, Horizon HTML Access, or Workspace ONE.</td>
</tr>
<tr>
<td></td>
<td>The user's session begins when the user authenticates to the desktop's Windows operating system.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Log Off Disconnected Sessions</strong> - Select when the system will log the user off of a disconnected session.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Max Session Lifetime</strong> - Specify the maximum number of minutes the system should allow for a single user session.</td>
</tr>
<tr>
<td><strong>Schedule Power Management</strong></td>
<td>To help optimize savings and performance of the desktop VMs in Microsoft Azure, you can optionally configure schedules to adjust the minimum number of powered-on desktop instances on a recurring weekly basis. For example:</td>
</tr>
<tr>
<td></td>
<td>- For weekends or night hours when you know that your end users will not be using their desktops, you can have a schedule for zero or a low number of powered-on desktops.</td>
</tr>
<tr>
<td></td>
<td>- For specific days or specific hourly stretches that you can predict will have increased end user demand, you can have a schedule that increases the minimum number of powered-on desktops to be available to meet that demand.</td>
</tr>
<tr>
<td></td>
<td>You can specify up to 10 schedules for the floating VDI desktop assignment. If any schedules have overlapping time periods but specify different minimum desktop numbers, the system uses the largest value of minimum desktops for the overlapping time period.</td>
</tr>
<tr>
<td></td>
<td>a Click the + icon to add the first row in the Schedule Power Management section.</td>
</tr>
<tr>
<td></td>
<td>b Type an identifying name for the first schedule.</td>
</tr>
<tr>
<td></td>
<td>c Select the days for the first schedule.</td>
</tr>
<tr>
<td></td>
<td>d Specify the applicable hours in the specified days. Either:</td>
</tr>
<tr>
<td></td>
<td>- Select the <strong>All Day</strong> check box to have this schedule in effect for all hours of the specified days.</td>
</tr>
<tr>
<td></td>
<td>- Specify start and end times for the time period in each day.</td>
</tr>
</tbody>
</table>

**Note** One day is automatically selected by default when the row is added. If you do not want to include the selected day in this schedule, click the drop-down and deselect that selected day.

**Note** Encrypted VMs take longer to power on than non-encrypted VMs. If you have set **Encrypt Disks** to **Yes**, and you want 100% of the encrypted VMs to be ready for end-user connections at a particular time of day, you might have to set an earlier start time here. See **When Scheduling Power Management for Farms and VDI Desktop Assignments That Have Large Numbers of Encrypted VMs**.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>Select the time zone. The time zone closest to your end users' location is recommended. As appropriate for the selected time zone, Daylight Savings Time is automatically applied.</td>
</tr>
<tr>
<td>Note</td>
<td>If two schedules have the same time zone setting and have overlapping times, a warning is displayed. However, if two schedules have different time zone settings and overlap, the warning is not displayed. As an example, if you have two all-day Saturday schedules and one has Europe/London time zone selected and the other has America/Toronto selected, the overlap warning does not display.</td>
</tr>
<tr>
<td>f</td>
<td>In the Min Desktops field, type the minimum number of desktops you want powered on during the specified time period. During the specified time period, that number of desktops at a minimum will be powered on to be available to take end user requests during that time. The number can range from zero (0) up to the number specified for Max Desktops for the overall floating VDI desktop assignment. When this number is zero (0) and there are no active end user sessions at the schedule's starting time point, the assignment's desktops are powered off. In that scenario, if an end user subsequently attempts to connect to a desktop from this assignment during the scheduled time period, there will be a delay before the desktop is in a usable state because the underlying desktop VM has to power on.</td>
</tr>
<tr>
<td>Note</td>
<td>By default, when a user logs off of a desktop at a time that lies outside of a schedule's time period, the system protects the desktop VM from powering off for the time specified in the Power Off Protect Time field. The default is 30 minutes.</td>
</tr>
</tbody>
</table>

6 On the Users step, search for users and groups in your registered Active Directory domains, select the ones you want to entitle to use desktops from this assignment, and then click Next.

7 On the Summary step, review the configuration and then click Submit.

Results

The system begins the process of configuring the desktop instances to provide VDI desktops to the selected users. On the Assignments page, the Status column reflects the current progress.

Note Creation of an encrypted desktop VM takes approximately twice as long as creating a non-encrypted VM. As a result, the end-to-end time to complete creating a VDI desktop assignment that has disk encryption enabled is approximately twice as long as creating that VDI desktop assignment without disk encryption enabled.

What to do next

If the image for this floating VDI desktop assignment has applications that require opening special ports, you might need to modify this assignment’s associated Network Security Group (NSG) in Microsoft Azure. For details about the NSG, see About Network Security Groups and Your VDI Desktops.
If you specified NSX Cloud management for this assignment, you can use your NSX Cloud environment's Service Manager (CSM) to see that the desktop VMs are managed in NSX Cloud. Log in to your environment's CSM and navigate to Clouds > Azure > Instances. When that Instances page shows a status of Managed for the desktop instances, you can start implementing NSX policies on them.

Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure

In Horizon Cloud, you create desktop assignments to provision virtual desktops to your end users. You create dedicated VDI desktop assignments using the Assignments area of the Horizon Cloud Administration Console. When your Horizon Cloud tenant is configured to use the single-pod type of brokering with your pods in Microsoft Azure, you follow the steps here to create a desktop assignment that brokers the virtual desktop from a single pod.

**Note** When your tenant is configured to use the Universal Broker with your pods in Microsoft Azure, instead of following these steps here, you would configure what is called a multi-cloud assignment, which can provision resources from multiple pods within the same assignment. See Chapter 6 Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment.

For general information about desktop assignments in your tenant environment, see About Desktop Assignments for Your Horizon Cloud Environment's Pods in Microsoft Azure.

**Prerequisites**

- In some deployments, you might see a message displayed on the console's assignment-related pages that states you must set up the broker configuration before you can create assignments involving your pods. If you see that message, follow the on-screen guidance.

- Verify that you have at least one published image, with a Microsoft Windows client operating system. You cannot create the VDI desktop assignment without such an image. To verify, navigate to the Images page and make sure it lists an appropriate image. For steps on creating a published image, see Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

- Decide whether you want the desktops to have encrypted disks. You must specify disk encryption when creating the VDI desktop assignment. You cannot later add disk encryption after the assignment is created. For a description of the disk capability, see Using Microsoft Azure Disk Encryption with Your Farms and VDI Desktops in Your Horizon Cloud Environment.

  **Important** This release does not support having disk encryption for floating VDI assignments that use image VMs with attached data disks. Make sure the image you plan to use in the assignment does not have data disks.

- Decide whether you want the ability to use NSX Cloud features with the desktop VMs. You must enable NSX Cloud management when creating the VDI desktop assignment. You cannot
later enable the assignment for NSX Cloud management after the assignment is created. The published image you select for this assignment must have the NSX agent installed in it. You must have installed the NSX agent before publishing the image. See VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure and its subtopics.

- Decide whether you want this assignment's desktop VMs to be connected a VM subnet that is different from the pod's primary VM subnet (also known as the tenant subnet). If your pod is running manifest 2298 or later and you have edited the pod to add additional VM subnets, you can specify use of those subnets for this desktop assignment. For this use case, you must verify that the VM subnet you want to use is listed on the pod’s details page’s Networking section in a Ready state so that the subnet will available for you to select in the workflow steps. For details, see Overview of Using Multiple Tenant Subnets with Your Horizon Cloud Pod for Your Farms and VDI Desktop Assignments.

Procedure

1. Navigate to the assignments-related console pages, locate the one on which VDI desktop assignments are created and start the new assignment workflow.

   **Tip** The console is dynamic and reflects the workflows and settings that are appropriate for the up-to-the-moment situation in your Horizon Cloud tenant environment. The labels displayed for the console’s assignment-related pages will vary depending on factors such as the tenant’s configured brokering setting, the types of cloud-connected pods in your fleet, the tenant’s regional cloud plane, and features that are based on specific licensing.

2. In the New Assignment start screen, click the Desktops icon.

   ![Desktops](image)

   The New Desktop Assignment window opens to the first wizard step.

3. Select **Dedicated**.
4 Complete the selections on the Definition step and then click **Next**.

**Note** You might have to use the scroll bar to see all the required fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location</strong></td>
<td>Select the location of the pod from which you want the desktops to be provided.</td>
</tr>
<tr>
<td><strong>Pod</strong></td>
<td>Select the pod.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>If you do not see any pods to select, verify that the <strong>Location</strong> list is not displaying a location without pods. The <strong>Location</strong> field works on the <strong>Pod</strong> list to filter out pods that are not associated with the selected location. If you previously had a pod at a location and then deleted that pod or moved it to a different location, so that the displayed location no longer has any pods, the <strong>Pod</strong> list will display no entries. Because the locations are listed alphabetically, when the screen opens, it automatically selects the one that is first in the alphabet. If that location no longer has any pods associated with it, you must switch the location to a different entry.</td>
</tr>
<tr>
<td><strong>Specify VM Subnet(s)</strong></td>
<td>Enable this toggle to select one or more specific subnets to which the assignment's desktop VMs will be connected. After enabling the toggle, you can select the specific subnets from the displayed list. When this toggle is disabled, the desktop VMs will be connected to the pod’s primary VM subnet by default.</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
Filter Models | Set one or more filters to control the models available in the Models drop-down menu. You can filter models by type, series, number of CPUs, memory, and tags. For more information about selecting models, see Managing VM Types and Sizes for Farms and Assignments, which describes the options on the VM Types & Sizes page (Settings > VM Types & Sizes).

To set a filter, you first select the criterion in the drop-down menu and then enter the desired values. By default, there is a single filter with the criterion ‘Tag’ the value ‘VMware Recommended’. You can edit this first filter and add more filters connected by And and Or operators.

The following are the criteria you can use for filters and descriptions of the values you can enter for each.

**Type**

When you select this option, the second drop-down menu defaults to GPU and High Performance - Models with GPU.

*Note* If you choose a GPU model (for example, Standard_NV6), then the list of images shown will contain only images that were created with the Include GPU flag selected, so you need at least one such image in order to create a farm or pool using a GPU model. If you choose a non-GPU model, then the list of images shown will contain only images that were created without the Include GPU flag.

**Series**

When you select this option, you can then select a series of models from a second drop-down menu. You can also filter this list by entering text in the Filter text box at the top of the list.

**CPUs**

When you select this option, you can then enter a CPU range.

*Important* For production environments, to avoid unexpected end-user connection issues, use VM models that have a minimum of two (2) CPUs.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Memory</strong></td>
<td>When you select this option, you can then enter a range of memory in GBs.</td>
</tr>
<tr>
<td><strong>Tag</strong></td>
<td>When you select this option, you can then select a tag from a second drop-down menu. You can also filter this list by entering text in the Filter text box at the top of the list. Tags available in the drop-down menu are both hard-coded system tags and custom tags that you created on the VM Types &amp; Sizes page (<a href="#">Settings &gt; VM Types &amp; Sizes</a>). You can set additional filters by performing the following steps for each filter:&lt;br&gt;a Click the Add link.&lt;br&gt;b Select either And or Or as the operator between the previous filter and the new one you are creating.&lt;br&gt;c Set the new filter by selecting a criterion and entering values.</td>
</tr>
<tr>
<td><strong>Model</strong></td>
<td>Select the model to use for the desktop instances. This selection defines the set of underlying resources that will be used when the desktop instances are created, in terms of capacity (compute, storage, and so on). The available choices map to standard VM sizes that are available in Microsoft Azure. <strong>Important</strong> For production environments, select a VM model that has a minimum of two (2) CPUs. VMware scale testing has shown that using 2 CPUs or more avoids unexpected end-user connection issues. Even though the system does not prevent you from choosing a VM model with a single CPU, you should use such models for tests or proof-of-concepts only.</td>
</tr>
<tr>
<td><strong>Disk Type</strong></td>
<td>Select a supported disk type from the available options. Disk type options are based on the model selected, and your Azure subscription and region. The following are some commonly available disk types.&lt;br&gt;- Standard HDD - Default disk type.&lt;br&gt;- Standard SSD&lt;br&gt;- Premium SSD - Option only appears if you selected a model that supports premium IO. You can edit your selection after creating the assignment if desired.</td>
</tr>
</tbody>
</table>
### Disk Size

Enter the OS disk size in GB for the VMs in this assignment.
- The default value is the base image OS disk size (typically 128 GB).
- If you edit the size, the value you enter must be greater than the base image OS disk size, and cannot exceed the largest size (typically 1024 GB) supported by the selected model.
- You can also edit this value later if desired.

**Important** If you edit the disk size, there are additional actions you must take to ensure that the VMs are created as expected. For more information, see [Required Administrator Actions When the Disk Size for a Farm or VDI Desktop Assignment is Increased](#).

### Domain

Select the Active Directory domain registered with your environment.

### Join Domain

Select **Yes** so that the desktop instances are automatically joined the domain when they are created.

### Encrypt Disks

Select **Yes** so that the desktop instances have encrypted disks.

**Important** If you want disk encryption, you must make this selection when creating the VDI desktop assignment. You cannot later add disk encryption after the assignment is created.

### NSX Cloud Managed

Select **Yes** so that you can use features of NSX Cloud with the assignment’s desktop instances. For a description of using NSX Cloud features with your desktops in Microsoft Azure, see [VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure](#) and its subtopics.

**Important**
- If you want to use NSX Cloud with the desktop instances, you must make this selection when creating the VDI desktop assignment. You cannot later enable NSX Cloud management after the assignment is created.
- For the NSX Cloud management features to work with the assignment’s desktop instances, the image that you select for this assignment must have the NSX agent already installed on it. When you set this toggle to **Yes**, ensure that the image you select in **Image** has the NSX agent installed on it. The system does not verify if the selected image has the NSX agent when it creates the VDI desktop assignment.

### Use Availability Set

Select **Yes** so that Availability Sets are created for the new assignment in Microsoft Azure.

Availability Sets are groups of VMs that Microsoft Azure uses to ensure higher availability. For more information, see the Microsoft Azure documentation.

- This option appears only if the pod is at manifest version 2298.0 or higher and your VMware representative has enabled the display of this option. If the pod is at manifest version 2298.0 or higher and this option is not displayed, then Availability Sets will be created for the assignment, since this is the default for these pods.
- The maximum number of VMs in an Availability Set is 200, so assignments larger than that will have multiple Availability Sets.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image</td>
<td>Select an image that you want to assign to the end users. Only those published images in the selected pod that are appropriate for VDI desktops are listed here. A published image, sometimes called a sealed image or an assignable image, is one that was published to the system by converting a base or golden image into a desktop. <strong>Important</strong> If you set the NSX Cloud Managed toggle to Yes, ensure that the image you select here has the NSX agent installed on it. For the NSX Cloud management features to work with the assignment's desktop instances, the image that you select for this assignment must have the NSX agent already installed on it. The system does not verify if the selected image has the NSX agent when it creates the VDI desktop assignment.</td>
</tr>
<tr>
<td>Assignment Name</td>
<td>Type a friendly name for this dedicated VDI desktop assignment. Entitled end users who have not yet claimed or been assigned a desktop from this assignment might see a form of this assignment name in the client they use to access their desktops. The name must contain only letters, hyphens, and numbers. Spaces are not allowed. The name cannot start with a non-alphabetic character.</td>
</tr>
<tr>
<td>VM Names</td>
<td>Base name for the desktop VMs created in this assignment. The VM names will have numbers appended to this base name, for example, win10-1, win10-2, etc. The name must start with a letter and can contain only letters, dashes, and numbers. The end users see a form of this name in the client they use to access their desktops.</td>
</tr>
<tr>
<td>Default Protocol</td>
<td>Select a default display protocol you want the end-user sessions to use. Circumstances might occur that cause another protocol to be used instead of the default protocol. For example, the client device does not support the default protocol or the end user overrides the default protocol selection. <strong>Note</strong> For images with the Microsoft Windows 7 Enterprise operating system, RDP is the only supported choice.</td>
</tr>
<tr>
<td>Preferred Client Type</td>
<td>Select the preferred client type used when end users launch their desktops from Workspace™ ONE™ Access, either a Horizon Client or a browser for HTML Access. <strong>Note</strong> For images with the Microsoft Windows 7 Enterprise operating system, Horizon Client is the only supported choice.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Type the number of desktops required in the assignment.</td>
</tr>
</tbody>
</table>
### Administration of Your Horizon Cloud Tenant Environment and Your Fleet of Onboarded Pods

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Min Desktops</strong></td>
<td>This <em>Min Desktops</em> setting for a dedicated VDI desktop assignment works slightly different from how the setting works for a floating VDI desktop assignment. For a dedicated VDI desktop assignment, the <em>Min Desktops</em> setting refers to the unassigned desktops. When a desktop becomes assigned to a user, that desktop VM is no longer an unassigned desktop, and as a result, is not considered part of the set of desktops governed by the <em>Min Desktops</em> setting. If the number of unassigned desktop VMs in the assignment are less than the value for <em>Min Desktops</em>, you will observe that the number of powered-on VMs is less than the <em>Min Desktops</em> value.</td>
</tr>
<tr>
<td><strong>Max Desktops</strong></td>
<td>Sets the total number of desktop VMs you want in the pool of VMs defined by this assignment.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>The benefit of setting some unassigned VMs to be powered on is primarily to have some unassigned VMs ready for users to quickly log in to. Over time, as these powered-on unassigned desktops get assigned to users — either from users doing their initial logins which claim desktops for them or from an administrator using the Assign action to explicitly assign a desktop to a user — the system powers on additional unassigned desktops until it reaches the <em>Max Desktops</em> number. Finally, when all of the desktop VMs in the assignment are assigned to users, the <em>Min Desktops</em> value is not much use until a time when you explicitly start unassigning desktops from users.</td>
</tr>
<tr>
<td><strong>Power Off Protect Time</strong></td>
<td>Specify the number of minutes that you want the system to wait before automatically powering off a powered-on desktop. You can enter a value from 1 to 60. The default is 30 minutes. This protect time is used primarily for the situations where the system will automatically power off a desktop VM. You can use this <em>Power Off Protect Time</em> setting to tell the system to wait the specified time before starting to power off the VM. For example, if there is a schedule defined in the Schedule Power Management, the system can automatically power off desktops to meet the configured schedule. If you manually power on one of the assignment’s desktops within the configured schedule, the system waits the time specified for the <em>Power Off Protect Time</em> before powering off the VM to match the configured schedule. The default wait time is 30 minutes.</td>
</tr>
<tr>
<td><strong>Windows license question</strong></td>
<td>The wizard asks you to confirm you have an eligible license to use the Microsoft Windows operating system that is in the image and which will be in the desktop VMs. Follow the on-screen instructions. For a client operating system, Horizon Cloud sets the VDI assignment’s desktop VMs to use the Windows Client license type by default and you cannot change that setting.</td>
</tr>
</tbody>
</table>
Optionally configure the advanced properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer OU</td>
<td>Active Directory Organizational Unit where the desktop VMs are to be located. Enter the Active Directory Organizational Unit using the distinguished name, for example, <code>OU=RootOrgName,DC=DomainComponent,DC=eng</code>, and so on. The OU and each path in a nested OU can contain any combination of letters, numbers, special characters, and spaces, and can have a maximum of 64 characters. If you need to use nested Organization Units, see <a href="#">Considerations For Using Nested Active Directory Domain Organizational Units</a></td>
</tr>
<tr>
<td>Note</td>
<td>If the Computer OU is set to CN=Computers, the system uses the default Active Directory Computers container for VMs. Your Active Directory might have this default container redirected to an organizational unit class container.</td>
</tr>
<tr>
<td>Run Once Script</td>
<td>(Optional) Location of a script that you want run in the assignment’s desktop VMs after the VM creation process.</td>
</tr>
<tr>
<td>Note</td>
<td>The script must end with a reboot step to reboot the VM. Otherwise, the end user will not be able to log in the desktop until doing a manual restart. A sample reboot line as a Windows command is:</td>
</tr>
<tr>
<td></td>
<td><code>shutdown /r /t 0</code></td>
</tr>
<tr>
<td></td>
<td>The reason why the script must end with a reboot step is due to the sequence when the script is run after the sysprep process. When the system creates a desktop VM for the assignment, the VM boots up and completes the sysprep process in the Windows operating system. When the sysprep process completes, the agent in the desktop VM reaches out to do the domain join. At the same time, the agent gets the script path you specify here. The agent sets the Windows RunOnce path (System run once) and then restarts the desktop VM. On the next restart, the system logs in to the Windows operating system using the local administrator account and runs the script. It is only after another subsequent restart, specified in the script, that the desktop VM is ready for a user to log in.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max Desktop Deletions</td>
<td>This sets the number of desktop VMs that can be deleted in the assignment before counting them against the rate you set for <strong>Deletion Protection</strong> on the <strong>Settings &gt; General Settings</strong> page. Select one of the following options from the drop-down menu.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Unlimited</strong> - Unlimited desktop VMs can be deleted from the assignment. In this case, the <strong>Deletion Protection</strong> setting is no longer relevant.</td>
</tr>
<tr>
<td></td>
<td>- <strong>None</strong> - No additional desktop VMs can be deleted before counting them against the rate you set for <strong>Deletion Protection</strong>. In this case, the system uses only the <strong>Deletion Protection</strong> to authorize or block deletions. <strong>None</strong> is the default value for <strong>Deletion Protection</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Custom</strong> - Number of additional desktop VMs that can be deleted before counting them against the rate you set for <strong>Deletion Protection</strong>. If you select <strong>Custom</strong>, you must also enter a numerical value to the right of this drop-down menu.</td>
</tr>
<tr>
<td></td>
<td>For example, you might set <strong>Max Desktop Deletions</strong> to 10 and <strong>Deletion Protection</strong> to 1. In this case, after the first 10 VMs are deleted (no matter how long it takes for the count to reach 10), the system only allows 1 additional VM to be deleted per hour from that time forward.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> If you specify a new image for a dedicated desktop assignment, the system changes the <strong>Max Desktop Deletions</strong> setting if necessary so that all unassigned desktop VMs can be rebuilt with the new image.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you select <strong>Unlimited</strong> for <strong>Deletion Protection</strong>, there is no need to use the <strong>Max Desktop Deletions</strong> setting.</td>
</tr>
<tr>
<td></td>
<td>For more information about the <strong>Deletion Protection</strong> setting, see <strong>Customizable General Settings for Your Horizon Cloud Tenant Environment</strong>.</td>
</tr>
</tbody>
</table>
|                        | To prevent all VM deletions in a dedicated desktop assignment, use the **Prevent Deletions** setting on the **Assignments** page. See **Prevent Deletions or Allow Deletions for a Dedicated Desktop Assignment**.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Session Timeout Interval</strong></td>
<td>This time interval is the amount of time the end users' sessions can be idle before the system forces a log off from the desktops. This timeout applies to the logged-in session to the underlying Windows operating system. The time you specify here is different from the time out settings that govern the end users' Horizon Client or HTML Access logged-in session.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong>   When the system forces the log off in the underlying Windows operating system session, any unsaved data is lost. To prevent an unintended loss of data, set this interval high enough to accommodate the business needs of your users.</td>
</tr>
<tr>
<td></td>
<td>The default interval is one week (10080 minutes).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>      If no user activity occurs before the timeout interval is reached, a message indicates that the user will be logged off if they do not click <strong>OK</strong> in the next 30 seconds. If the logout occurs, any unsaved user data, such as documents or files, is lost.</td>
</tr>
<tr>
<td><strong>Azure Resource Tags</strong></td>
<td>(Optional) Create custom tags to be applied to Azure resource groups. Azure resource tags are only applied to the resource groups, and are not inherited by the resources in the groups. To create the first tag, enter information in the Name and Value fields. To create an additional tag, click <strong>Add</strong> and then enter information in the Name and Value fields that appear below the existing ones.</td>
</tr>
<tr>
<td></td>
<td>■ You can create a maximum of 10 tags.</td>
</tr>
<tr>
<td></td>
<td>■ The tag name is limited to 512 characters, and the tag value is limited to 256 characters. For storage accounts, the tag name is limited to 128 characters, and the tag value is limited to 256 characters.</td>
</tr>
<tr>
<td></td>
<td>■ Tag names cannot contain the following characters:</td>
</tr>
<tr>
<td></td>
<td>\ &lt; &gt; % &amp; \ ? /</td>
</tr>
<tr>
<td></td>
<td>■ Tag names cannot contain these case-insensitive strings:</td>
</tr>
<tr>
<td></td>
<td>‘azure’, ‘windows’, ‘microsoft’</td>
</tr>
<tr>
<td></td>
<td>After an assignment has been created, you can add more Azure resource tags and edit or delete tags for that assignment.</td>
</tr>
</tbody>
</table>
5 In the wizard’s Management step, complete the fields and make your selections as appropriate and then click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Image Updates</strong></td>
<td>The <strong>Concurrent Quiescing Desktops</strong> setting controls the number of unassigned desktops in this dedicated VDI desktop assignment that can be concurrently quiesced during the time the assignment’s image is being updated. For example, when you later edit this dedicated VDI desktop assignment to use another image, the system will power off at the same time this number of unassigned desktops. Then the system performs the required actions to provision the new image to that set of powered-off unassigned desktops. <strong>Note</strong> Desktops in a dedicated VDI desktop assignment that are mapped to users are said to be assigned to those users. Unassigned desktops in a dedicated VDI desktop assignment are desktops which have not yet been mapped to specific users.</td>
</tr>
</tbody>
</table>
| **Timeout Handling**          | Configure how you want the system to handle the desktops’ user sessions. **Note** The user sessions governed by these settings are the user logins to the desktops’ Windows operating system. These sessions are not the user logins in Horizon Client, Horizon HTML Access, or Workspace ONE. The user’s session begins when the user authenticates to the desktop’s Windows operating system.  
|                               | - **Log Off Disconnected Sessions** - Select when the system will log the user off of a disconnected session.  
|                               | - **Max Session Lifetime** - Specify the maximum number of minutes the system should allow for a single user session. |
| **Schedule Power Management** | To help optimize savings and performance of the desktop VMs in Microsoft Azure, you can optionally configure schedules to adjust the minimum number of powered-on unassigned desktop instances on a recurring weekly basis. For example:  
|                               | - For weekends or night hours when you know that your end users will not be using their desktops, you can have a schedule for zero or a low number of powered-on unassigned desktops.  
<p>|                               | - For specific days or specific hourly stretches that you can predict will have increased end user demand, you can have a schedule that increases the minimum number of powered-on unassigned desktops to be available to meet that demand. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can specify up to 10 schedules for the dedicated VDI desktop assignment. If any schedules have overlapping time periods but specify different minimum unassigned desktop numbers, the system uses the largest value minimum unassigned desktops for the overlapping time period.</td>
<td></td>
</tr>
</tbody>
</table>

**Caution** By default, when you configure a schedule here for a dedicated VDI desktop assignment, the system keeps all of the already assigned desktop VMs powered on, regardless of the schedule. That is:

- If you set any schedule here, it results in the system leaving the currently assigned (mapped to a user) desktop VMs on. The schedule only controls the power state of unassigned desktops, if any.
- Having a schedule here changes the system’s treatment of the power-on behavior of the assigned desktops from what it would be in the absence of a schedule. When there is no schedule configured here, the system powers off the assigned desktops that have no logged-in users.

For example, if all of the desktops in this dedicated VDI desktop assignment are mapped to users (assigned), and there is a schedule configured here, the system does not power off those assigned desktops by design. This design is for ensuring an assigned desktop is ready to meet its mapped-to user’s request to log in, even when a schedule is in effect.

As a result, if all of the desktops are in assigned state, when a schedule is set here, those assigned desktops will remain powered on, even when their assigned users are not logged in. If you want all assigned desktop VMs to be powered off during a specific day, like a weekend day, do not configure any schedules here.

To configure a schedule:

a. Click the + icon to add the first row in the Schedule Power Management section.

b. Type an identifying name for the first schedule.

c. Select the days for the first schedule.

**Note** One day is automatically selected by default when the row is added. If you do not want to include the selected day in this schedule, click the drop-down and deselect that selected day.

d. Specify the applicable hours in the specified days. Either:

- Select the **All Day** check box to have this schedule in effect for all hours of the specified days.

- Specify start and end times for the time period in each day.

**Note** Encrypted VMs take longer to power on than non-encrypted VMs. If you have set **Encrypt Disks** to Yes, and you want 100% of the encrypted VMs to be ready for end-user connections at a particular time of day, you might have to set an earlier start time here. See When Scheduling Power Management for Farms and VDI Desktop Assignments That Have Large Numbers of Encrypted VMs.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>Select the time zone. The time zone closest to your end users' location is recommended. As appropriate for the selected time zone, Daylight Savings Time is automatically applied.</td>
</tr>
<tr>
<td>Note</td>
<td>If two schedules have the same time zone setting and have overlapping times, a warning is displayed. However, if two schedules have different time zone settings and overlap, the warning is not displayed. As an example, if you have two all-day Saturday schedules and one has Europe/London time zone selected and the other has America/Toronto selected, the overlap warning does not display.</td>
</tr>
<tr>
<td>f</td>
<td>In the Min Desktops field, type the minimum number of unassigned desktops you want powered on during the specified time period. During the specified time period, that number of unassigned desktops at a minimum will be powered on to be available to take end user requests during that time. The number can range from zero (0) up to the number specified for Max Desktops for the overall dedicated VDI desktop assignment.</td>
</tr>
<tr>
<td>Important</td>
<td>The Min Desktops field in the power management schedules controls only the unassigned desktops. Assigned desktops do not participate in the power management schedule. When all desktops in the dedicated VDI desktop assignment are in Assigned state, this Min Desktops value, which controls the unassigned desktops, defaults to zero (0).</td>
</tr>
<tr>
<td></td>
<td>When this number is zero (0) and there are no active end user sessions at the schedule's starting time point, the assignment's desktops are powered off. In that scenario, if an end user subsequently attempts to connect to a desktop from this assignment during the scheduled time period, there will be a delay before the desktop is in a usable state because the underlying desktop VM has to power on.</td>
</tr>
<tr>
<td>Note</td>
<td>By default, when a user logs off of a desktop at a time that lies outside of a schedule's time period, the system protects the desktop VM from powering off for the time specified in the Power Off Protect Time field. The default is 30 minutes.</td>
</tr>
</tbody>
</table>

6. On the Users step, search for users and groups in your registered Active Directory domains, select the ones you want to entitle to use desktops from this assignment, and then click Next.

7. On the Summary step, review the configuration and then click Submit.
Results

The system begins the process of configuring the desktop instances to provide VDI desktops to the selected users. On the Assignments page, the Status column reflects the current progress.

**Note** Creation of an encrypted desktop VM takes approximately twice as long as creating a non-encrypted VM. As a result, the end-to-end time to complete creating a VDI desktop assignment that has disk encryption enabled is approximately twice as long as creating that VDI desktop assignment without disk encryption enabled.

Also, when the image VM has a data disk, additional time is needed for creating an encrypted desktop VM based on that image VM. The longest times occur for data disks of larger, terabyte sizes.

What to do next

If the VDI desktop has applications that require opening special ports, you might need to modify this VDI desktop assignment's associated Network Security Group (NSG) in Microsoft Azure. For details about the pod's NSG, see [About Network Security Groups and Your VDI Desktops](#).

If you specified NSX Cloud management for this assignment, you can use your NSX Cloud environment's Service Manager (CSM) to see that the desktop VMs are managed in NSX Cloud. Log in to your environment's CSM and navigate to **Clouds > Azure > Instances**. When that Instances page shows a status of Managed for the desktop instances, you can start implementing NSX policies on them.

Create a URL Redirection Customization and Assign it to Users

In the Horizon Cloud Administration Console, you create customization assignments to assign settings that customize your end users' environments. One type of customization is URL redirection. You can define URL handling rules where the Horizon Client redirects URLs from the end user’s client machine to a desktop or application provided by your Horizon Cloud environment. A URL redirection configuration gives the Horizon Client information about which URLs should be handled by one of the end user's assigned Horizon Cloud desktops or applications instead of being opened by the user's local system.

**Note**
- The administrative console provides a user interface for you to configure client-to-agent URL redirection. To configure agent-to-client URL redirection, you must use group policy settings as described in [Configuring Agent-to-Client Redirection](#). The steps below are for configuring client-to-agent URL redirection.
- When your Horizon Cloud tenant is configured to use Universal Broker for your pods in Microsoft Azure, creating these URL redirection customizations is not currently supported.
The Horizon Client fetches an end user's assigned URL redirection rules when the user logs in to the Horizon Client on their local device. Then when that user attempts to open a link in a local document or file and the link matches a URL pattern rule in the assigned settings, Horizon Client determines the appropriate handler to use. The handlers are specified opens the user's assigned desktop or application to handle the URL link, as determined by the appropriate handler you specified in the URL redirection configuration. If the URL redirection handler specifies to use a desktop, the desktop's default application for the link's specified protocol processes the URL. If the handler specifies to use an application, the user's assigned application processes the URL. If the user is not entitled to the desktop or application specified in the handler, Horizon Client displays a message to the user, unless you have specified **Strict Match as No** for the handler.

In the scenario where **Strict Match** is set to **No**, the system locates a resource to use based on this fall-back behavior:

1. The system searches the user's assignments using a substring match of the target resource specified for the handler. If the system finds an assignment that matches the substring, that assigned desktop or application is used to open the link.

2. When the handler's **Resource Type** is set to **Application**, if the search for a substring match fails, the system searches the user's application assignments for an assigned application that can handle the protocol specified in the handler's **Scheme** field.

   **Note** This step in the fall-back behavior only applies for applications. If the **Resource Type** is set to **Desktops**, this step is skipped.

3. If the system cannot locate a resource in the user's assignments that can handle the protocol, Horizon Client displays a message to the user.

**Important** The user's Horizon Client must be installed with the `URL_FILTERING_ENABLED=1` option to give the client the capability to handle the URL redirection feature. For details, see the [Installing Horizon Client for Windows with the URL Content Redirection Feature](#) topic in the VMware Horizon documentation.

When your environment is integrated with Workspace ONE Access, the user must have opened at least one application using Horizon Client before the URL redirection feature can work for that user. By opening at least one application using the **Open in Client** option, the user's assigned URL redirection configuration is loaded into the client device's registry where Horizon Client can get the configuration values.

A customization assignment can be turned inactive by using the **Take Offline** button on the Assignments page. A user can be assigned more than one active customization for URL redirection settings. To avoid potential conflicts between rules from different active configurations, when the user logs in to Horizon Client, the system:

- Sets only one configuration in effect, even when that user has more than one active configuration assigned.
- Uses the URL redirection configuration that is alphabetically first as the configuration in effect for the user.
Prerequisites

In the console, you can create a customization for URL redirection even before you have any desktops or remote applications in your Horizon Cloud inventory. However, before the URL redirection flow works for those end users specified in the customization, the following prerequisites must be met:

- When the image VM was created using the Import Virtual Machine from Marketplace workflow, you set the Horizon agent feature named **URL Redirection** to **Yes**.
- Your Horizon Cloud inventory has the desktops and remote applications that you intend to use in the configuration.
- If the customization has **Strict Match** set to **Yes**, assignments must exist that entitle the specific desktops and remote applications to the end users specified in the customization.

Procedure

1. On the Assignments page, click **New**.
2. In the New Assignment window, click the **Customizations** icon. The New Customization Assignment wizard opens to its first step.
3. In the Definition step, configure the general settings and then click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment Name</td>
<td>Enter a friendly name for this assignment.</td>
</tr>
<tr>
<td>Location</td>
<td>Select the location that has the pod you want to use.</td>
</tr>
<tr>
<td>Pod</td>
<td>Select the pod. This pod is the one from which the session desktops and remote applications are served.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally enter a description for the configuration.</td>
</tr>
</tbody>
</table>
In the Configuration step’s Source section, create a list of URL patterns that this configuration will tell Horizon Client to intercept on the client system.

- In the **URL Pattern** field, type a string that specifies the URL matching pattern to be intercepted.

  You can use wildcards to specify a URL pattern that matches multiple URLs. For example:
  
  - If you type `google.*`, all URLs that include the text `google` are intercepted.
  - If you type `.*` (period asterisk), all URLs are intercepted for all protocol schemes (matches all).
  - If you type `mailto://.*.example.com` all URLs that contain the text `mailto://.*.example.com` are intercepted.

  **Important** You should always consider that the URLs you enter in the **URL Pattern** field are case-sensitive, including the host name part like `docs.vmware.com`. The URL redirection feature behavior is sensitive to the case of the URL patterns you enter here. As an example, if you enter `DOCS.VMWARE.COM/*` as the pattern and the end user clicks a link `https://docs.vmware.com`, the URL redirection does not happen, because the host name exists actually in lowercase. For host names, enter them as lowercase. If you need to match subdirectories in the URL path, use a wildcard or enter those URLs as the path actually exists, such as `docs.vmware.com/en/VMware-Horizon-Cloud-Service/*`.

- Press Enter to add your specified URL pattern to the list.

- Repeat the steps of typing in a pattern and pressing Enter to add more URL matching patterns.
5 In the Rules section, define the set of handlers that determine which target inventory resource should handle various protocols.

A handler defines which of the user’s entitled desktops or applications should handle that specific protocol. For example, if the user opens a Microsoft Word document that has a mailto hypertext link and the user clicks on that link in the document, the handler defines what entitled application should handle the request, such as Microsoft Outlook or Mozilla Thunderbird.

a In the Rules section, configure the settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td>Enter the protocol to which this handler applies, such as http, https, mailto, callto, and so on.</td>
</tr>
<tr>
<td>Resource Type</td>
<td>Select whether a desktop or application is to handle the specified protocol.</td>
</tr>
<tr>
<td>Target Resource</td>
<td>Enter the name of the target resource in your inventory that you want handling the protocol specified in the Scheme field.</td>
</tr>
<tr>
<td>Strict Match</td>
<td>Select Yes to force an exact match between the name specified in the Target Resource field and the names of the user’s available entitled session desktops or remote applications. Select No if you want the system to use its fall-back behavior to support the situation where an end user does not have an assignment for a resource with the exact name specified in the Target Resource field. For example, when the Resource Type is set to Applications and you specify Microsoft Outlook as the target resource to handle the mailto protocol, but the user does not have an assignment for any Microsoft Outlook applications, when Strict Match is set to No, the system will search for a compatible application assigned to that user to handle the mailto protocol, such as Mozilla Thunderbird.</td>
</tr>
</tbody>
</table>

b To add more handlers, click Add a row and complete the fields.

6 Click Next to proceed to the next wizard step.

7 Search for and select the users and groups for this assignment and click Next.

8 Review the summarized information and click Submit.

Understanding What URL Content Redirection Is

Generally speaking, the URL content redirection feature supports redirection from a remote desktop or application to a client, and from a client to a remote desktop or application.

Redirection from a remote desktop or application to a client is called agent-to-client redirection. Redirection from a client to a remote desktop or application is called client-to-agent redirection.

Agent-to-client redirection
With agent-to-client redirection, Horizon Agent sends the URL to Horizon Client, which opens the default application for the protocol in the URL on the client machine. For details about configuring agent-to-client redirection, see Configuring Agent-to-Client Redirection.

Client-to-agent redirection

With client-to-agent redirection, the system opens a remote desktop or remote application that you specified to handle the URL. For details about configuring client-to-agent redirection, see Create a URL Redirection Customization and Assign it to Users.

You can redirect some URLs from a remote desktop or application to a client, and redirect other URLs from a client to a remote desktop or application. You can redirect any number of protocols, including HTTP, HTTPS, mailto, and callto.

Configuring Agent-to-Client Redirection

With agent-to-client redirection, Horizon Agent sends the URL to Horizon Client, which opens the default application for the protocol in the URL.

To enable agent-to-client redirection, perform the following configuration tasks.

- Ensure the URL content redirection feature is enabled in Horizon Agent in the image VM, as described in the prerequisites section in Create a URL Redirection Customization and Assign it to Users.
- Apply the URL Content Redirection group policy settings to your remote desktops and applications. See Add the URL Content Redirection ADMX Template to a GPO.
- Configure group policy settings to indicate, for each protocol, how the Horizon Agent should redirect the URL. See URL Content Redirection Group Policy Settings.

Add the URL Content Redirection ADMX Template to a GPO

The URL Content Redirection ADMX template file, called urlRedirection.admx, contains settings that enable you to control whether a URL link is opened on the client (agent-to-client redirection) or in a remote desktop or application (client-to-agent redirection).

To apply the URL Content Redirection group policy settings to your remote desktops and applications, add the ADMX template file to GPOs on your Active Directory server. For rules regarding URL links clicked in a remote desktop or application, the GPOs must be linked to the OU that contains your virtual desktops and RDS hosts.

You can also apply the group policy settings to a GPO that is linked to the OU that contains your Windows client computers, but the preferred method for configuring client-to-agent redirection is to use the vdmutil command-line utility. Because macOS does not support GPOs, you must use vmdutil if you have Mac clients.

Prerequisites

- Verify that the URL content redirection feature is included when Horizon Agent is installed in the image VM, as described in Create a URL Redirection Customization and Assign it to Users.
Verify that Active Directory GPOs are created for the URL Content Redirection group policy settings.

Verify that the MMC and the Group Policy Management Editor snap-in are available on your Active Directory server.

Procedure

1. Download the Horizon GPO Bundle ZIP file from the Horizon Cloud downloads page located within the Downloads area of my.vmware.com.

Log in to my.vmware.com, navigate to the Product Downloads area, and navigate to the latest VMware Horizon Cloud Service on Microsoft Azure entry. In the Files area, look for a row that displays Horizon View GPO Bundle. Click Read More to see the file name. The file has a name in the form VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyyy.zip where x.x.x is the version and yyyyyyyy is the build number. All ADMX files that provide group policy settings for the product are available in this file.

2. Unzip that ZIP file and copy the URL Content Redirection ADMX file to your Active Directory server.
   a. Copy the urlRedirection.admx file to the C:\Windows\PolicyDefinitions folder.
   b. Copy the urlRedirection.adml language resource file to the appropriate subfolder in C:\Windows\PolicyDefinitions.

      For example, for the EN locale, copy the urlRedirection.adml file to the C:\Windows\PolicyDefinitions\en-US folder.

3. On your Active Directory server, open the Group Policy Management Editor.

The URL Content Redirection group policy settings are installed in Computer Configuration > Policies > Administrative Templates > VMware Horizon URL Redirection.

What to do next

Configure the group policy settings in your Active Directory server. For descriptions of the settings, see URL Content Redirection Group Policy Settings.

URL Content Redirection Group Policy Settings

The URL Content Redirection template file contains group policy settings that enable you to create rules for configuring the agent-to-client redirection capability for your Horizon Cloud
environment. The template file contains only Computer Configuration settings. All of the settings are in the **VMware Horizon URL Redirection** folder in the Group Policy Management Editor.

**Important** Even though the URL Content Redirection template file contains group policy settings related to client-to-agent redirection, you do not use group policy settings to configure client-to-agent redirection. Instead, you use the Horizon Cloud Administration Console to create the rules for client-to-agent redirection. You create rules for client-to-agent redirection when you create a URL redirection assignment in the console. For detailed steps, see [Create a URL Redirection Customization and Assign it to Users](#).

The following table describes the group policy settings available in the URL Content Redirection template file.

**Table 7-3. URL Content Redirection Group Policy Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE Policy: Prevent users from changing URL Redirection plugin loading behavior</td>
<td>Determines whether users can disable the URL Content Redirection feature. This setting is not configured by default.</td>
</tr>
<tr>
<td>IE Policy: Automatically enable URL Redirection plugin</td>
<td>Determines whether newly installed Internet Explorer plug-ins are automatically activated. This setting is not configured by default.</td>
</tr>
<tr>
<td>Url Redirection Enabled</td>
<td>Determines whether the URL Content Redirection feature is enabled. You can use this setting to disable the URL Content Redirection feature even if the feature has been installed in the client or agent. This setting is not configured by default.</td>
</tr>
</tbody>
</table>
Table 7-3. URL Content Redirection Group Policy Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Url Redirection Protocol 'http'</strong></td>
<td>For all URLs that use the HTTP protocol, specifies the URLs that should be redirected. This setting has the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Broker Hostname</strong> - IP address or fully qualified name of the Connection Server host to use when redirecting URLs to a remote desktop or application.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Remote Item</strong> - display name of the remote desktop or application pool that can handle the URLs specified in <strong>Agent Rules</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Client Rules</strong> - the URLs that should be redirected to the client. For example, if you set Client Rules to *.mycompany.com, all URLs that include the text mycompany.com are redirected to the Windows-based client and are opened in the default browser on the client.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Agent Rules</strong> - the URLs that should be redirected to the remote desktop or application specified in <strong>Remote Item</strong>. For example, if you set Agent Rules to *.mycompany.com, all URLs that include mycompany.com are redirected to the remote desktop or application.</td>
</tr>
<tr>
<td></td>
<td>When you create agent rules, you must also use the <strong>Broker Hostname</strong> option to specify the IP address or fully qualified domain name of the Connection Server host, and the <strong>Remote Item</strong> option to specify the display name of the desktop or application pool.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The preferred method for configuring client rules is to use the vdmutil command-line utility.</td>
</tr>
<tr>
<td></td>
<td>This setting is enabled by default.</td>
</tr>
</tbody>
</table>

| **Url Redirection Protocol '[...]'** | Use this setting for any protocol other than HTTP, such as HTTPS, email, or callto. The options are the same as for **Url Redirection Protocol 'http'**.                                                               |
|                                     | If you do not need to configure other protocols, you can delete or comment out this entry before adding the URL Content Redirection template file to Active Directory.                                           |
|                                     | As a best practice, configure the same redirection settings for the HTTP and HTTPS protocols. That way, if a user types a partial URL into Internet Explorer, such as mycompany.com, and that site automatically redirects from HTTP to HTTPS, the URL Content Redirection feature will work as expected. In this example, if you set a rule for HTTPS but do not set the same redirection setting for HTTP, the partial URL that the user types is not redirected. |
|                                     | This setting is not configured by default.                                                                                                                                                                  |

Managing Published Images for Horizon Cloud Pods in Microsoft Azure

After you publish an image, you can manage that image using the Administration Console. A published image is an image that has successfully completed the Horizon Cloud sealing process and Horizon Cloud can use it to provision RDS farms (in the case of RDSH-capable images) or VDI desktops. Other terms sometimes used to describe such images are sealed images and
assignable images. Sealing an image is sometimes referred to as publishing the image or converting the image to a desktop.

**Actions You Can Perform on Published Images from Horizon Cloud Pods in Microsoft Azure**

After you publish an image, you can manage that image using the Horizon Cloud Administration Console. A published image is an image that has successfully completed the Horizon Cloud sealing process and Horizon Cloud can use it to provision the RDSH VMs in an RDSH farm (in the case of RDSH-capable images) or provision VDI desktop VMs. Other terms sometimes used to describe such images are sealed images and assignable images. When an image is sealed, the Images page shows it having Published status.

**Procedure**

1. Select **Inventory > Images**.
2. Click the check box corresponding to the image you want to act on.
To perform an action on an image, select the image's check box and click one of the action buttons.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename</td>
<td><strong>Note</strong> This page contains an action named <strong>Rename</strong> in a deactivated state, because that action is not supported currently for images from a pod deployed in Microsoft Azure.</td>
</tr>
<tr>
<td>Duplicate</td>
<td>The duplicate workflow is typically used when updating a farm's or VDI desktop assignment's underlying golden image, for example, to install or update applications in the image VM. Duplicating an existing image creates an image with the same configuration and a new name. For detailed steps of changing images used for farms and VDI desktop assignments, see Change Images Used for Farms in Horizon Cloud and Change Images Used for VDI Desktop Assignments. When you click <strong>Duplicate</strong>, you must enter a name for the new duplicated VM. After you enter a new name and click <strong>Save</strong>, the system clones the sealed image's VM to make a new base VM, and lists the new VM on the <strong>Imported VMs</strong> page. When you see that the <strong>Imported VMs</strong> page reports the new VM's agent is active, you can log in to it and make changes. When you are finished making your changes, you convert the duplicate to an assignable (sealed) image by either using the Images page's <strong>New</strong> action or by selecting the image on the <strong>Imported VMs</strong> page and selecting <strong>Convert to Image</strong>. <strong>Note</strong> As the system begins the cloning process, the original sealed image goes into <strong>Transition</strong> status for the first part of the process. After some time, the original sealed image returns to its original state. You can monitor the progress of the duplicate image on the <strong>Imported VMs</strong> page or using the Activity page.</td>
</tr>
<tr>
<td>Update Agent</td>
<td>Update the image's agent-related software components to a newer version. Clicking this button opens the Agent Update wizard. A blue dot appears next to the name of an image when agent updates are available for it. When you hover over that blue dot, a popup indicates all of the agent updates that are available for that image. For details, see one of the following topics: - Update Agent Software for RDSH Images in Horizon Cloud - Update Agent Software for Images Used by Floating VDI Desktop Assignments <strong>Important</strong> For dedicated VDI desktop assignments, you usually update the agents from the Assignments page instead of by updating the agents in the image. See Update Agent Software for Dedicated VDI Desktop Assignments.</td>
</tr>
</tbody>
</table>
To perform one of the other available actions, click **More** and select the option you want.

**Note** Even though the **Download Bootstrap** and **Refresh Password** actions are visible when an image is selected, those actions are not applicable to any one image.

<table>
<thead>
<tr>
<th>Drop-Down Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Delete**       | Permanently deletes the selected image.  
  **Note** An image cannot be deleted if the system detects the image is in use, such as by a farm. |
| **Publish**      | For images used in farms or VDI desktop assignments, this action republishes a duplicated image to make it assignable again. This action is not available if the image already is an assignable (sealed) image. An assignable image is one that has Published status. |
| **Convert to Desktop** | Use this action only on images that have failed the publishing workflow and did not reach the Published status. This action converts the published image to an unsealed VM. The unsealed VM is listed on the **Imported VMs** page at that point.  
  **Caution** Use this action sparingly. Repeated use of this action on the same image can result in unexpected results and failure to seal the image when attempting to republish the image. As an example, if you create a new image, then run Publish on it and it reaches Published status, then you run Convert to Desktop on that image, then run Publish again, the Sysprep process that happens in the publishing workflow can fail. If you again convert the image back to an unsealed image, from that point on, the image might always fail the publishing workflow. At that point, it is prudent to start fresh and make a new base image. |
| **Assign Image** | Even though the console displays this action, this action is not used for images in a Microsoft Azure environment. As a result, the action is inaccessible. |
| **Bulk Assign Image** | Assigns the image to multiple assignments or farms that are based on the immediate parent image (the image from which the selected image was duplicated or updated).  
In the Bulk Assign Image dialog box, select the assignments and farms in the list and click **Update**.  
**Note** This option is only available for images created using the **Duplicate** operation and images updated to newer agent versions using the **Update Agent** operation. |

4. (Optional) View details about the image by clicking the image's name.

The screen displays the image's details page and buttons for those actions you can perform on the image from its details page.

For example, this screen is the information for an RDS-enabled assignable server image named lawin2016. This image belongs to a pod named lakjun30 and is referenced by two RDSH farms.
Change Images Used for Farms in Horizon Cloud

After you publish your initial RDSH-capable image and create farms using it, you can make changes to that image and push the changes to all of the farms using that image. A typical reason to update an already published image is to install additional third-party applications or other features. You start this workflow in the Horizon Cloud Administration Console.

**Note**  If you are changing the RDSH-capable image to update the Horizon Cloud agent-related components, you use a different procedure. See Update Agent Software for RDSH Images in Horizon Cloud.

At a high-level, the workflow to update an in-use image is:

1. Duplicate the existing image to create an image with the same configuration and a new name. In the duplication process, the system clones the sealed image’s virtual machine (VM) to make a new unpublished golden image VM, and lists the new VM on the Imported VMs page.

2. When you see that the Imported VMs page reports the new VM’s agent is active, log in to the VM and make your desired changes to that duplicate VM.

3. Use **Convert to Image** to publish that duplicate VM, making it an assignable (sealed) image.

4. Edit the farms that are using the original image to use the newly updated duplicate image instead of the original one.
Prerequisites

Verify you have local administrator account credentials to log in to the image and update it. This administrator account is the same one that was used to publish the image using the New Image workflow. See Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

Note  When using the Microsoft Remote Desktop Client as your RDP software to connect to the VM, ensure it is the most up-to-date version. For example, the default RDP software in the Windows 7 operating system is not at a high enough version. The version must be version 8 or higher.

Procedure

1  In the console, navigate to Inventory > Images.

2  Select the check box for the image and click Duplicate.

   In the dialog box, enter a name for the duplicate image. After you enter a new name and click Save, the system clones the sealed image's VM to make a new image VM, and lists that new VM on the Imported VMs page.

   Note  As the system begins the cloning process, the original sealed image goes into Transition status for the first part of the process. After some time, the original sealed image returns to its original state.

3  Navigate to Inventory > Imported VMs to see when the Imported VMs page reports the new VM's agent is active.

4  When you see on the Imported VMs page that the new VM's agent is active, use the VM's IP address and your RDP software to connect to the RDSH-capable Windows operating system.

   - If the original image was created with a public IP address, the new duplicate VM has a public IP address and you can use that IP address in your RDP software
   
   - If the original image was not created with a public IP address, the new duplicate VM has an IP that is private in your Microsoft Azure cloud environment, and you must RDP into it by one of these two methods:
   
     - Using another VM in your Microsoft Azure subscription that does have a public IP address and doing an outbound RDP into the VM.
     
     - Use your VPN and RDP into the VM over your corporate network

5  Log in to the Windows operating system using the username and password that was supplied in the Import Image wizard when the image was created.

   If using the local administrator name, enter the username as \username.

6  In the Windows operating system, perform your intended updates.

   If you are installing additional third-party applications, see the steps described in For a Horizon Cloud Imported VM with a Microsoft Windows Server Operating System — Customize the VM for Your Organization's Needs.
7 Return to the Imported VMs page, select the check box for that duplicate VM, and click More > Convert to Image.

The system takes the image, which was duplicated and then updated, through its standard publishing process. The image is displayed on the Images page. When the publishing process is complete, the image has the Published status on the Images page.

8 When you see that the duplicated and updated image is in Published status, update each farm that is using the original image to use the new duplicate image instead, the image which now has your changes in it.

In each farm's details page, click the General Settings Edit link to open a window, select the new duplicate image, and save.

Results

The farms you update automatically delete and re-create their RDSH instances using the updated image.

What to do next

When you have updated the farms that are using the original image and can determine the original image is no longer needed by your organization, use the Images page to delete the original image. Deleting the original image is a best practice, to prevent other administrators in your organization from using an image that has down-level software.

Change Images Used for VDI Desktop Assignments

After you publish an image and create VDI desktop assignments using it, you can make changes to that image and push the changes to all of the VDI desktop assignments that use that image. A typical reason to update an already published image is to install additional third-party applications or other features. You start this workflow in the Horizon Cloud Administration Console.

Note If you are changing the image to update the Horizon Cloud agent-related components, you use a different procedure. See Updating the Agent-Related Software Used by Horizon Cloud and its subtopics.

At a high-level, the workflow to update an in-use image is:

1 Duplicate the existing image to create an image with the same configuration and a new name. In the duplication process, the system clones the sealed image's virtual machine (VM) to make a new unpublished golden image VM, and lists the new VM on the Imported VMs page.

2 When you see that the Imported VMs page reports the new VM's agent is active, log in to the VM and make your desired changes to that duplicate VM.

3 Use Convert to Image to publish that duplicate VM, making it an assignable (sealed) image.

4 Edit the VDI desktop assignments that are using the original image to use the newly updated duplicate image instead of the original one.
Prerequisites

Verify you have local administrator account credentials to log in to the image and update it. This administrator account is the same one that was used to publish the image using the New Image workflow. See Convert a Configured Image VM to an Assignable Image in Horizon Cloud.

Note When using the Microsoft Remote Desktop Client as your RDP software to connect to the VM, ensure it is the most up-to-date version. For example, the default RDP software in the Windows 7 operating system is not at a high enough version. The version must be version 8 or higher.

Procedure

1. In the console, navigate to Inventory > Images.
2. Select the check box for the image and click Duplicate.

   In the dialog box, enter a name for the duplicate image. After you enter a new name and click Save, the system clones the sealed image's VM to make a new image VM, and lists the new VM on the Imported VMs page.

   Note As the system begins the cloning process, the original sealed image goes into Transition status for the first part of the process. After some time, the original sealed image returns to its original state.

3. Navigate to Inventory > Imported VMs to see when the Imported VMs page reports the new VM's agent is active.

4. When you see on the Imported VMs page that the new VM's agent is active, use the VM's IP address and your RDP software to connect to the Windows operating system.
   - If the original image was created with a public IP address, the new duplicate VM has a public IP address and you can use that IP address in your RDP software
   - If the original image was not created with a public IP address, the new duplicate VM has an IP that is private in your Microsoft Azure cloud environment, and you must RDP into it by one of these two methods:
     - Using another VM in your Microsoft Azure subscription that does have a public IP address and doing an outbound RDP into the VM.
     - Use your VPN and RDP into the VM over your corporate network

5. Log in to the Windows operating system using the username and password that was supplied in the Import Image wizard when the image was created.
   - If using the local administrator name, enter the username as \username.

6. In the Windows operating system, perform your intended updates.
   - If you are installing additional third-party applications, see the steps described in For a Horizon Cloud Imported VM with a Microsoft Windows Client Operating System — Customize the VM for Your Organization's Needs.
7 Return to the Imported VMs page, select the check box for that duplicate VM, and click More > Convert to Image.

The system takes the image, which was duplicated and then updated, through its standard publishing process. The image is displayed on the Images page. When the publishing process is complete, the image has the Published status on the Images page.

8 When you see that the duplicated and updated image is in Published status, edit each VDI desktop assignment that is using the original image to use the new duplicate image instead, the image which now has your changes in it.

Results

When you update a VDI desktop assignment to change its image:

- Unassigned, powered-off VMs in the assignment are automatically recreated using the new image.
- Unassigned VMs that are powered on but do not have an active end user connection are automatically recreated with the new image.
- Unassigned VMs that are powered on and which have an active end user connection, such as those from a floating VDI desktop assignment, are automatically updated with the new image when the end user logs off.
- Desktop VMs that are mapped to an end user, such as those from a dedicated VDI desktop assignment, are not automatically updated to the new image. To get such an assigned desktop VM updated to use the new duplicate image instead, you must manually unassign that desktop VM. The next time the system goes to power on the desktop VM, it will apply the new image. Then you can manually assign that desktop VM back to a specific end user.

What to do next

When you have updated the VDI desktop assignments that are using the original image and you can determine the original image is no longer needed by your organization, use the Images page to delete the original image. Deleting the original image is a best practice, to prevent other administrators in your organization from using an image that has down-level software.

Managing Assignments Provisioned By Horizon Cloud Pods in Microsoft Azure

After you create an assignment that uses resources from one or more of your pods in Microsoft Azure, you can manage the assignment using the Horizon Cloud Administration Console. The
types of assignments in your Horizon Cloud tenant environment depend on what you have created.

**Tip** The console is dynamic and reflects the workflows and settings that are appropriate for the up-to-the-moment situation in your Horizon Cloud tenant environment. The labels displayed for the console's assignment-related pages will vary depending on factors such as the tenant's configured brokering setting, the types of cloud-connected pods in your fleet, the tenant's regional cloud plane, and features that are based on specific licensing.

You work with assignments from the console's assignments-related pages. The types of actions you can use on an assignment depends on the assignment's type and whether you can use that action on that type. As an example, the **Update Agent** action applies only to dedicated VDI desktop assignments, while the **Delete** action can be used on all assignment types. For information about creating assignments, see the respective instructions. Usually, but not always, the console will hide an action from view if that action is not applicable to the listed assignments.

The following table provides links to the steps for creating various assignment types.

<table>
<thead>
<tr>
<th>Assignment Type</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| VDI desktop                      | - Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure  
- Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure  
- Pods in Microsoft Azure - Create a VDI Multi-Cloud Assignment |
| Session-based desktop            | Create an RDSH Session Desktop Assignment                                      |
| App Volumes application assignment | Create an App Volumes Assignment                                               |
| Remote application               | Remote Applications - Create a Remote Application Assignment for Remote Applications Provisioned By Horizon Cloud Pods in Microsoft Azure |
| URL redirection customization     | See [Create a URL Redirection Customization and Assign it to Users](#).          |

**Note** When your tenant environment is configured to use Universal Broker for your pods in Microsoft Azure, use of URL redirection customizations is not currently supported.
After locating the assignment you want to work with listed on one of the pages within the console's **Assignments** area, you can invoke an action on that assignment by selecting its corresponding check box and clicking the appropriate displayed action. Some buttons are accessed under the **More** or ... actions.

**Remember** Because the console is dynamic and reflects the workflows that are appropriate for a particular use case and the up-to-the-moment situation in your tenant environment, the action buttons displayed on a console page will vary depending on whether an action is appropriate for the page on which the assignment is listed. As a result, some of the buttons listed below might not be displayed on a particular assignment-related page, or if displayed, might not be actionable for a specific listed assignment.

**Edit**

Clicking this button launches a wizard in which you can change the editable settings in the assignment. The launched wizard is similar to the creation wizard for that assignment type, with read-only fields for those settings that cannot be changed. For detailed descriptions of the fields, see the creation topics at the above documentation links.

For some assignment types, instead of using the **Edit** button, you can click an assignment's name and update the settings from the assignment's summary page.

**Duplicate**

You can use this action to duplicate the selected desktop assignment and create a new one with the same specifications but a new name. The wizard that opens is the same as the creation wizard for the same desktop assignment type as the one you are duplicating.

**Take Offline**

This action applies to floating VDI desktop assignments, dedicated VDI desktop assignments, and URL redirection customization assignments. Clicking this button opens a window in which you can select to take the assignment offline.

The system behavior when you take an assignment offline depends on the selected assignment type.

- For an active URL redirection customization assignment, you use **Take Offline** to turn off the URL redirection behavior defined in the assignment.

- For VDI desktop assignments, you use **Take Offline** to take the assignments off line to perform maintenance actions that would impact incoming connection requests. When you click **Take Offline** for a VDI desktop assignment, the system puts the assignment into offline mode and prevents users from logging in to the assignment's desktops.

**Note** Image update does not start in an offline assignment. Even though you can edit the offline assignment to have it use an updated image, the system does not start the update operation until you bring the assignment back online.

**Update Agent**
On the Assignments page, this action applies only to dedicated VDI desktop assignments. See Update Agent Software for Dedicated VDI Desktop Assignments.

**Bring Online**

Clicking this button opens a window in which you can select to bring an offline assignment back online.

**Delete, Remove**

The console can display this action using one of these two labels. You use this button to delete the selected assignment. Delete an Assignment from Your Horizon Cloud Environment.

**Actions You Can Perform Within a VDI Desktop Assignment's Detailed Pages**

For VDI desktop assignments, you can perform actions specific to those assignment types from within the assignment's detailed pages. To see these detailed pages, locate the assignment within the console's assignment-related pages and click its name. Initially the Summary page is displayed.

**Summary page**

The Summary page displays the VDI desktop assignment's current settings. If the console provides for editing values from this page, you can click the edit-related icon to change those settings that the system allows to be updated for an existing VDI desktop assignment. Some settings cannot be changed on a VDI desktop assignment after it is created, such as its pod.

**Desktops page**

The Desktops page displays the existing desktop VMs in the VDI desktop assignment. As a result of the console's dynamic nature, the actions that are displayed and available to click will depend on the desktop VM's current state and whether the assignment is a floating VDI desktop assignment or a dedicated VDI desktop assignment. As an example, even though the Reset Agent Pairing action is provided for desktops in a dedicated VDI desktop assignment, it is not provided for desktops in a floating VDI desktop assignment.

- For a desktop in floating VDI desktop assignments, you can restart it, power it off (if the desktop is powered on), and log off or disconnect the currently connected user (if any).

**Note** Do not manually delete a desktop in a floating VDI desktop assignment, because the system's power management feature will automatically creates a new desktop VM to take the place of the deleted one. To adjust the number of desktops in a floating VDI desktop assignment, see Resizing a VDI Desktop Assignment in Your Horizon Cloud Environment.

- For a desktop in dedicated VDI desktop assignments, you can restart it, power it on or off (depending on the desktop's current state), log off or disconnect the currently connected user (if any), assign the desktop to a specific user (if the desktop is unassigned), unassign the desktop (if the desktop is assigned to a user), and reset the agent pairing for cases...
where the desktop is powered on but the agent status is not showing as active. Unassigning the desktop removes the mapping of the desktop to that user and makes it available to be mapped to a different user. Resetting the agent pairing repairs the desktop VM's pairing state with Horizon Cloud.

**Note** Do not manually power on a desktop, even if the action is available in the Desktops page. Manually powering on a desktop might conflict with the power management settings that are set in the dedicated VDI desktop assignment. If you manually power on a desktop, unexpected results of other desktops powering off might occur. Instead of powering on a desktop, use the **Restart** action.

### System Activity page

The System Activity page displays activity in the desktop assignment due to system actions, such as powering off desktops to meet the power management schedule.

You can cancel some tasks before they complete by selecting the task in the list and clicking **Cancel Tasks**.

- Before attempting to select a task for cancellation, refresh the view to update the status for the tasks displayed.
- If a task is currently in a state where the system allows you to cancel it, you can select the check box corresponding to that cancellable task.

The table below shows tasks that you can cancel.
<table>
<thead>
<tr>
<th>Task</th>
<th>Cancel When Task is in Queued State</th>
<th>Cancel When Task is in Running State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Farm Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the system has</td>
<td><strong>Note</strong> the following:</td>
</tr>
<tr>
<td></td>
<td>automatically created an expansion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>task for an RDSH farm, the farm must</td>
<td></td>
</tr>
<tr>
<td></td>
<td>be offline before you can cancel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>that task.</td>
<td></td>
</tr>
<tr>
<td>Assignment Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the system has</td>
<td><strong>Note</strong> the following:</td>
</tr>
<tr>
<td></td>
<td>automatically created an expansion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>task for a VDI desktop assignment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and assignment creation or update is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in progress, tasks can be cancelled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>After assignment creation/updation is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>finished, no tasks can be cancelled.</td>
<td></td>
</tr>
<tr>
<td>Convert VM to Image</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you cancel this task,</td>
<td><strong>Note</strong> If you cancel this task,</td>
</tr>
<tr>
<td></td>
<td>and wish to retry it, first confirm</td>
<td>and wish to retry it, first confirm</td>
</tr>
<tr>
<td></td>
<td>that the VM is in a state where it</td>
<td>that the VM is in a state where it</td>
</tr>
<tr>
<td></td>
<td>can be converted. If you are not</td>
<td>can be converted. If you are not</td>
</tr>
<tr>
<td></td>
<td>sure, power off and then power on</td>
<td>sure, power off and then power on</td>
</tr>
<tr>
<td></td>
<td>the VM.</td>
<td>the VM.</td>
</tr>
</tbody>
</table>

**User Activity page**

The User Activity page displays activity in the VDI desktop assignment due to user actions, such as logging on and logging off sessions provided by the assignment.

**Viewing the Assignments Currently Configured in Your Horizon Cloud Environment**

Use **Assignments** in the left hand navigation bar of the Horizon Cloud Administration Console to navigate to various pages in which you can get an overview or detailed view of all the assignments currently configured in your Horizon Cloud environment. You can view the details of individual assignments by clicking the respective assignment. For some assignment types, you
can click on the assignment’s hyperlink name to navigate to where you can perform actions on the individual assets used in that assignment.

**Tip**  The console is dynamic and reflects the workflows and settings that are appropriate for the up-to-the-moment situation in your Horizon Cloud tenant environment. The labels displayed for the console’s assignment-related pages will vary depending on factors such as the tenant’s configured brokering setting, the types of cloud-connected pods in your fleet, the tenant’s regional cloud plane, and features that are based on specific licensing.

<table>
<thead>
<tr>
<th>Assignment Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session-based desktop</td>
<td>View the desktop assignment’s details and optionally click <strong>Edit</strong> to update specific properties. You can click on the link for the associated RDSH farm to navigate to information about the individual desktop sessions, system and user activity in the farm, and perform actions on the farm’s RDSH VMs.</td>
</tr>
<tr>
<td>Remote application</td>
<td>View remote application’s details and optionally click <strong>Edit</strong> to update specific properties. You can click on the link for the associated RDSH farm to navigate to information about the individual sessions, system and user activity in the farm, and perform actions on the farm’s RDSH VMs.</td>
</tr>
<tr>
<td>App Volumes application</td>
<td>View the App Volumes application’s details and optionally use the available actions to update specific properties.</td>
</tr>
<tr>
<td>URL redirection customization</td>
<td>View the customization’s details and optionally click <strong>Edit</strong> to update specific properties.</td>
</tr>
<tr>
<td>VDI desktop</td>
<td>View the desktop assignment’s details and click <strong>Desktops</strong>, <strong>System Activity</strong>, or <strong>User Activity</strong> to view the information on those respective pages or work with the virtual desktops.</td>
</tr>
<tr>
<td></td>
<td>- The Summary page provides definition information about the assignment, the name of an image from which the desktop was created, and a list of the assigned users.</td>
</tr>
<tr>
<td></td>
<td>- The Desktops page provides information about the individual desktops created as part of the desktop assignment. You can also perform actions on an individual desktop, depending on its current state.</td>
</tr>
<tr>
<td></td>
<td>- You can also use the Desktops page to manage the individual desktops in a desktop assignment.</td>
</tr>
<tr>
<td></td>
<td>- The System Activity and User Activity pages provide activity information for that assignment over a specified time.</td>
</tr>
</tbody>
</table>

**Note**  If this VDI desktop assignment was created in a pod in Microsoft Azure that has a pod manifest version lower than 1101, the **License Type** field displays No License even though the assignment has inherited the Windows client license from the image used for this assignment. If you click the **Edit** link, the editing window shows that the Windows client license is being used.

**Edit an Assignment in Your Horizon Cloud Environment**

Using the Horizon Cloud Administration Console, you can edit the assignments that are in your Horizon Cloud environment. Click **Assignments** to navigate to the appropriate page in which to
locate the assignment you want to change. The specific properties you can change depends on the assignment type.

Procedure

1. In the console, click **Assignments**.
2. Select the page that corresponds to the type of assignment you want to change.
3. Select the check box next to the assignment you want to edit and click **Edit**.
   
   The corresponding assignment type's wizard appears.
4. Proceed through the wizard making your changes and click **Submit**.
   
   For instructions on filling in the fields in the wizard, see the documentation topic that describes how to create the type of assignment you are editing. Those topics are listed in **Managing Assignments Provisioned By Horizon Cloud Pods in Microsoft Azure**.

Delete an Assignment from Your Horizon Cloud Environment

You can delete assignments if they are no longer needed. In the Horizon Cloud Administration Console, locate the assignment you want to delete by clicking **Assignments** and using the displayed choices to navigate to the applicable assignments page where that assignment is listed. Then delete that assignment using the **Remove** action or **Delete** action, depending on which action is available in that particular assignments page. The **Delete** action is typically located under the **More** menu (**More > Delete**).

The specific steps for deleting an assignment from your environment vary depending on the assignment type. The table below describes the steps you take on the assignment when you have already navigated to the applicable console page on which that assignment is listed.

<p>| Tip | The console is dynamic and reflects the workflows and settings that are appropriate for the up-to-the-moment situation in your Horizon Cloud tenant environment. The labels displayed for the console's assignment-related pages will vary depending on factors such as the tenant's configured brokering setting, the types of cloud-connected pods in your fleet, the tenant's regional cloud plane, and features that are based on specific licensing. |</p>
<table>
<thead>
<tr>
<th>Assignment Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Floating VDI desktop assignment</td>
<td>Select the assignment and click <strong>More &gt; Delete</strong>. When you confirm the deletion, the system starts deleting the desktop VMs. You can use the Activity page to monitor the deletion process. As the system deletes the desktop VMs, it marks all of the VMs as not brokerable, which prevents new end user connections during the deletion process. For any desktop VMs that have existing end user connections, the console will display a warning to you that those sessions will be terminated. The connected end users will not get a warning in their desktops.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Do not manually delete desktop VMs in a floating VDI desktop assignment from the assignments Desktops tab. When you manually delete a desktop VM from a floating VDI desktop assignment, the system's power management feature automatically creates a new desktop VM to take the place of the deleted one. To remove desktop VMs from a floating VDI desktop assignment, always edit the <strong>Min Desktops</strong> and <strong>Max Desktops</strong> values.</td>
</tr>
</tbody>
</table>
| Dedicated VDI desktop assignment | To delete a dedicated VDI desktop assignment:  
1. Take the assignment offline, using the **Take Offline** button on the Assignments page. Taking the assignment offline prevents the system's power management feature from attempting to automatically create new desktop VMs as you delete instances during the next step.  
2. Delete all of the assignment's desktop VMs. Navigate into the assignment's details page, click the Desktops tab, select all of the desktop VMs, click **More > Delete**, select **Yes** under the **Reduce assignment size** section in the dialog, and confirm the deletion.  
**Note** | A desktop VM with a logged-in user session cannot be deleted. Use the **Log Off** action and then delete the desktop VM.  
3. Use the Activity page to monitor the deletion process and determine when all of the desktop VMs are deleted and all tasks are finished. Do not rely on the console page displaying the assignment's size as zero, because even though all of the desktop VMs might be zero, additional tasks to fully update the system's records might still be running. Those running tasks will prevent you from deleting the assignment from the console page until all of those tasks are done. Deleting all of the desktops can take a long time depending on how many there are.  
4. When all of the desktop VMs are deleted and the assignment's capacity is reported as zero, then you can delete the assignment by selecting it and clicking **More > Delete**. |
| Session desktop assignment | Select the assignment and click **More > Delete**. Because session desktop assignments are for entitling users to connect to the RDSH VMs in a farm, no VMs are actually deleted when you delete this assignment type. The assignment record is removed from the system. |
| - App Volumes applications assignment  
- Remote applications assignment  
- URL redirection customization assignment | Select the assignment and use the **Remove** or **Delete** action, depending on which one the console provides for that assignments-listing page. |
Resizing a VDI Desktop Assignment in Your Horizon Cloud Environment

When you create VDI desktop assignments, you assign an initial capacity of VDI desktop instances using the **Max Desktops** value. As the user population changes, you might need to expand or shrink the VDI desktop assignment.

You would expand a VDI desktop assignment by adding additional desktop VMs to meet your end user needs.

You would shrink a VDI desktop assignment to free up capacity in your Microsoft Azure cloud environment so you can use that capacity for something else. When your end users no longer need to access the desktop VMs from a particular VDI desktop assignment, you might want to free up that unneeded capacity.

**Important**  For a dedicated VDI desktop assignment, to reduce its capacity, you must delete the desktop VMs from the Desktops tab in the assignment's details page. You cannot shrink an existing dedicated VDI desktop assignment by decreasing the **Max Desktops** value.

Expanding a VDI Desktop Assignment

You increase the capacity of a VDI desktop assignment by adding VDI desktop VMs to the VDI desktop assignment. You add desktop VMs by editing the VDI desktop assignment, floating or dedicated, to increase the **Max Desktops** value. See **Edit an Assignment in Your Horizon Cloud Environment** for how to edit a VDI desktop assignment using the Horizon Cloud Administration Console. You can expand an assignment up to the scale limits for VDI desktops in a pod.

When you submit the change, the system starts creating the new desktop VMs to match the new larger **Max Desktops** value. You can use the VDI desktop assignment's Desktops and Activity tabs to monitor the process. For details about those tabs, see **Viewing the Assignments Currently Configured in Your Horizon Cloud Environment**.

Shrinking a VDI Desktop Assignment

The method to reduce capacity in a VDI desktop assignment varies depending on which type it is.
<table>
<thead>
<tr>
<th>VDI Desktop Assignment Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Floating                   | To reduce the capacity of a floating VDI desktop assignment, edit the assignment and change **Max Desktops** value to a new smaller value. When you submit the change, the system starts to delete not-in-use VDI desktop VMs until the total number in the assignment matches the new value. If the new requested number is smaller than the number of not-in-use desktop VMs due to currently logged-in end users or because end users have disconnected sessions to the desktop VMs, the system prevents the process and an error message displays in the console. To shrink the assignment in this situation, you can use one, or a combination, of the following methods:  
  - Re-edit the assignment and use a different **Max Desktops** value to remove any currently not-in-use desktops.  
  - Wait for, or force, the users to fully log off of the in-use desktops before you edit the assignment to reduce the **Max Desktops** value. you can force a log off from the assignment’s Desktops tab by selecting the desktop and clicking **Log Off**. |
| Dedicated                  | Because the desktop instances in a dedicated VDI desktop assignment are mapped to specific end users when they first connect to a desktop from the assignment, the system prevents reducing the capacity of the assignment by changing the **Max Desktops** value. The reason is because reducing that number would not inform the system about which specific desktop instances to delete out of the total number. To reduce the size of the dedicated VDI desktop assignment, you must explicitly delete desktops from the assignment’s Desktops tab. On that tab, select the check box next to the desktops you want to delete, click **Delete**, and confirm the deletion. You can delete both VDI desktops that are assigned to users and unassigned ones.  
1. Take the dedicated VDI desktop assignment offline using the Assignment page’s **Take Offline** button. Taking the assignment offline prevents the system’s power management feature from attempting to automatically create new desktop VMs as you delete some.  
2. Select the check box next to the desktops you want to delete, click **Delete**, select **Yes** under ‘Reduce assignment size’ in the dialog, and confirm the deletion.  
3. When the system has finished deleting the desktops, bring the assignment back online again using the **Bring Online** button.  
After the system has deleted the selected VDI desktops, the assignment’s size automatically decreases down to the number that matches the original **Max Desktops** value minus the ones you deleted.  
**Note** You cannot delete a desktop that the Desktops tab indicates has an active or disconnected session. That end user must be fully logged off before you can delete that desktop.  
If you want to keep the same overall capacity of the dedicated VDI desktop assignment, but want to have a different user consume a desktop that is already mapped to a user, on the assignment’s Desktops tab, you can select the desktop and select **Unassign**. Then you can explicitly assign that desktop to another user. |

**Prevent Deletions or Allow Deletions for a Dedicated Desktop Assignment**

You can prevent deletions or allow deletions of VMs for a dedicated desktop assignment using a setting on the **Assignments** page.
The Prevent Deletions option causes the system to deny all requests to delete a desktop VM from a dedicated desktop assignment. You can also set limits on VM deletions using the following options.

- **Deletion Protection** - For more information, see Customizable General Settings for Your Horizon Cloud Tenant Environment.
- **Max Desktop Deletions** - You can set this option when creating or editing a dedicated desktop assignment. The option is described in Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure.

---

**Note** If you specify a new image for a dedicated desktop assignment that has deletion prevention enabled, the system disables deletion prevention and changes deletion settings so that all unassigned desktop VMs can be rebuilt with the new image.

---

### Prevent Deletions

1. On the Assignments page, select the check box for the assignment. Options for the assignment are enabled.
2. Click More > Prevent Deletions. A dialog box displays asking you to confirm that you want to prevent deletions for the assignment.
3. Click Continue. A message displays indicating that the operation was successful.

### Allow Deletions

1. On the Assignments page, select the check box for the assignment. Options for the assignment are enabled.
2. Click More > Allow Deletions. A dialog box displays asking you to confirm that you want to allow deletions for the assignment.
3. Click Continue. A message displays indicating that the operation was successful.

### About Network Security Groups and Your VDI Desktops

For every Horizon Cloud pod deployed into your Microsoft Azure cloud, a network security group (NSG) is also created in the pod's resource group to act as a template. You can use this template to ensure you have opened those additional ports that you might need for the VDI desktops provided by your VDI desktop assignments.
In Microsoft Azure, a network security group (NSG) governs the network traffic to the resources connected to Azure Virtual Networks (VNet). An NSG defines the security rules that allow or deny that network traffic. For more detailed information about how NSGs filter network traffic, see the Microsoft Azure documentation topic Filter network traffic with network security groups.

When a Horizon Cloud pod is deployed into Microsoft Azure, an NSG named vmw-hcs-podID-nsg-template is created in the pod’s same resource group named vmw-hcs-podID, where podID is the pod’s ID. You can obtain the pod’s ID from the pod’s details page, navigating from the Capacity page in the .

By default, the pod’s template NSG is configured with no outbound security rules and with the following inbound security rules. These default inbound security rules support your end-user clients' access to their VDI desktops using Blast and PCOIP and USB redirection.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Name</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>AllowBlastUdpIn</td>
<td>22443</td>
<td>UDP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>1100</td>
<td>AllowBlastTcpIn</td>
<td>22443</td>
<td>TCP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>1200</td>
<td>AllowPcoipTcpIn</td>
<td>4172</td>
<td>TCP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>1300</td>
<td>AllowPcoipUdpIn</td>
<td>4172</td>
<td>UDP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>1400</td>
<td>AllowTcpSideChannelIn</td>
<td>9427</td>
<td>TCP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>1500</td>
<td>AllowUsbRedirectionIn</td>
<td>32111</td>
<td>TCP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
</tbody>
</table>

In addition to this template NSG, when a VDI desktop assignment is created, the system creates an NSG for that assignment’s pool of desktops by copying the template NSG. Every VDI desktop assignment’s pool has its own NSG that is a copy from the template NSG. A pool’s NSG is assigned to the NICs of that pool’s VDI desktop virtual machines (VMs). By default, every VDI desktop pool uses the same default security rules as configured in the pod’s template NSG.

You can modify both the template NSG and the per-VDI-desktop-assignment NSGs. For example, if you have an application in a VDI desktop that you know needs an additional port opened for that application, you would modify the corresponding VDI desktop assignment pool's NSG to allow network traffic on that port. If you are planning to create multiple VDI desktop assignments that need the same port opened, a simple way to support that scenario is to edit the template NSG prior to creating the VDI desktop assignments.

**Important** When planning to modify the base template, make a copy before modifying it. The copy can be a backup in case you need to revert back to the original default settings.

**Updating the Agent-Related Software Used by Horizon Cloud**

Horizon Cloud communicates with agent-related software that is installed in the virtual machines (VMs) that are involved in the system operations for base image VMs, published images, RDSH farms, and VDI desktop assignments. VMware updates the agent-related software periodically to
include new features and bug fixes. As appropriate for your environment, use the steps in the topics below to update the agent-related software.

**Important** The system’s update-manager job runs once a day to evaluate whether an image or assignment is a candidate for updating its agent-related software. If the agent-related software changes for that image or assignment in between the times the daily job is run, the status in the Horizon Cloud administrative console can be out of sync until the next time the daily job is run. This situation primarily occurs when you do a manual update to the latest agent software, either by running the Horizon Agents Installer manually on the virtual machine to update the agent software or by using a GPO. As an example:

1. The update-manager job runs at its daily scheduled time and indicates in the console that an agent update is available on an image.
2. You manually update the desktop instances in a VDI desktop assignment to the latest agent using a GPO.

Even though the agent-related software on the desktop instances are running the latest software, the console will still show the blue dot on the image, indicating an agent update is available until the next scheduled run of the update-manager job.

### About the VMware Dynamic Environment Manager Agent Software

Starting with the July 2019 Horizon Cloud release, installation of the VMware Dynamic Environment Manager agent is incorporated into the Horizon Agents Installer. The Horizon Agents Installer is the software package that:

- Installs the agent-related software in a new image VM, when you run the Import Virtual Machine workflow or manually create and import an image VM. When you [Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it with Horizon Cloud](https://www.vmware.com/horizon/azure.html), the Horizon Agents Installer runs behind the scenes to install the agents. When you [Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud](https://www.vmware.com/horizon/azure-manual-import.html), you download and run the Horizon Agents Installer as part of those steps.

- Updates the agent-related software in existing image VMs, and in dedicated VDI desktop assignments, when you run the Update Agent workflow. The Horizon Agents Installer runs behind the scenes to update the installed agents.

After you run the Update Agent workflow on an image VM or on the desktop VMs in a dedicated VDI desktop assignment, the install path of the VMware Dynamic Environment Manager files in the updated VMs depends on whether the original agent installation into the VM was at version 19.2 or later prior to running the Update Agent workflow.

**When the base image VM was originally created using the Import Desktop workflow**
In this case, the VMware Dynamic Environment Manager agent was installed automatically by default. The specific install file path depends on whether the base image VM was created starting with the 19.2 version of the agent software:

- If the image VM was created new in a pod of manifest 1493 or later, the VMware Dynamic Environment Manager install file path is `C:\Program Files\VMware\Horizon Agents\User Environment`. When you subsequently run the Update Agent workflow on that VM, the file path remains as `C:\Program Files\VMware\Horizon Agents\User Environment`.

- If the image VM was created in a pod of manifest earlier than 1493, the VMware Dynamic Environment Manager install file path is `C:\Program Files\Immidio\Flex Profiles`. When you subsequently run the Update Agent workflow on that VM, the file path remains as `C:\Program Files\Immidio\Flex Profiles`.

When the base image VM was originally created manually in Microsoft Azure

The VMware Dynamic Environment Manager install file path depends on how you installed the VMware Dynamic Environment Manager agent in that manually created VM:

- If you installed the VMware Dynamic Environment Manager agent using the Horizon Agents Installer version 19.2, the VMware Dynamic Environment Manager install file path is `C:\Program Files\VMware\Horizon Agents\User Environment`. When you subsequently run the Update Agent workflow on that VM, the file path remains as `C:\Program Files\VMware\Horizon Agents\User Environment`.

- If you installed the VMware Dynamic Environment Manager agent using the separate stand-alone VMware Dynamic Environment Manager installer, the VMware Dynamic Environment Manager install file path is `C:\Program Files\Immidio\Flex Profiles`. When you subsequently run the Update Agent workflow on that VM, the file path remains as `C:\Program Files\Immidio\Flex Profiles`.

Also, when the base image VM was originally created manually in Microsoft Azure and you did not install the VMware Dynamic Environment Manager agent at that time, if you want to subsequently install the agent during the Update Agent workflow, use the command-line argument `ADDLOCAL=UEM` in the Agent Update wizard’s Command Line step.

Update Agent Software for RDSH Images in Horizon Cloud

To update the agent-related software that is installed on RDSH images that are currently in use by farms, you first use the Images page’s Update Agent action. Then you edit the farms to use those updated images.

At a high-level, the system’s agent update capability works as follows:

- The system makes regular contact with the VMware CDS (Component Download Service) software distribution network to see if a new version of the Horizon Agents Installer is available. If so, the system automatically downloads that version to your Horizon Cloud pods.
After a new version is downloaded, the Images page reflects that an update is available. A visual indicator is displayed for those images that have the agent-related software at a level prior to the new version.

During the agent update process:

- The system powers on the selected image's virtual machine (VM), clones a duplicate VM from the powered-on image, and then runs the convert-to-image process on the selected image to return it to its original published state. During this part of the process, the selected image's status on the Images page changes from Published to In Transition.

- When the duplicate VM exists, the system powers it on, installs the agent-related software using the newer update version that was selected in the wizard, and then runs the convert-to-image process on that duplicate to publish it.

At the end of the agent update process, the Images page lists both the originally selected image and its duplicate, where the duplicate image is the one with the updated agent software installed in it.

**Important** At the end of the agent update process, the RDSH image you selected when you clicked Update Agent ends up in the same state it was in when the process started, with its original agent version level. The new duplicate image gets the agent software at the selected update level.

The agent update process results in a new assignable image that is a duplicate of the original, with the agent-related software updated to the version you specify in the wizard. The agent update workflow automatically clones the original image to make a new VM, installs the agent-related software of the specified level into that VM, and then converts that VM to make it an assignable (published) image. The system bases the name of the new image on the original image's name appended with a dash and a number. For example, if the original image's name is SalesGold, the agent update process results in an image such as SalesGold-2. At the end of the process, both images are listed on the Images page.

The screenshot below illustrates the two images listed on the Images page after running the agent update process on the image named pat2016 and selecting the most recently available update version. Because the original image is unchanged at the end of the process, the blue dot remains displayed next to it. The pat2016-1 image contains the agent software are the update level, and because there are no newer update versions in the system yet, the pat2016-1 image has no blue dot next to it.
Prerequisites

Procedure

1. Navigate to the Images page by clicking Inventory > Images.

   On the Images page, a blue dot appears next to the name of any image for which an update applies. If you hover over a blue dot, a popup displays indicating the new version of the Horizon Agents Installer available for that image.

   The screenshot below illustrates that an agent update is available for the image named pat2016.

   ![Images screenshot](image1.png)

   Hover your cursor over that blue dot to see what updates are available.

2. Select the check box next to the image you want to update.

3. Click Update Agent.

   The Agent Update wizard appears.
4 In the Software step, select the update version you want to use from the drop-down list and click Next.

5 (Optional) In the Command Line step, add any command-line options that might be relevant for this update on the image.

The wizard displays a message that indicates whether command-line options are available for the specified update.

6 Click Submit.

- A message displays at the top of the page indicating that the update has started.
- The system creates a clone virtual machine (VM) of the original image and then updates the agent-related components on that clone image. After the clone image is updated, the system runs the convert-to-desktop process to turn it into a published image.

You can view the progress of the update task by selecting Monitor > Activity. If the task is not completed successfully within 24 hours, it is shown in failure status.

What to do next

- Update the farms that are using the original image by editing the farms to use the new duplicate image, the image which now has the updated agent software on it. Use the Edit action on the farm, then in the window that opens, locate the Image field, select the new duplicate image, and save.
- When you have updated the farms that were using the original image and can determine the original image is no longer needed by your organization, use the Images page to delete the original image. Deleting the original image is a best practice, to prevent other administrators in your organization from using an image that has down-level agents.

Update Agent Software for Dedicated VDI Desktop Assignments

To update the agent-related software that is installed in the desktop VMs that are used by a dedicated VDI desktop assignment, first update the image the assignment is using, then use the Assignments page's Update Agent action. Updating the image updates the unassigned desktops in the dedicated VDI assignment. This process is the same as it is for floating VDI desktop
assignments. For a dedicated VDI desktop assignment, you then update the assignment on the Assignments page to update the assigned desktops in the assignment.

Procedure

1. If you have a large number of unassigned desktops in the assignment, update agent software for the image the assignment is using and edit the assignment to use the updated image, as described in Update Agent Software for Images Used by Dedicated VDI Desktop Assignments.

   This allows you to avoid unnecessary and time-consuming agent updates for unassigned desktops. It is possible to update all desktops using the second step below, but it is unnecessary to use that process for unassigned desktops if you are planning to update the image soon.

   **Important** When you have finished updating the image and editing the assignment to use the updated image, you must confirm that all unassigned desktops have refreshed and are using the updated image before you proceed.

2. Update the agent for the assignment on the Assignments page, as described in Update Agent Software on the Assignments Page for Dedicated VDI Desktop Assignments.

**Update Agent Software for Images Used by Dedicated VDI Desktop Assignments**

To update agent-related software for a dedicated VDI desktop assignment, the first task is to update the software installed on the image used by the assignment and edit the dedicated VDI desktop assignment to use that updated image. This procedure updates the unassigned desktops in the assignment.

At a high level, the system's agent update capability works as follows:

- The system makes regular contact with the VMware CDS (Component Download Service) software distribution network to see if a new version of the Horizon Agents Installer is available. If so, the system downloads that version to your Horizon Cloud pods.

- After a new version is downloaded, the Images page reflects that an update is available. A visual indicator is displayed for those images that have the agent-related software at a level earlier than the new version.

- During the agent update process:
  - The system powers on the selected image, clones a duplicate virtual machine (VM) from the powered-on image, and then runs the convert-to-image process on the selected image to return it to its original published state. During this part of the process, the image's status on the Images page changes from Published to In Transition.
  
  - When the duplicate VM exists, the system powers it on, installs the agent-related software using the newer update version that was selected in the wizard, and then runs the convert-to-image process on that duplicate to publish it.
At the end of the agent update process, the Images page lists both the original image and its duplicate, where the duplicate image has the updated agent software installed in it.

**Important** At the end of the agent update process, the image you selected when you clicked Update Agent ends up in the same state it was in when the process started, with its original agent version level. The new duplicate image gets the agent software at the selected update level.

The agent update process results in a new assignable image that is a duplicate of the original, with the agent-related software updated to the version you specify in the wizard. The agent update workflow automatically clones the original image to make a new VM, installs the agent-related software of the specified level into that VM, and then converts that VM to make it an assignable (published) image. The system bases the name of the new image on the original image's name appended with a dash and a number. For example, if the original image's name is SalesGold, the agent update process results in an image such as SalesGold-2. At the end of the process, both images are listed on the Images page.

The following screenshot illustrates the two images listed on the Images page after running the agent update process on one image and selecting the most recently available update version. Because the original image is unchanged at the end of the process, the blue dot remains displayed next to it. The other image contains the agent software at the update level, and because there are no newer update versions in the system yet, that image has no blue dot next to it.

---

**Prerequisites**

**Procedure**

1. Navigate to the Images page by clicking **Inventory > Images**.

On the Images page, a blue dot appears next to the name of any image for which an update applies. If you place your pointer on a blue dot, a pop-up window displays indicating the new version of the Horizon Agents Installer available for that image.
The screenshot below illustrates that an agent update is available for the image named la24win10N.

![Image](image.png)

Place your pointer on that blue dot to see what updates are available.

2 Select the check box next to the image you want to update.

3 Click **Update Agent**.

   The Agent Update wizard appears.

4 In the Software step, select the update version you want to use from the drop-down menu and click **Next**.

   ![Agent Update](agent-update.png)

5 (Optional) In the Command Line step, add any command-line options that might be relevant for this update on the image.

   The wizard displays a message that indicates whether command-line options are available for the specified update.
6  Click **Submit**.

- A message displays at the top of the page indicating that the update has started.
- The system creates a clone virtual machine (VM) of the original image and then updates the agent-related components on that clone image. After the clone image is updated, the system runs the convert-to-desktop process to turn it into a published image.

You can view the progress of the update task by selecting **Monitor > Activity**. If the task is not completed successfully within 24 hours, it is shown in failure status.

7  Perform any desired tests on the updated image.

8  Update the dedicated VDI desktop assignments that are using the original image by editing the assignments to use the new duplicate image, the image which now has the updated agent software on it. Use the **Edit** action on the assignment, then in the window that opens, locate the **Image** field, select the new duplicate image, and save.

For more information about editing assignments, see **Edit an Assignment in Your Horizon Cloud Environment**.

9  Confirm that all unassigned desktops are now linked to the updated image.

10  When you have updated the assignments that were using the original image and can determine the original image is no longer needed by your organization, use the Images page to delete the original image. Deleting the original image is a best practice, to prevent other administrators in your organization from using an image that has down-level agents.

**What to do next**

Complete the agent software update for the assignment using the Update Agent action on the Assignments page. See **Update Agent Software on the Assignments Page for Dedicated VDI Desktop Assignments**.

**Important** You must perform the agent software update on the Assignments page to complete the update for the dedicated VDI desktop assignment.

**Update Agent Software on the Assignments Page for Dedicated VDI Desktop Assignments**

After you have updated the image used by a dedicated VDI desktop assignment, you can update the assignment on the Assignments page to update the assigned desktops in the assignment.

For a high-level description of how the agent update capability works in Horizon Cloud for dedicated VDI desktop assignments, see **How the Agent Update Feature Works for Dedicated VDI Desktop Assignments**.

**Important** These steps are for dedicated VDI desktop assignments. These steps do not apply to floating VDI desktop assignments. For information on updating agents in your floating VDI desktop assignments, see **Update Agent Software for Images Used by Floating VDI Desktop Assignments**.
Prerequisites

**Caution** While the update agent operation is in progress, you must ensure that you have no other planned activities that might cause any of the assignment's desktop VMs to experience a power change operation. For example, notify your other administrators to avoid manually powering off or on one of these desktop VMs, and ensure that any power management schedules configured in this assignment will not cause the desktops to power on or off while the update agent tasks are running. If a desktop VM experiences a power-change operation while the system is running its agent update tasks on the VM, unexpected results can occur and leave that desktop VM in a state that requires manual recovery.

A best practice is to edit the assignment and remove any configured power management schedules to eliminate the chance a power-change operation will occur while the agent update tasks are running.

Procedure

1. Navigate to the Assignments page by clicking **Assign**.

   On the Assignments page, a blue dot appears next to the name of any dedicated VDI desktop assignment for which an update applies. If you point at a blue dot, a pop-up box displays indicating the new version of the Horizon Agents Installer available for that assignment.

   The following screenshot illustrates that an agent update is available for the assignment named *la24dedsales*.

   [Image of Assignments page with blue dot indicating update available]

   Hold your pointer over that blue dot to see what updates are available.

2. Select the check box next to the image you want to update.

3. Click **Update Agent**.

   The Agent Update wizard appears.
4 In the Software step, select the update version you want to use from the drop-down list.

5 (Required) In the **Available VMs to Users** field, specify the percentage of desktop VMs in the assignment that you want powered on and available to end users during the update process.

**Important** If you do not need desktops available, type a zero (0). You must specify a value for **Available VMs to Users**, even when you do not care about having desktop VMs available to users during the update process.

This value determines how many desktop VMs will be accessible to users over the time the system performs the update on the assignment. This setting is useful for a desktop assignment with a small number of desktops, less than 30 desktops or a few multiples of 30 (like 60 or 90), because it can ensure a higher percentage of a small-sized pool is available as the system goes through updating the desktops. For examples, see [How the Agent Update Feature Works for Dedicated VDI Desktop Assignments](#).

Setting a higher availability percentage results in an adjustment to the number of desktops in the batch of currently updating VMs. When updating the assignment, the system updates a batch of VMs in parallel. By default, the system uses 30 VMs for each batch until the remaining number of VMs to update is less than 30. At that point, the final batch is for those remaining VMs. Because it takes approximately 30 minutes to fully update a VM, even though a set of VMs is getting updated in parallel, that set of update-in-progress VMs is unavailable for that amount of time.

This option has less effect when the assignment has many desktops, where the system's maximum default 30 VMs per batch is a small percentage of the assignment's total number of desktops.
6 (Optional) To have the system skip those desktops that have logged-in users, set the Skip VMs with Logged-In User toggle to Yes.

When that toggle is set to Yes, the Retry Skipped VMs toggle appears.

![Skip Disconnected and Active Sessions](image)

7 (Optional) To have the system automatically retry any of skipped VMs, set the Retry Skipped VMs toggle to Yes.

When that toggle is set to Yes, the Job Timeout field appears.

![Retry Skipped VMs:](image)

8 (Optional) In the Job Timeout field, specify the time period over which you want the system to continue automatically trying to update the skipped VMs.

The Job Timeout field sets the number of minutes that the system retries updating the skipped VMs. Every 30 minutes, the system tries to update the skipped VMs until it reaches the end of this time period or until all of the assignment's desktop VMs have been updated.

You can enter a value that ranges from 120 minutes (2 hours) to 1440 minutes (24 hours). The default value is 720 minutes (12 hours).

**Note** VMs that encounter an error during the update process are not retried. For a failed update, the VM rolls back to the agent version that it had before the update process started.

9 Click Next.

10 (Optional) In the Command Line step, add any command-line options that might be relevant for this update on the image.

The wizard displays a message that indicates whether command-line options are available for the specified update.

11 Click Submit.

Results

- A message displays at the top of the page indicating that the update has started.
- The system updates the agent-related components on the desktop VMs in the dedicated VDI desktop assignment.
You can view the progress of the update task by selecting **Monitor > Activity**.

**How the Agent Update Feature Works for Dedicated VDI Desktop Assignments**

This topic is a high-level description of how the agent update capability works in Horizon Cloud for dedicated VDI desktop assignments.

The system makes regular contact with the VMware CDS (Component Download Service) software distribution network to see if a new version of the Horizon Agents Installer is available. If so, the system automatically downloads that version to your Horizon Cloud pods.

After a new version is downloaded, the administrative console's page on which that assignment is listed reflects that an update is available. A visual indicator is displayed for those dedicated VDI desktop assignments that have the agent-related software at a level prior to the new version.

You initiate the update by selecting the dedicated VDI assignment and starting the agent update wizard as described in the steps in **Update Agent Software for Dedicated VDI Desktop Assignments**. Besides selecting the version to use for the update, you can specify the following options.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Available VMs to Users         | Use this field to specify a percentage of the assignment’s VMs to keep available for users during the update. This option is useful for a small-sized desktop assignment, with desktops fewer than 30 or a couple of multiples of 30 (like 60 or 90).  
Because the system updates the desktops in batches of 30 by default, if the assignment has 30 or less desktops, all the desktops will start the update process at the same time. If all the desktops are actively in the update process, none of the entitled users can make new connections to the desktops until the update process has completed. The agent update process takes approximately 30 minutes until the updated desktop is ready for an end-user connection. Similarly, in the case where the desktop assignment's desktops are around 60, the default batch of 30 results in 50% of the desktops being unavailable. Therefore, you can use this field to ensure that a greater percentage of a small-sized pool is available as the system goes through and updates the desktops. Setting a higher availability percentage results in an adjustment to the number of desktops in each batch of updating VMs. For an assignment with many desktops, this option has less effect because the system's maximum default 30 VMs per batch is a small percentage of the assignment's total number of desktops. |
| Skip VMs with Logged-In User   | Have the system skip updating VMs that have a logged-in user, a session that is either active or disconnected. This setting avoids the system's default behavior of forcing end users off their desktop when the update process starts on that desktop. |
| Retry Skipped VMs and Job Timeout | When you have the system skip updating VMs that have a logged-in user, you can optionally specify whether to have the system automatically retry updating any skipped VMs. In this case, after the system has gone through the assignment's desktop VMs and updated those VMs without logged-in users, the system:  
1 Checks the ones that it initially skipped to see if those VMs have logged-in users.  
2 Updates any of the skipped VMs which have no logged-in users.  
3 Periodically repeats steps 1 and 2 until the time specified in the Job Timeout field has elapsed.  
If you do not have the system automatically retry the skipped VMs, you can manually take care of those VMs later.  
**Important** VMs that encounter an error during the update process are not retried. For a failed update, the VM rolls back to the agent version that it had before the update process started. |

After you submit the update task in the wizard's last step, the system begins updating the desktops in the dedicated VDI desktop assignment. When updating the assignment, the system updates a batch of VMs in parallel. By default, the system uses 30 VMs for each batch until the remaining number of VMs to update is less than 30. At that point, that final set is for updating those remaining VMs. Because it takes approximately 30 minutes to fully update a VM, even though a set of VMs is getting updated in parallel, that set of update-in-progress VMs is
unavailable for that stretch of time. The number of in-progress VMs depends on whether you specified to have a percentage of the VMs to be kept available during the update. When you set an availability percentage, the system adjusts the set of in-progress VMs to meet the availability percentage. The following table illustrates some examples.

<table>
<thead>
<tr>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available VMs to Users not set (= 0%)</td>
<td>When you do not set an availability percentage, the availability percentage is zero and the run-time batch size is 30 VMs, the default. If the assignment has 30 or fewer desktops, all desktops in the assignment are updated together in one batch.</td>
</tr>
</tbody>
</table>
| Assignment has 20 desktops and Available VMs to Users= 80% | With an assignment of 20 desktops, and you want 80% of them to be kept available, that means the system must keep 16 available at any time. In this case, the system:
1. First updates a batch of 4 VMs (20 minus 16).
2. Counts the 4 updated VMs plus 12 not-yet-updated ones to keep 16 available, and updates a second batch of 4 VMs.
3. At this point, 8 VMs are updated and 12 are not-yet-updated. The system continues updating the not-yet-updated VMs in batches of 4. With each subsequent batch, the ones kept available are a mixture of updated VMs and not-yet-updated VMs. |
| Assignment has 100 desktops and Available VMs to Users= 80% | With an assignment of 100 desktops, and you want 80% of them to be kept available, that means the system must keep 80 available at any time. In this case, the system:
1. First updates a batch of 20 VMs (100 minus 80).
2. Counts the 20 updated VMs plus 60 not-yet-updated ones to keep 80 available, and updates a second batch of 20 VMs.
3. At this point, 40 VMs are updated and 60 are not-yet-updated. The system continues updating the not-yet-updated VMs in batches of 20. |
| Assignment has 100 desktops and Available VMs to Users= 25% | With an assignment of 100 desktops, and you want 25% of them to be kept available, that leaves 75 VMs that can be updated first. In this case, the system:
1. First updates a batch of 30 VMs, which is its default batch size, leaving 70 not-yet-updated.
2. Out of the 70 not-yet-updated, updates a second batch of 30 VMs out of that, to make 60 VMs updated and 40 VMs not-yet-updated from the 100 total number of desktops.
3. Now that 60 VMs are updated, 25 of those updated VMs can meet the 25% availability setting. So the system uses its default 30 VM batch size and updates 30 VMs out of the remaining 40 not-yet-updated VMs.
4. The system updates the remaining VMs, with 10 in this final batch. |

At the end of the agent update process, the assignment's summary page lists the version of the Horizon Agents Installer that is in effect.

During the time the system is updating the desktops, the desktops' end users encounter the following behaviors:

- If a desktop has an active session and you did not specify skipping VM with active users, that user is warned five minutes before the update occurs. This five-minute warning is to give the user time to save any in-progress work.
If a user attempts to log in to a desktop that is being updated, the login is unsuccessful and the user receives a message that the desktop is not yet available.

You can view the progress of the update task by selecting **Monitor > Activity**. The task description indicates the update being performed and the assignment on which it is being performed. If the task is not completed successfully within 24 hours, and the retry and job timeout options are not in effect, the update task is shown in failure status.

If any VMs are skipped in the update task, the update task has Partial Success status on the Activity page. In the Activity page, you can see how many VMs are skipped in the update task.

If the Activity page shows a number of skipped VMs at the end of the update task even though the retry option was set to **Yes**, either the **Job Timeout** value was not long enough for the system to get to all of the skipped VMs or the end users never logged out of those VMs.

VMs can also be skipped with preflight check errors such as “Windows updates in-progress”, “low disk space”, and "reboot pending on machine".

For VMs that were skipped for any reason, the administrator can retry the agent update later.

**Update Agent Software for Images Used by Floating VDI Desktop Assignments**

To update the agent-related software that is installed on the images that are used by floating VDI desktop assignments, you first use the Images page's **Update Agent** action. Then you edit the floating VDI desktop assignments to use those updated images.

At a high-level, the system's agent update capability works as follows:

- The system makes regular contact with the VMware CDS (Component Download Service) software distribution network to see if a new version of the Horizon Agents Installer is available. If so, the system automatically downloads that version to your Horizon Cloud pods.

- After a new version is downloaded, the Images page reflects that an update is available. A visual indicator is displayed for those images that have the agent-related software at a level prior to the new version.

- During the agent update process:
  - The system powers on the selected image, clones a duplicate virtual machine (VM) from the powered-on image, and then runs the convert-to-image process on the selected image to return it to its original published state. During this part of the process, the image's status on the Images page changes from Published to In Transition.
  - When the duplicate VM exists, the system powers it on, installs the agent-related software using the newer update version that was selected in the wizard, and then runs the convert-to-image process on that duplicate to publish it.
At the end of the agent update process, the Images page lists both the original image and its duplicate, where the duplicate image has the updated agent software installed in it.

**Important** At the end of the agent update process, the image you selected when you clicked **Update Agent** ends up in the same state it was in when the process started, with its original agent version level. The new duplicate image gets the agent software at the selected update level.

The agent update process results in a new assignable image that is a duplicate of the original, with the agent-related software updated to the version you specify in the wizard. The agent update workflow automatically clones the original image to make a new VM, installs the agent-related software of the specified level into that VM, and then converts that VM to make it an assignable (published) image. The system bases the name of the new image on the original image's name appended with a dash and a number. For example, if the original image's name is SalesGold, the agent update process results in an image such as SalesGold-2. At the end of the process, both images are listed on the Images page.

The screenshot below illustrates the two images listed on the Images page after running the agent update process on one image and selecting the most recently available update version. Because the original image is unchanged at the end of the process, the blue dot remains displayed next to it. The other image contains the agent software at the update level, and because there are no newer update versions in the system yet, that image has no blue dot next to it.

**Prerequisites**

**Procedure**

1. Navigate to the Images page by clicking **Inventory > Images**.

On the Images page, a blue dot appears next to the name of any image for which an update applies. If you hover over a blue dot, a popup displays indicating the new version of the Horizon Agents Installer available for that image.
The screenshot below illustrates that an agent update is available for the image named la24win10N.

Hover your cursor over that blue dot to see what updates are available.

2. Select the check box next to the image you want to update.

3. Click **Update Agent**.

The Agent Update wizard appears.

4. In the Software step, select the update version you want to use from the drop-down list and click **Next**.

5. (Optional) In the Command Line step, add any command-line options that might be relevant for this update on the image.

The wizard displays a message that indicates whether command-line options are available for the specified update.
6 Click **Submit**.

- A message displays at the top of the page indicating that the update has started.
- The system creates a clone virtual machine (VM) of the original image and then updates the agent-related components on that clone image. After the clone image is updated, the system runs the convert-to-desktop process to turn it into a published image.

You can view the progress of the update task by selecting **Monitor > Activity**. If the task is not completed successfully within 24 hours, it is shown in failure status.

**What to do next**

- Update the floating VDI desktop assignments that are using the original image by editing the assignments to use the new duplicate image, the image which now has the updated agent software on it. Use the **Edit** action on the assignment, then in the window that opens, locate the **Image** field, select the new duplicate image, and save.
- If you have any dedicated VDI desktop assignments that are using the original image and you want to move them to the same agent level, update the agent on those assignments following the steps in **Update Agent Software for Dedicated VDI Desktop Assignments**.

  **Important** Even though you can edit a dedicated VDI desktop assignment to use the new duplicate image, only unassigned desktop VMs will be updated in that method. If you want to update agents on all desktop VMs in a dedicated VDI desktop assignment, use the steps in **Update Agent Software for Dedicated VDI Desktop Assignments**.

- When you have updated the assignments that were using the original image and can determine the original image is no longer needed by your organization, use the Images page to delete the original image. Deleting the original image is a best practice, to prevent other administrators in your organization from using an image that has down-level agents.

**Managing Your Horizon Cloud Pods Deployed in Microsoft Azure**

After your customer account has its first cloud-connected pod and you have fully registered the Active Directory domain, you can deploy additional pods and work with your pod fleet using the Horizon Cloud Administration Console. For pods deployed in Microsoft Azure, you can perform tasks to manage them, such as monitoring their capacity limits and updating their stored subscription information or deleting unused stored subscription information, as needed. You can also edit a pod to change its settings, including its gateway configuration settings.

You primarily use the Capacity page to work with your pods, as well as the pods' individual detail pages. You navigate to a pod’s details page from the Capacity page. For details about the Capacity page, see **Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types**.
In addition to the Capacity page, you can use the Dashboard page to get a snapshot view of the health, allocated capacity and utilization, and user activity for your entire set of pods. See Health Visibility and Insights into Your Cloud-Connected Pods Provided by the Cloud Monitoring Service in Horizon Cloud.

**Obtain the Pod Gateway's Load Balancer Information to Map in your DNS Server**

When a deployed Horizon Cloud pod in Microsoft Azure has a gateway configuration, you must create a CNAME record in your DNS server that maps the fully qualified domain name (FQDN) that you entered in the deployment wizard to the pod gateway's deployed Azure load balancer information. For an external gateway configuration with a public load balancer IP address, you map the FQDN that you entered in the deployment wizard to the gateway's Azure load balancer resource's auto-generated FQDN. For an internal gateway configuration or an external gateway configuration with a private load balancer IP address, you map the FQDN that you entered in the deployment wizard to the gateway's Azure internal load balancer resource's private IP address. You can obtain the Azure load balancer information from the pod's details page in the Horizon Cloud Administration Console, or console for short.

In the deployment wizard, you provided:

- Your FQDN (for example, ourOrg.example.com or ourApps.ourOrg.example.com). This FQDN is the one which your end users use to access their desktops.
- An SSL certificate that is associated with that FQDN and which is signed by a trusted certificate authority.

**External gateway configuration with a public load balancer IP address**

If your pod deployment specified using an external gateway with a public IP address, the deployed Unified Access Gateway instances are configured with an Azure load balancer resource that has a public IP address and an auto-generated public FQDN. The form of the auto-generated public FQDN is in the pattern vmw-hcs-ID-uag.region.cloudapp.azure.com, where vmw-hcs-ID matches the pattern within the name of the resource group in which the Unified Access Gateway instances reside, and region is the Microsoft Azure region where the pod is located.

**Tip**  The pod's details page displays the auto-generated public FQDN.

For the external gateway, your DNS server must map those two FQDNs. When the addresses are mapped, your end users can enter your provided FQDN as the server address in the Horizon Client or use with HTML Access to access the desktops served by that pod.

```
ourApps.ourOrg.example.com  vmw-hcs-ID-uag.region.cloudapp.azure.com
```

**Internal gateway configuration or an external gateway configuration with a private load balancer IP address**
When you specify using an internal gateway or using an external gateway without a public IP address on its load balancer, the deployed Unified Access Gateway instances are configured with an Azure load balancer resource that has a private IP address. The typical reason why you deploy an external gateway without a public IP address is to add a firewall or NAT in front of that Azure load balancer, to remove the ability of directly connecting to it.

**Tip**  The pod’s details page displays the IP address to use.

For the internal gateway or an external gateway without a public IP address on its load balancer, your DNS server would map your FQDN to the deployed Azure load balancer’s private IP address. When they are mapped, your end users can enter your provided FQDN as the server address in the Horizon Client or use with HTML Access to access the desktops served by that pod.

| ourApps.ourOrg.example.com | Azure-load-balancer-private-IP |

The pod’s details page lists the information you need for this mapping. Use these steps to locate the appropriate information in the pod’s details page.

**Prerequisites**

The pod must be successfully deployed into your Microsoft Azure environment, according to the steps in *Horizon Cloud Deployment Guide*.

**Procedure**

1. In the console, navigate to **Settings > Capacity**, and click on the pod to open its details page.
2. On the **Summary** tab, scroll down towards the bottom of the page and locate the sections labeled **Internal UAG** and **External UAG**.

**Note**  The page includes a section only when the pod has the corresponding gateway configured. If the pod only has an internal gateway, then only the **Internal UAG** section appears and not the section for the external one. If the pod has both configurations, then both sections appear in the page.

The following screenshot shows the portion of the page for a pod that has both types of configurations, internal and external.
3 For each configuration that your pod has, locate the **Load Balancer FQDN** field and copy its displayed value.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal</strong></td>
<td>The displayed value is the gateway configuration's Microsoft Azure load balancer resource's private IP address. This numeric IP address is assigned to the gateway's load balancer resource from the pod's desktop subnet.</td>
</tr>
<tr>
<td><strong>External with a public load balancer IP address</strong></td>
<td>The displayed value is the Microsoft Azure load balancer resource's auto-generated public FQDN in the form <code>vmw-hcs-podID-uag.region.cloudapp.azure.com</code>, where region is the Microsoft Azure region and where podID is the pod's ID value. That pod ID is displayed on its details page.</td>
</tr>
<tr>
<td><strong>External with a private load balancer IP address</strong></td>
<td>The displayed value is the Microsoft Azure load balancer resource's private IP address. This numeric IP address is assigned to the load balancer resource from the pod's DMZ subnet.</td>
</tr>
</tbody>
</table>
4 In your DNS server, map that load balancer FQDN value to the FQDN that was provided in the wizard when the pod was deployed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>ourApps.ourOrg.example.com</td>
</tr>
<tr>
<td>External with a public load balancer IP address</td>
<td>ourApps.ourOrg.example.com vwm-hcs-ID-uag.region.cloudapp.azure.com</td>
</tr>
<tr>
<td>External with a private load balancer IP address</td>
<td>ourApps.ourOrg.example.com Azure-load-balancer-private-IP</td>
</tr>
</tbody>
</table>

Changing Gateway-Related Items for a Deployed Horizon Cloud Pod in Microsoft Azure

You can change the gateway configurations on a deployed pod in a variety of ways. You make these changes using the pod’s details page in the Horizon Cloud Administration Console. The console is dynamic. It will only make available to you those actions that make sense to perform based on what gateway configuration already exists on the pod.

As described in the Deploy a Horizon Cloud Pod into Microsoft Azure documentation topics, the pod can be deployed an external or internal gateway configuration, or with both. The deployed pod can also have RADIUS two-factor authentication set on neither, one, or both of its gateway configurations. You can change the following gateway-related items on a deployed pod from the pod's details page.

- Add gateway configurations to the pod. If the pod has no gateway configuration, you can add one or both types. If the pod has one type of gateway, you can add the one that's missing.
- Delete gateway configurations from the pod.
- Edit an existing gateway configuration to add, change, or disable the RADIUS two-factor authentication settings for that gateway.
- Change a gateway configuration's Unified Access Gateway software settings.

**Note** Currently, items that are related to the gateway deployment's specifications can be set only during deployment of that gateway configuration into your subscription environment. The console does not yet provide a way to use the Edit Pod workflow to update the gateway's deployment configuration, even though the Edit Pod workflow can be used to update the gateway's software configuration at any time. Examples of these items that cannot be changed using the Edit Pod workflow are the VM model used for the Unified Access Gateway instances, the network-related settings, and the Microsoft Azure resource tags for the gateway's resource groups. If you want to change an item that is related to an existing gateway's deployment configuration, you must first delete that existing gateway configuration from the pod and the use the Edit Pod workflow to re-deploy a gateway configuration for the pod using the new settings you want. Keep in mind that starting with pod manifest 2298.0, the pod must have at least one gateway configuration for supported operations. If you leave a pod of manifest 2298.0 or later without a gateway configuration, that pod is in an unsupported configuration.

**Add a Gateway Configuration to a Deployed Horizon Cloud Pod**

When you initially deployed a Horizon Cloud pod into Microsoft Azure no gateway, or with only one type of gateway, you can later add a gateway configuration to the pod using the Edit Pod workflow. You launch that workflow from the pod's details page.

**Tip** The console is dynamic. It will only make available in the user interface those workflows and toggles and fields that make sense and are appropriate based on the current configuration of the pod and the configuration of your overall environment.
As described in Chapter 7 Introduction to Horizon Cloud Pods in Microsoft Azure, a pod can have an external gateway configuration or an internal one or both. You can use this workflow to add the type that the pod does not already have. At the same time that you edit the pod to add a gateway configuration, you can also specify two-factor authentication settings for that gateway.

**Important** When modifying the pod using these steps, keep in mind the following points:

- Keep in mind that the IP setting for an external gateway’s load balancer cannot be changed after the external gateway configuration is originally set. When you add an external gateway configuration, you have the option to have it use a private IP address for the gateway’s load balancer instead of a public one. The default is to use a public IP.

- During the time the system is changing the pod’s configuration until it is finished, the following limitations apply:
  - You cannot perform administration tasks on the pod.
  - End users who do not have connected sessions to their desktops or remote applications served by the pod and who attempt to connect cannot do so.
  - End users who have connected sessions served by the pod will have those active sessions disconnected. No data loss will occur. After the configuration changes are complete, those users can reconnect.

**Prerequisites**

**Note** If the pod has high availability enabled and one of the pod manager VMs is offline, the system prevents adding a gateway to the pod. The message will appear after you click **Save & Exit**. You must bring the offline pod manager VM back online using the Microsoft Azure portal before you can add the gateway.

When adding a gateway configuration to an existing pod in Microsoft Azure, to complete the fields in the Edit Pod wizard, you must provide the information as described in **Prerequisites for the Unified Access Gateway Configurations**. If you are also specifying two-factor authentication settings at the same time that you’re adding the gateway, you must provide the information described in **Prerequisites When Deploying With a Two-Factor Authentication Configuration**. If you are adding an external gateway configuration and you want it to use its own subscription, you also need that subscription information and ensure that the VNet that you’ll use for that gateway meets the VNet requirements. For those VNet requirements, see **Configure the Required Virtual Network in Microsoft Azure**.

**Important** All certificates in the certificate chain must have valid time frames. The Unified Access Gateway VMs require that all of the certificates in the chain, including any intermediate certificates, have valid time frames. If any certificate in the chain is expired, unexpected failures can occur later as the certificate is uploaded to the Unified Access Gateway configuration.
Procedure

1. In the console, navigate to **Settings > Capacity** and click the pod's name to open its details page.

2. In the pod’s details page, click **Edit**.

3. In the Subscription step, if you are adding an external gateway configuration and want it to use a subscription separate from the pod’s, enable **Use a Different Subscription for External Gateway** and enter the subscription information.

4. Click **Next** until you reach the **Gateway Settings** step.

   This step has a section for the external gateway configuration and a section for the internal gateway configuration. The user interface reflects the pod's current configuration and the gateway settings it already has.

5. To add an external gateway, switch on the **Enable External UAG?** toggle and complete the fields in the **External UAG** section.

<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable External Gateway?</strong></td>
<td>Controls whether the pod has an external gateway configuration. The external configuration allows access to desktops and applications for users located outside of your corporate network. The pod includes a Microsoft Azure load balancer resource and Unified Access Gateway instances to provide this access.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Leaving the default enabled setting is recommended.</td>
</tr>
<tr>
<td></td>
<td>When this toggle is switched off, clients must either connect through **Workspace ONE Access integrated with the pod or directly to the pod managers' load balancer, or they connect through an internal gateway configuration. In the case of clients connecting through **Workspace ONE Access integrated with the pod or directly, some post-deployment steps are required. In this case, after the pod is deployed, follow the steps in <strong>Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs.</strong></td>
</tr>
<tr>
<td><strong>FQDN</strong></td>
<td>Enter the required fully qualified domain name (FQDN), such as <em>ourOrg.example.com</em>, which your end users will use to access the service. You must own that domain name and have a certificate in PEM format that can validate that FQDN.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>This FQDN cannot contain underscores. In this release, connections to the Unified Access Gateway instances will fail when the FQDN contains underscores.</td>
</tr>
<tr>
<td><strong>DNS Addresses</strong></td>
<td>Optionally enter addresses for additional DNS servers that Unified Access Gateway can use for name resolution, separated by commas. When configuring this external Unified Access Gateway configuration to use two-factor authentication with your on-premises RADIUS server, you would specify the address of a DNS server that can resolve the name of your on-premises RADIUS server. As described in the <strong>Prerequisites for All Deployments</strong>, a DNS server must be set up internally in your subscription and configured to provide external name resolution. The Unified Access Gateway instances use that DNS server by default. If you specify addresses in this field, the deployed Unified Access Gateway instances use the addresses in addition to the prerequisite DNS server that you configured in your subscription's virtual network.</td>
</tr>
</tbody>
</table>
Option | Description
---|---
**Routes** | Optionally specify custom routes to additional gateways that you want the deployed Unified Access Gateway instances to use to resolve network routing for the end user access. The specified routes are used to allow Unified Access Gateway to resolve network routing such as to RADIUS servers for two-factor authentication.

When configuring this pod to use two-factor authentication with an on-premises RADIUS server, you must enter the correct route the Unified Access Gateway instances can use to reach the RADIUS server. For example, if your on-premises RADIUS server uses 10.10.60.20 as its IP address, you would enter 10.10.60.0/24 and your default route gateway address as a custom route. You obtain your default route gateway address from the Express Route or VPN configuration you are using for this environment.

Specify the custom routes as a comma-separated list in the form ipv4-network-address/bits ipv4-gateway-address, for example: 192.168.1.0/24 192.168.0.1, 192.168.2.0/24 192.168.0.2.

**VM Model** | Select a model to use for the Unified Access Gateway instances. You must ensure that the Microsoft Azure subscription you specified for this pod can provide the capacity for two VMs of the selected model.

**Certificate** | Upload the certificate in PEM format that Unified Access Gateway will use to allow clients to trust connections to the Unified Access Gateway instances running in Microsoft Azure. The certificate must be based on the FQDN you entered and be signed by a trusted CA. The PEM file must contain the entire certificate chain and the private key: SSL certificate intermediate certificates, root CA certificate, private key.

Specify the settings for this gateway's Microsoft Load Balancer.

Option | Description
---|---
**Enable Public IP?** | Controls whether this gateway’s load balancing type is configured as private or public. If switched on, the deployed Microsoft Azure load balancer resource is configured with a public IP address. If switched off, the Microsoft Azure load balancer resource is configured with a private IP address.

**Important** In this release, you cannot later change the external gateway’s load balancing type from public to private, or from private to public. The only way to make that change would be to delete the gateway configuration entirely from the deployed pod and then edit the pod to add it back with the opposite setting.

If you switch off this toggle, the field **Public IP for Horizon FQDN** appears.

**Public IP for Horizon FQDN** | When you have chosen not to configure the deployed Microsoft Azure load balancer with a public IP, you must provide the IP address that you are mapping in your DNS to the FQDN that your end users' Horizon clients will use for PCoIP connections to the gateway. The deployer will configure this IP address in the Unified Access Gateway configuration settings.

Specify the external gateway's networking settings.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use a Different Virtual Network</strong></td>
<td>This toggle controls whether the external gateway will be deployed into its own VNet, separate from the pod's VNet. The following rows describe the different cases.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When you specified to use a different subscription for the external gateway in the first step of the wizard, this toggle is enabled by default. You must choose a VNet for the gateway in that situation.</td>
</tr>
</tbody>
</table>

**Use a Different Virtual Network — Switched off**

When the toggle is switched off, the external gateway will be deployed into the pod's VNet. In this case, you must specify the DMZ subnet.

- **DMZ Subnet** - When **Use Existing Subnet** is enabled in the Pod Setup wizard step, **DMZ Subnet** lists the subnets available on the VNet selected for **Virtual Network**. Select the existing subnet that you want to use for the pod's DMZ subnet.

  **Important** Select an empty subnet, one that has no other resources attached to it. If the subnet is not empty, unexpected results might occur during the deployment process or pod operations.

- **DMZ Subnet (CIDR)** - When **Use Existing Subnet** is switched off in the preceding wizard step, enter the subnet (in CIDR notation) for the DMZ (demilitarized zone) network that will be configured to connect the Unified Access Gateway instances to the gateway's Microsoft Azure public load balancer.

**Use a Different Virtual Network — Enabled**

When the toggle is enabled, the external gateway will be deployed into its own VNet. In this case, you must select the VNet to use and then specify the three required subnets. Enable the **Use Existing Subnet** toggle to select from subnets that you have created in advance on the specified VNet. Otherwise, specify the subnets in CIDR notation.

**Important** Select empty subnets, ones that have no other resources attached to them. If the subnets are not empty, unexpected results might occur during the deployment process or pod operations.

In this case, the gateway's VNet and pod's VNet are peered. The best practice is to have the subnets created in advance, and not use the CIDR entries here. See Prerequisites When Deploying With an External Unified Access Gateway Configuration Using its Own VNet or Subscription Separate from the Pod's VNet or Subscription.

- **Management subnet** - Specify the subnet to use for the gateway's management subnet. A CIDR of at least /27 is required. This subnet must have the Microsoft.SQL service configured as a service endpoint.

- **Back-end subnet** - Specify the subnet to use for the gateway's back end subnet. A CIDR of at least /27 is required.

- **Front-end subnet** - Specify the subnet for the front-end subnet that will be configured to connect the Unified Access Gateway instances to the gateway's Microsoft Azure public load balancer.

6  (Optional) In the **Deployment** section, use the toggle to optionally select an existing resource group into which you want the deployer to deploy the resources for the external gateway configuration.

This toggle displays when you have specified to use a different subscription for the external gateway in the first step of the wizard. When you enable the toggle, a field appears in which you can search for and select the resource group.
To add an internal gateway, switch on the **Enable Internal UAG?** toggle and complete the fields in the **Internal UAG** section.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Internal Gateway?</strong></td>
<td>Controls whether the pod has an internal gateway configuration. The internal configuration provides trusted access to desktops and applications for HTML Access (Blast) connections for users located inside of your corporate network. The pod includes an Azure load balancer resource and Unified Access Gateway instances to provide this access. By default, this gateway's load balancing type is private. The load balancer is configured with a private IP address.</td>
</tr>
<tr>
<td><strong>FQDN</strong></td>
<td>Enter the required fully qualified domain name (FQDN), such as ourOrg.example.com, which your end users will use to access the service. You must own that domain name and have a certificate in PEM format that can validate that FQDN. If you specified an FQDN for the external gateway, you must enter the same FQDN here. <strong>Important</strong> This FQDN cannot contain underscores. In this release, connections to the Unified Access Gateway instances will fail when the FQDN contains underscores.</td>
</tr>
<tr>
<td><strong>DNS Addresses</strong></td>
<td>Optionally enter addresses for additional DNS servers that Unified Access Gateway can use for name resolution, separated by commas. When configuring this internal gateway configuration to use two-factor authentication with your on-premises RADIUS server, you would specify the address of a DNS server that can resolve the name of your on-premises RADIUS server. As described in the Prerequisites for All Deployments, a DNS server must be set up internally in your subscription and configured to provide name resolution. The Unified Access Gateway instances use that DNS server by default. If you specify addresses in this field, the deployed Unified Access Gateway instances use the addresses in addition to the prerequisite DNS server that you configured in your subscription's virtual network.</td>
</tr>
<tr>
<td><strong>Routes</strong></td>
<td>Optionally specify custom routes to additional gateways that you want the deployed Unified Access Gateway instances to use to resolve network routing for the end user access. The specified routes are used to allow Unified Access Gateway to resolve network routing such as to RADIUS servers for two-factor authentication. When configuring this pod to use two-factor authentication with an on-premises RADIUS server, you must enter the correct route the Unified Access Gateway instances can use to reach the RADIUS server. For example, if your on-premises RADIUS server uses 10.10.60.20 as its IP address, you would enter 10.10.60.0/24 and your default route gateway address as a custom route. You obtain your default route gateway address from the Express Route or VPN configuration you are using for this environment. Specify the custom routes as a comma-separated list in the form ipv4-network-address/bits ipv4-gateway-address, for example: 192.168.1.0/24 192.168.0.1, 192.168.2.0/24 192.168.0.2.</td>
</tr>
<tr>
<td><strong>VM Model</strong></td>
<td>Select a model to use for the Unified Access Gateway instances. You must ensure that the Microsoft Azure subscription you specified for this pod can provide the capacity for two VMs of the selected model.</td>
</tr>
<tr>
<td><strong>Certificate</strong></td>
<td>Upload the certificate in PEM format that Unified Access Gateway will use to allow clients to trust connections to the Unified Access Gateway instances running in Microsoft Azure. The certificate must be based on the FQDN you entered and be signed by a trusted CA. The PEM file must contain the entire certificate chain and the private key: SSL certificate intermediate certificates, root CA certificate, private key.</td>
</tr>
</tbody>
</table>

In the section for whichever gateway you are adding, if you want to optionally configure the end users' desktops to use RADIUS two-factor authentication, follow the steps in **Enable Two-Factor Authentication on a Horizon Cloud Pod's Gateways.**
In the **Azure Resource Tags** section, if you want to specify resource tags for the gateway-related resource groups that are different from the ones specified on the pod's other resource groups, deactivate the **Inherit Pod Tags** toggle and specify the tags in the fields that appear.

For a description of the **Azure Resource Tags** fields, see Specify the Horizon Cloud Pod's Gateway Configuration. The same set of tags will be used for both types of gateways on the pod.

**Click Save & Exit.**

A confirmation message appears asking you to confirm the start of the workflow.

**Click Yes to start the workflow.**

**Results**

Until the system is finished deploying the elements for the gateway, the pod summary page's section for that configuration type shows Pending status. Also, you cannot perform additional Edit Pod workflow-related activities until the system is finished with its actions to deploy the gateway.

When the workflow is completed, the status will show as Ready and the load balancer FQDN will be displayed in the page.

**Note** When running this workflow for a pod in Microsoft Azure China, the process can take longer than an hour to complete. The process is subject to geographic network issues that can cause slow download speeds as the binaries are downloaded from the cloud control plane.

**What to do next**

**Important** Before your end users can start using the newly added gateway, you must complete the following tasks.

- For the newly added gateway configuration, ensure you have a CNAME record in your DNS server to map the configuration's deployed load balancer to the FQDN that you entered in the deployment wizard. See Obtain the Pod Gateway's Load Balancer Information to Map in your DNS Server for details.

- If you specified RADIUS two-factor authentication for the added gateway, you must do these tasks:
  - If you configured an external gateway with RADIUS settings and that RADIUS server is not reachable within the same VNet as used by the pod, or within the peered VNet topology if you deployed the external gateway into its own VNet, verify, configure that RADIUS server to allow client connections from the IP address of the external gateway's load balancer. In an external gateway configuration, the Unified Access Gateway
instances attempt contact with the RADIUS server using that load balancer address. To allow the connections, ensure the load balancer resource's IP address that is in that external gateway's resource group is specified as a client in your RADIUS server configuration.

- If you configured an internal gateway, or an external gateway and your RADIUS server is reachable within the same VNet as used by the pod, configure the RADIUS server to allow connections from the appropriate NICs that were created in the gateway's resource group in Microsoft Azure that must communicate with the RADIUS server. Your network administrator determines the RADIUS server's network visibility to the pod's Azure Virtual Network and subnets. Your RADIUS server must allow client connections from the IP addresses of those gateway NICs that correspond to the subnet for which your network administrator has given network visibility to the RADIUS server. The gateway's resource group in Microsoft Azure has four NICs that correspond to that subnet, two that are currently active for the two Unified Access Gateway instances and two that are idle and will become the active ones after the pod goes through an update. To support connectivity between the gateway and the RADIUS server both for ongoing pod operations and after each pod update, ensure the IP addresses of those four NICs are specified as clients in the RADIUS server configuration.

For information on how to obtain those IP addresses, see Update Your RADIUS System with the Required Horizon Cloud Pod Gateway Information.

Enable Two-Factor Authentication on a Horizon Cloud Pod's Gateways

To enable use of two-factor authentication in the gateway settings of an already deployed pod, use the Edit action in the pod's details page. Gateway configurations on your pod use Unified Access Gateway VMs and are configured to provide your end users' access to their desktops and applications. You can add these two-factor authentication settings to the pod's existing gateway configurations, or you can add them at the same time that you add a new gateway configuration. You use the Edit Pod workflow to add the two-factor authentication settings to the pod's gateway configuration.

Prerequisites

For the gateway on which you are adding two-factor authentication, verify that you have Add a Gateway Configuration to a Deployed Horizon Cloud Pod. When configuring two-factor authentication to an on-premises authentication server, you also provide information in the following fields so that the Unified Access Gateway instances for that gateway can resolve routing to that on-premises server.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Addresses</td>
<td>Specify one or more addresses of DNS servers that can resolve the name of your on-premises authentication server.</td>
</tr>
<tr>
<td>Routes</td>
<td>Specify one or more custom routes that allow the pod's Unified Access Gateway instances to resolve network routing to your on-premises authentication server. For example, if you have an on-premises RADIUS server that uses 10.10.60.20 as its IP address, you would use 10.10.60.0/24 and your default route gateway address as a custom route. You obtain your default route gateway address from the Express Route or VPN configuration you are using for this environment. Specify the custom routes as a comma-separated list in the form ipv4-network-address/bits ipv4-gateway-address, for example: 192.168.1.0/24 192.168.0.1, 192.168.2.0/24 192.168.0.2.</td>
</tr>
</tbody>
</table>

Verify that you have the following information used in your authentication server's configuration, so that you can provide it in the appropriate fields in the pod deployment wizard. If you have both a primary and secondary server, obtain the information for each of them.

- IP address or DNS name of the authentication server
- The shared secret that is used for encryption and decryption in the authentication server's protocol messages
- Authentication port numbers, typically the 1812 UDP port.
- Authentication protocol type. The authentication types include PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, version 1 and 2).

**Note** Check your RADIUS vendor's documentation for the authentication protocol that your RADIUS vendor recommends and follow their indicated protocol type. The pod's capability to support two-factor authentication with RADIUS is provided by the Unified Access Gateway instances, and Unified Access Gateway supports PAP, CHAP, MSCHAP1, and MSCHAP2. PAP is generally less secure than MSCHAP2. PAP is also a simpler protocol than MSCHAP2. As a result, even though most RADIUS vendors are compatible with the simpler PAP protocol, some RADIUS vendors are not as compatible with the more secure MSCHAP2.

**Procedure**

1. If the Edit Pod window's **Gateway Settings** step is not already open, click **Edit** in the pod's details page and then click **Next** to move to the **Gateway Settings** step.

2. Position the window at the gateway type for which you want to enable two-factor authentication, either external or internal.

3. Switch on the **Enable 2 Factor Authentication** toggle.

When the toggle is enabled, the wizard displays the additional configuration fields. Use the scroll bar to access all of the fields.

The following screenshot is an example of what is displayed after you switch on the toggle in the **External UAG** section.
4 Select your two-factor authentication method in the drop-down list. In this release, RADIUS authentication is supported.

5 In the **Name** field, enter an identifying name for this configuration.

6 In the **Properties** section, specify details related to the end users' interaction with the login screen they will use to authenticate for access.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>You can leave this field blank. Even though this field is visible in the wizard, it only sets an internal name in Unified Access Gateway. This name is not used by Horizon clients.</td>
</tr>
<tr>
<td>Display Hint</td>
<td>Optionally enter a text string that will be displayed to the end users in the message on the end-user client login screen when it prompts the user for their RADIUS user name and passcode. The specified hint appears to the end user as <em>Enter your DisplayHint user name and passcode</em>. This hint can help guide users to enter the correct RADIUS passcode. As an example, specifying a phrase like <strong>Example Company user name and domain password below</strong> for would result in a prompt to the end user that says <em>Enter your Example Company user name and domain password below for user name and passcode</em>.</td>
</tr>
<tr>
<td>Name ID Suffix</td>
<td>This setting is used in SAML scenarios, where your pod is configured to use TrueSSO for single sign-on. Optionally provide a string which the system will append to the SAML assertion user name that is sent to the broker. For example, if the user name is entered as <em>user1</em> on the login screen and a name ID suffix of <em>example.com</em> was specified here, the system sends a SAML assertion user name of <em><a href="mailto:user1@example.com">user1@example.com</a></em> to the broker.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number of Iterations</td>
<td>Enter the maximum number of failed authentication attempts that a user is allowed when attempting to log in using this RADIUS system.</td>
</tr>
<tr>
<td>Maintain Username</td>
<td>Enable this toggle to maintain the user’s RADIUS username during authentication to Horizon Cloud. When enabled:</td>
</tr>
<tr>
<td></td>
<td>- The user must have the same username credentials for RADIUS as for their Active Directory authentication to Horizon Cloud.</td>
</tr>
<tr>
<td></td>
<td>- The user cannot change the username in the login screen.</td>
</tr>
<tr>
<td></td>
<td>If this toggle is switched off, the user is able to type a different user name in the login screen.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> For the relationship between enabling Maintain Username and the domain security settings in Horizon Cloud, see the Domain Security Settings on General Settings Page topic.</td>
</tr>
</tbody>
</table>

7 In the Primary Server section, specify details about the authentication server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name / IP Address</td>
<td>Enter the DNS name or the IP address of the authentication server.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the secret for communicating with the authentication server. The value must be identical to the server-configured value.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Specify the UDP port configured on the authentication server for sending or receiving authentication traffic. The default is 1812.</td>
</tr>
<tr>
<td>Accounting Port</td>
<td>Optionally specify the UDP port configured on the authentication server for sending or receiving accounting traffic. The default is 1813.</td>
</tr>
<tr>
<td>Mechanism</td>
<td>Select the authentication protocol that is supported by the specified authentication server and which you want the deployed pod to use.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>Specify the number of seconds that the pod should wait for a response from the authentication server. After this number of seconds, a retry is sent if the server does not respond.</td>
</tr>
<tr>
<td>Max Number of Retries</td>
<td>Specify the maximum number of times the pod should retry failed requests to the authentication server.</td>
</tr>
<tr>
<td>Realm Prefix</td>
<td>Optionally provide a string which the system will place at the beginning of the user name when the name is sent to the authentication server. The user account location is called the realm. For example, if the user name is entered as user1 on the login screen and a realm prefix of DOMAIN-A\ was specified here, the system sends DOMAIN-A\user1 to the authentication server. If you do not specify a realm prefix, only the entered user name is sent.</td>
</tr>
<tr>
<td>Realm Suffix</td>
<td>Optionally provide a string which the system will append to the user name when the name is sent to the authentication server. For example, if the user name is entered as user1 on the login screen and a realm suffix of @example.com was specified here, the system sends <a href="mailto:user1@example.com">user1@example.com</a> to the authentication server.</td>
</tr>
</tbody>
</table>

8 (Optional) In the Secondary Server section, optionally specify details about an auxiliary authentication server.

You can configure a secondary authentication server to provide for high availability. Enable the Auxiliary Server toggle and complete the fields as described in Primary Server section.
9 When you have made all the settings you want, click **Save & Exit**.

A confirmation message appears asking you to confirm the start of the workflow.

10 Click **Yes** to start the workflow.

**Results**

Until the system is finished deploying the new configuration to the pod, the pod summary page's section for the gateway on which you added two-factor authentication will show the **Pending** status.

When the workflow is completed, the status will show as **Ready** and the gateway's two-authentication settings will be displayed in the page.

**Note** When running this workflow for a pod in Microsoft Azure China, the process can take longer than an hour to complete. The process is subject to geographic network issues that can cause slow download speeds as the binaries are downloaded from the cloud control plane.

**What to do next**

**Important** Before your end users can start using the gateway with the two-factor authentication feature, you must complete the following tasks.

- If you configured an external gateway with RADIUS settings and that RADIUS server is not reachable within the same VNet as used by the pod, or within the peered VNet topology if you deployed the external gateway into its own VNet, verify, configure that RADIUS server to allow client connections from the IP address of the external gateway's load balancer. In an external gateway configuration, the Unified Access Gateway instances attempt contact with the RADIUS server using that load balancer address. To allow the connections, ensure the load balancer resource's IP address that is in that external gateway's resource group is specified as a client in your RADIUS server configuration.

- If you configured an internal gateway, or an external gateway and your RADIUS server is reachable within the same VNet as used by the pod, configure the RADIUS server to allow connections from the appropriate NICs that were created in the gateway's resource group in Microsoft Azure that must communicate with the RADIUS server. Your network administrator determines the RADIUS server's network visibility to the pod's Azure Virtual Network and subnets. Your RADIUS server must allow client connections from the IP addresses of those gateway NICs that correspond to the subnet for which your network administrator has given network visibility to the RADIUS server. The gateway's resource group in Microsoft Azure has four NICs that correspond to that subnet, two that are currently active for the two Unified Access Gateway instances and two that are idle and will become the active ones after the pod goes through an update. To support connectivity between the gateway and the RADIUS server both for ongoing pod operations and after each pod update, ensure the IP addresses of those four NICs are specified as clients in the RADIUS server configuration.

For information on how to obtain those IP addresses, see [Update Your RADIUS System with the Required Horizon Cloud Pod Gateway Information](#).
Change or Disable the Two-Factor Authentication Settings on a Horizon Cloud Pod's Gateways

You can use the Edit Pod workflow to change the two-factor authentication settings on the pod's gateways, or disable the two-factor authentication entirely. When you change the settings, you basically type a new name for the set of two-factor authentication settings, enter the new settings you want, make sure that new name is selected for the specific gateway, and save. You use the Edit Pod workflow to change the two-factor authentication settings.

Prerequisites

If you are keeping two-factor authentication enabled for one of the gateways but are changing the specific settings, verify that you have the following information:

- When the two-factor authentication server is on-premises, verify that you have the relevant information for the following fields so that the Unified Access Gateway instances for that gateway can resolve routing to that server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Addresses</td>
<td>Specify one or more addresses of DNS servers that can resolve the name of your on-premises authentication server.</td>
</tr>
<tr>
<td>Routes</td>
<td>Specify one or more custom routes that allow the pod's Unified Access Gateway instances to resolve network routing to your on-premises authentication server. For example, if you have an on-premises RADIUS server that uses 10.10.60.20 as its IP address, you would use 10.10.60.0/24 and your default route gateway address as a custom route. You obtain your default route gateway address from the Express Route or VPN configuration you are using for this environment. Specify the custom routes as a comma-separated list in the form ipv4-network-address/bits ipv4-gateway-address, for example: 192.168.1.0/24 192.168.0.1, 192.168.2.0/24 192.168.0.2.</td>
</tr>
</tbody>
</table>

- Verify that you have the following information used in your authentication server's configuration, so that you can provide it in the appropriate fields in the pod deployment wizard. If you have both a primary and secondary server, obtain the information for each of them.

  - IP address or DNS name of the authentication server
  - The shared secret that is used for encryption and decryption in the authentication server's protocol messages
  - Authentication port numbers, typically the 1812 UDP port.
Authentication protocol type. The authentication types include PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, version 1 and 2).

**Note** Check your RADIUS vendor's documentation for the authentication protocol that your RADIUS vendor recommends and follow their indicated protocol type. The pod's capability to support two-factor authentication with RADIUS is provided by the Unified Access Gateway instances, and Unified Access Gateway supports PAP, CHAP, MSCHAP1, and MSCHAP2. PAP is generally less secure than MSCHAP2. PAP is also a simpler protocol than MSCHAP2. As a result, even though most RADIUS vendors are compatible with the simpler PAP protocol, some RADIUS vendors are not as compatible with the more secure MSCHAP2.

**Procedure**

1. Open the Edit Pod window from the pod's details page by clicking **Edit**.
2. In the Edit Pod window, click **Next** to move to the Gateway Settings step.

   This step has a section for the external gateway configuration and a section for the internal gateway configuration. The user interface reflects the pod's current configuration and the gateway settings it already has.
3. Position the window at the gateway type for which you want to change the two-factor authentication, either external or internal.
4. To disable two-factor authentication on the gateway, switch off the **Enable 2 Factor Authentication** toggle and then go to Step step 9 to save the changes.

   If the other gateway also has two-factor authentication enabled and you want to disable it, switch off the toggle in the section for that other gateway.
5. To change the specific two-factor authentication settings that are set on the gateway, continue with the following steps.

   You create a new name for the new set of two-factor authentication values and save the configuration with that new name selected for that gateway section in the window.
6. In the **Name** field, enter an identifying name for this configuration.
7 In the Properties section, specify details related to the end users' interaction with the login screen they will use to authenticate for access.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>You can leave this field blank. Even though this field is visible in the wizard, it only sets an internal name in Unified Access Gateway. This name is not used by Horizon clients.</td>
</tr>
<tr>
<td>Display Hint</td>
<td>Optionally enter a text string that will be displayed to the end users in the message on the end-user client login screen when it prompts the user for their RADIUS user name and passcode. The specified hint appears to the end user as Enter your DisplayHint user name and passcode, where DisplayHint is the text you specify in this field. This hint can help guide users to enter the correct RADIUS passcode. As an example, specifying a phrase like Example Company user name and domain password below for would result in a prompt to the end user that says Enter your Example Company user name and domain password below for user name and passcode.</td>
</tr>
<tr>
<td>Name ID Suffix</td>
<td>This setting is used in SAML scenarios, where your pod is configured to use TrueSSO for single sign-on. Optionally provide a string which the system will append to the SAML assertion user name that is sent to the broker. For example, if the user name is entered as user1 on the login screen and a name ID suffix of @example.com was specified here, the system sends a SAML assertion user name of <a href="mailto:user1@example.com">user1@example.com</a> to the broker.</td>
</tr>
<tr>
<td>Number of Iterations</td>
<td>Enter the maximum number of failed authentication attempts that a user is allowed when attempting to log in using this RADIUS system.</td>
</tr>
</tbody>
</table>
| Maintain Username | Enable this toggle to maintain the user's RADIUS username during authentication to Horizon Cloud. When enabled:  
  - The user must have the same username credentials for RADIUS as for their Active Directory authentication to Horizon Cloud.  
  - The user cannot change the username in the login screen.  
  If this toggle is switched off, the user is able to type a different user name in the login screen. |

8 In the Primary Server section, specify details about the authentication server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name / IP Address</td>
<td>Enter the DNS name or the IP address of the authentication server.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the secret for communicating with the authentication server. The value must be identical to the server-configured value.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Specify the UDP port configured on the authentication server for sending or receiving authentication traffic. The default is 1812.</td>
</tr>
<tr>
<td>Accounting Port</td>
<td>Optionally specify the UDP port configured on the authentication server for sending or receiving accounting traffic. The default is 1813.</td>
</tr>
<tr>
<td>Mechanism</td>
<td>Select the authentication protocol that is supported by the specified authentication server and which you want the deployed pod to use.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>Specify the number of seconds that the pod should wait for a response from the authentication server. After this number of seconds, a retry is sent if the server does not respond.</td>
</tr>
</tbody>
</table>
### Option | Description
--- | ---
Max Number of Retries | Specify the maximum number of times the pod should retry failed requests to the authentication server.
Realm Prefix | Optionally provide a string which the system will place at the beginning of the user name when the name is sent to the authentication server. The user account location is called the realm. For example, if the user name is entered as user1 on the login screen and a realm prefix of DOMAIN-A\ was specified here, the system sends DOMAIN-A\user1 to the authentication server. If you do not specify a realm prefix, only the entered user name is sent.
Realm Suffix | Optionally provide a string which the system will append to the user name when the name is sent to the authentication server. For example, if the user name is entered as user1 on the login screen and a realm suffix of @example.com was specified here, the system sends user1@example.com to the authentication server.

9 (Optional) In the Secondary Server section, optionally specify details about an auxiliary authentication server.

You can configure a secondary authentication server to provide for high availability. Enable the **Auxiliary Server** toggle and complete the fields as described in Primary Server section.

10 When you have made all the settings you want, click **Save & Exit**.

11 Click **Yes** to start the workflow.

### Results
Until the system is finished deploying the new configuration to the pod, the pod summary page’s section for the gateway on which you added two-factor authentication will show the Pending status.

When the workflow is completed, the status will show as Ready and the gateway’s two-authentication settings will be displayed in the page.

**Note** When running this workflow for a pod in Microsoft Azure China, the process can take longer than an hour to complete. The process is subject to geographic network issues that can cause slow download speeds as the binaries are downloaded from the cloud control plane.

### What to do next

**Important** When you change the values of a gateway’s two-factor authentication settings to new ones, before your end users resume using the gateway that has the new two-factor authentication values, you must complete the following tasks.

- If you configured an external gateway with RADIUS settings and that RADIUS server is not reachable within the same VNet as used by the pod, or within the peered VNet topology if you deployed the external gateway into its own VNet, verify that the RADIUS server that you specified in the gateway configuration allows client connections from the IP address of the external gateway’s load balancer. In an external gateway configuration, the Unified Access
Gateway instances attempt contact with the RADIUS server using that load balancer address. To allow the connections, ensure the load balancer resource's IP address that is in that external gateway’s resource group is specified as a client in your RADIUS server configuration.

- If you configured an internal gateway, or an external gateway and your RADIUS server is reachable within the same VNet as used by the pod, verify that the RADIUS server is configured to allow connections from the appropriate NICs that were created in the gateway's resource group in Microsoft Azure. Your network administrator determines the RADIUS server's network visibility to the pod's Azure Virtual Network and subnets. Your RADIUS server must allow client connections from the IP addresses of those gateway NICs that correspond to the subnet for which your network administrator has given network visibility to the RADIUS server. The gateway's resource group in Microsoft Azure has four NICs that correspond to that subnet, two that are currently active for the two Unified Access Gateway instances and two that are idle and will become the active ones after the pod goes through an update. To support connectivity between the gateway and the RADIUS server both for ongoing pod operations and after each pod update, ensure the IP addresses of those four NICs are specified as clients in the RADIUS server configuration.

For information on how to obtain those IP addresses, see Update Your RADIUS System with the Required Horizon Cloud Pod Gateway Information.

Customize the Session Timeout Setting in a Deployed Horizon Cloud Pod's Gateway Configuration

When a gateway is initially configured on a Horizon Cloud pod in Microsoft Azure, its session timeout value is the default Unified Access Gateway value of 10 hours (36000000 milliseconds). Using the Edit Pod workflow, you can edit the pod’s gateway configuration to customize that timeout value according to your own organization’s needs.

Prerequisites

The pod must already have the gateway configuration for which you want to customize the session timeout.

Procedure

1. From the pod's details page, open the Edit Pod window by clicking Edit.
2. In the Edit Pod window, click Next to move to the Gateway Settings step.
   This step has a section for the external gateway configuration and a section for the internal gateway configuration. The user interface reflects the pod's current configuration and the gateway settings it already has.
3. Locate the Session Timeout field for the gateway type for which you want to change it, either external or internal.
4 In **Session Timeout**, type a new value.

   If the pod has another gateway type and you want to change its session timeout value, repeat this step for that other gateway.

   The timeout value can be a minimum of 5 minutes (300,000 milliseconds).

5 Click **Save & Exit**.

**Results**

The system updates the session timeout in the pod's gateway configuration according to the value you typed for that gateway configuration.

**Replace a Gateway's SSL Certificate with a New One, Such as For a New Expiration Date or to Use a Different FQDN, For a Horizon Cloud Pod in Microsoft Azure**

Use this workflow to replace the SSL certificate that is in place on either type of gateway configuration that is deployed on your pod. You can also use this workflow to replace the fully-qualified domain name (FQDN) that is configured on the gateway, if you need to do that. One likely reason for replacing the SSL certificate is when the SSL certificate currently in place in the gateway configuration is nearing its expiration date. You perform these steps using the Edit Pod wizard in the Horizon Cloud Administration Console.

**Important**  If your environment is configured to use Workspace ONE Access with your pods, and your goal is to replace the SSL certificate used by the Workspace ONE Access Connector when communicating with the pod, there is a different set of steps to follow for that use case. Do not follow the steps below if your use case is about the Workspace ONE Access Connector integration with your pods. Those steps are completely different than the ones below. For an overview of Workspace ONE Access Connector integration and its needs, see *Configure a Horizon Cloud Pod in Microsoft Azure for Workspace ONE Access*. Also, if your deployment is a rare, atypical scenario where you are having your end users' clients and browser connect directly to the pod manager appliances, do not follow the steps below to replace the SSL certificate that is used in those rare scenarios. For a description of certificate configuration that applies in the Workspace ONE Access connector use case and the atypical, rare scenario use case, instead read *Overview of Configuring SSL Certificates on the Horizon Cloud Pod's Manager VMs, Primarily For Use By the Workspace ONE Access Connector*.

After time has passed since the pod's gateways were first deployed for the pod, you might find that you need to replace the SSL certificates that are configured on the pod's gateways or replace the FQDN that is configured on the gateways, or both. Typically, you give your end users an FQDN to use in their Horizon client or browser to access their pod-provisioned resources. As described in the topics *Log In to Desktops and RDS-Based Remote Applications Using a Browser* and *Log In to Desktops or RDS-Based Remote Applications Using the Horizon Client*, some end users open a browser and type in that FQDN while others might use one of the Horizon Clients. The SSL certificate that is configured on the gateway to which you tell end users to point their clients and browsers allows those clients and browser to trust connections to that gateway. As
described in Horizon Cloud Pod Deployed in Microsoft Azure, the pod can have an external Unified Access Gateway configuration, an internal type, or both. In either type of Unified Gateway configuration, the Unified Access Gateway instances are configured with FQDN and SSL certificate information.

You might want to replace the SSL certificate and FQDN that are configured on the pod’s gateways for various reasons. One reason might be because the in-place SSL certificate configured on a gateway has an expiration date in its certificate chain and that calendar date and time is approaching soon. In that situation, you would want to replace the SSL certificate prior to reaching the current one's expiration date, to prevent certificate trust issues in the end users' clients or browsers as they try to connect to the gateway. Another reason for replacing the SSL certificate is when you want your end users to begin using a different FQDN in their clients and browsers. Because the SSL certificate goes in tandem with an FQDN, when you want to change the FQDN to another one, you usually replace the SSL certificate with one that is based on the new FQDN.

**Note**  During the time the system is changing the configuration, end users who have connected sessions served by the pod will have those active sessions disconnected. No data loss will occur. After the configuration changes are complete, those users can reconnect.

**Prerequisites**

To complete this workflow, you must have:

- The replacement SSL certificate that meets the following criteria. That certificate should use the FQDN that you are having your end users use in their clients and browsers to connect to the pod's gateway for access to their entitled resources.

- A signed SSL server certificate (in PEM format) based on that FQDN. The Unified Access Gateway capabilities require SSL for client connections, as described in the Unified Access Gateway product documentation. The certificate must be signed by a trusted Certificate Authority (CA). The single PEM file must contain the full entire certificate chain with the private key. For example, the single PEM file must contain the SSL server certificate, any necessary intermediate CA certificates, the root CA certificate, and private key. OpenSSL is a tool you can use to create the PEM file.

**Important**  All certificates in the certificate chain must have valid time frames. The Unified Access Gateway VMs require that all of the certificates in the chain, including any intermediate certificates, have valid time frames. If any certificate in the chain is expired, unexpected failures can occur later as the certificate is uploaded to the Unified Access Gateway configuration.

- The FQDN that corresponds to that SSL certificate. This FQDN is the one used in your end users' clients and browsers to connect to the pod's gateway. If your reason for replacing the
SSL certificate is to avoid expiration date issues in your users' clients, you will likely be retaining the same FQDN that is already configured on the gateway, which will be displayed in the wizard. If you are also changing the FQDN to a new one, you must have one that is unique to this pod. You cannot reuse an FQDN that is already configured for your other pods.

**Important**  This FQDN cannot contain underscores. In this release, connections to the Unified Access Gateway instances will fail when the FQDN contains underscores.

**Procedure**

1. In the console, navigate to **Settings > Capacity** and click the pod's name to open its details page.

2. In the pod's details page, click **Edit**.

3. In the Edit Pod window, click **Next** to move to the **Gateway Settings** step.

4. Depending on the changes you need to make in the gateway configuration, complete the relevant step, in either the **External UAG** section or **Internal UAG** section.
   a. Replace the **FQDN** value with a new one.
   b. Replace the SSL certificate by clicking **Change** to upload the new certificate.

   Upload the certificate in PEM format that Unified Access Gateway will use to allow clients to trust connections to the Unified Access Gateway instances running in Microsoft Azure. The certificate must be based on the specified FQDN and be signed by a trusted CA.

5. Click **Save & Exit**.

   A confirmation message appears stating that updating the FQDN or certificate disconnects existing user connections and asking you to confirm the start of the workflow.

6. Click **Yes** to start the workflow.

   **Important**  If any of the certificates in the certificate chain has expired, the **Update status** will display **Update has failed**. If you see this, check the certificate file and verify that the certificates all have valid time frames.

**What to do next**

For whichever Unified Access Gateway configuration you changed, if you changed to an FQDN that is different from the previous one, ensure you update the CNAME record in your DNS server to map the FQDN of the configuration's load balancer to the new FQDN. See **Obtain the Pod Gateway's Load Balancer Information to Map in your DNS Server** for details.

**Convert a Certificate File to the PEM Format Required for Pod Deployment**

The Unified Access Gateway capability in your pod requires SSL for client connections. When you want the pod to have a Unified Access Gateway configuration, the pod deployment wizard requires a PEM-format file to provide the SSL server certificate chain to the pod's Unified Access Gateway configuration. The single PEM file must contain the full entire certificate chain including
the private key: the SSL server certificate, any necessary intermediate CA certificates, the root CA certificate, and private key.

For additional details about certificate types used in Unified Access Gateway, see the topic titled Selecting the Correct Certificate Type in the Unified Access Gateway product documentation.

In the pod deployment wizard step for the gateway settings, you upload a certificate file. During the deployment process, this file is submitted to the configuration of the deployed Unified Access Gateway instances. When you perform the upload step in the wizard interface, the wizard verifies that the file you upload meets these requirements:

- The file can be parsed as PEM-format.
- It contains a valid certificate chain and a private key.
- That private key matches the public key of the server certificate.

If you do not have a PEM-format file for your certificate information, you must convert your certificate information into a file that meets those above requirements. You must convert your non-PEM-format file into PEM format and create a single PEM file that contains the full certificate chain plus private key. You also need to edit the file to remove extra information, if any appears, so that the wizard will not have any issues parsing the file. The high-level steps are:

1. Convert your certificate information into PEM format and create a single PEM file that contains the certificate chain and the private key.
2. Edit the file to remove extra certificate information, if any, that is outside of the certificate information between each set of `----BEGIN CERTIFICATE----` and `-----END CERTIFICATE-----` markers.

The code examples in the following steps assume you are starting with a file named `mycaservercert.pfx` that contains the root CA certificate, intermediate CA certificate information, and private key.

**Prerequisites**

- Verify that you have your certificate file. The file can be in PKCS#12 (.p12 or .pfx) format or in Java JKS or JCEKS format.

**Important** All certificates in the certificate chain must have valid time frames. The Unified Access Gateway VMs require that all of the certificates in the chain, including any intermediate certificates, have valid time frames. If any certificate in the chain is expired, unexpected failures can occur later as the certificate is uploaded to the Unified Access Gateway configuration.

- Familiarize yourself with the `openssl` command-line tool that you can use to convert the certificate. See [https://www.openssl.org/docs/apps/openssl.html](https://www.openssl.org/docs/apps/openssl.html).

- If the certificate is in Java JKS or JCEKS format, familiarize yourself with the Java `keytool` command-line tool to first convert the certificate to .p12 or .pks format before converting to .pem files.
Procedure

1. If your certificate is in Java JKS or JCEKS format, use `keytool` to convert the certificate to `.p12` or `.pks` format.

   **Important** Use the same source and destination password during this conversion.

2. If your certificate is in PKCS#12 (.p12 or .pfx) format, or after the certificate is converted to PKCS#12 format, use `openssl` to convert the certificate to a `.pem` file.

   For example, if the name of the certificate is `mycaservercert.pfx`, you can use the following commands to convert the certificate:

   ```
   openssl pkcs12 -in mycaservercert.pfx -nokeys -out mycaservercertchain.pem
   openssl pkcs12 -in mycaservercert.pfx -nodes -nocerts -out mycaservercertkey.pem
   ```

   The first line above obtains the certificates in `mycaservercert.pfx` and writes them in PEM format to `mycaservercertchain.pem`. The second line above obtains the private key from `mycaservercert.pfx` and writes it in PEM format to `mycaservercertkey.pem`.

3. (Optional) If the private key is not in RSA format, convert the private key to the RSA private key format.

   The Unified Access Gateway instances require the RSA private key format. To check if you need to run this step, look at your PEM file and see if the private key information starts with

   ```
   -----BEGIN PRIVATE KEY-----
   ```

   If the private key starts with that line, then you should convert the private key to the RSA format. If the private key starts with `-----BEGIN RSA PRIVATE KEY-----`, you do not have to run this step to convert the private key.

   To convert the private key to RSA format, run this command:

   ```
   openssl rsa -in mycaservercertkey.pem -check -out mycaservercertkeyrsa.pem
   ```

   The private key in the PEM file is now in RSA format (`-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----`).

4. Combine the information in the certificate chain PEM file and private key PEM file to make a single PEM file.

   The example below shows a sample where the contents of `mycaservercertkeyrsa.pem` is first (the private key in RSA format), followed by the contents from `mycaservercertchain.pem`, which is your primary SSL certificate, followed by one intermediate certificate, followed by the root certificate.

   ```
   -----BEGIN CERTIFICATE-----
   .... (your primary SSL certificate)
   -----END CERTIFICATE-----
   ```
Note  The server certificate should come first, followed by any intermediate ones, and then the trusted root certificate.

5  If there are any unnecessary certificate entries or extraneous information between the BEGIN and END markers, edit the file to remove those.

Results

The resulting PEM file meets the requirements of the pod deployment wizard.

Update Your RADIUS System with the Required Horizon Cloud Pod Gateway Information

After you configure RADIUS two-factor authentication settings in a Horizon Cloud pod’s gateway configuration, you must also configure your RADIUS server's configuration to allow client requests from specific gateway-related IP addresses. The gateway’s Unified Access Gateway instances will attempt to communicate with the RADIUS server from specific IP addresses. Your network administrator determines the RADIUS server’s network visibility to the pod’s Azure Virtual Network (VNet) and subnets. The combination of that network visibility and the pod gateway type, external or internal, determines the specific gateway-related IP addresses that you must configure as allowed clients in your RADIUS server configuration.

Important  Follow the documentation that is appropriate for your RADIUS two-factor authentication system to see the syntax for the specific configuration file used in your RADIUS system in which you must configure this client information. As an example, as described in the FreeRADIUS wiki for FreeRADIUS client configuration, the /etc/raddb/clients.conf file contains the definitions of RADIUS clients as:

```
client NAME {
    ipaddr = IPADDRESS
    secret = SECRET
}
```

This topic describes the information from your Horizon Cloud pod that you must use in your RADIUS server to enable communication between the pod’s gateway and also to maintain resiliency of that communication after each pod update. To accept connections from client machines that attempt to reach it, RADIUS servers need to register the IPs of those client machines as allowed clients. In this case of a Horizon Cloud pod gateway configured with RADIUS
two-factor authentication settings, those client machines are that gateway's Unified Access Gateway instances. Usually your network administrator determines what network access the RADIUS server has to the VNet and the subnets that are connected to the deployed pod. The specific source IPs that the Unified Access Gateway instances use when contacting the RADIUS server depend on:

- Whether the gateway configuration is internal or external
- Whether your network administrator has configured the RADIUS server as accessible from inside the pod's VNet, or is located outside the VNet
- If the RADIUS server is accessible within the pod's VNet, from which of the pod's subnets in that VNet has your network administrator configured access to the RADIUS server

**Internal gateway configuration**

The Unified Access Gateway instances deployed for an internal gateway configuration use their NICs' private IP addresses to contact that RADIUS server. The RADIUS server sees the requests coming from source IP addresses that are the NICs' private IP addresses. Your network administrator has configured whether the RADIUS server is accessible to the pod's management or tenant subnet's IP address range. The internal gateway's resource group in Microsoft Azure has four (4) NICs that correspond to that subnet: two that are currently active for the two Unified Access Gateway instances and two NICs that are idle and will become the active ones after the pod goes through an update. To support the communication connectivity between the gateway and the RADIUS server both for ongoing pod operations and after each pod update, you must configure the RADIUS server to allow client connections from the IP addresses of the four NICs in the internal gateway's resource group in Microsoft Azure that correspond to the subnet that has visibility to the RADIUS server. See [How to Add Pod Gateway NICs' IP Addresses as Allowed Clients for Requests](#).

**External gateway configuration and the RADIUS server is accessible inside the pod's VNet**

When your network administrator has configured the RADIUS server to be accessible on the same VNet as the pod, the Unified Access Gateway instances use their NICs' private IP addresses to contact that RADIUS server. The RADIUS server sees the requests coming from source IP addresses that are the NICs' private IP addresses. Your network administrator has configured whether the RADIUS server is accessible to the pod's management, tenant, or DMZ subnet's IP address range. The external gateway's resource group in Microsoft Azure has four (4) NICs that correspond to that subnet: two that are currently active for the two Unified Access Gateway instances and two that are idle and will become the active ones after the pod goes through an update. To support the communication connectivity between the gateway and the RADIUS server both for ongoing pod operations and after each pod update, you must configure the RADIUS server to allow client connections from the IP addresses of the four NICs in the external gateway's resource group in Microsoft Azure that correspond to
the subnet that has visibility to the RADIUS server. See How to Add Pod Gateway NICs' IP Addresses as Allowed Clients for Requests.

External gateway configuration and the RADIUS server that is accessible outside the pod's VNet

When your network administrator has configured the RADIUS server outside of the pod's VNet, the external gateway configuration's Unified Access Gateway instances use the external gateway's Azure load balancer resource's IP address to contact that RADIUS server. You must configure the RADIUS server to allow client connections from the external gateway's load balancer resource's IP address. See How to Add the Pod External Gateway's Load Balancer IP Address as an Allowed Client for Requests.

How to Add Pod Gateway NICs' IP Addresses as Allowed Clients for Requests

When the pod is deployed, the pod deployer creates a set of NICs in the gateway's resource group in your Microsoft Azure subscription. The following screenshots are examples of the NICs for the internal gateway type and external gateway type. Even though the pod ID is pixelated out in these screenshots, you can see the pattern in which the deployer names the NICs, with -management, -tenant and -dmz in those names. For the names of the pod's resource groups, see Resource Groups Created For a Pod Deployed In Microsoft Azure.

```
<table>
<thead>
<tr>
<th>NIC Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmw-hcs-154158-05127-02254-00-1132121-01111-00-112000-00-uag-internal-nic1-management</td>
<td>Network interface</td>
</tr>
<tr>
<td>vmw-hcs-154158-05127-02254-00-1132121-01111-00-112000-00-uag-internal-nic1-tenant</td>
<td>Network interface</td>
</tr>
<tr>
<td>vmw-hcs-154158-05127-02254-00-1132121-01111-00-112000-00-uag-internal-nic2-management</td>
<td>Network interface</td>
</tr>
<tr>
<td>vmw-hcs-154158-05127-02254-00-1132121-01111-00-112000-00-uag-internal-nic2-tenant</td>
<td>Network interface</td>
</tr>
<tr>
<td>vmw-hcs-154158-05127-02254-00-1132121-01111-00-112000-00-uag-internal-nic3-management</td>
<td>Network interface</td>
</tr>
<tr>
<td>vmw-hcs-154158-05127-02254-00-1132121-01111-00-112000-00-uag-internal-nic3-tenant</td>
<td>Network interface</td>
</tr>
<tr>
<td>vmw-hcs-154158-05127-02254-00-1132121-01111-00-112000-00-uag-internal-nic4-management</td>
<td>Network interface</td>
</tr>
<tr>
<td>vmw-hcs-154158-05127-02254-00-1132121-01111-00-112000-00-uag-internal-nic4-tenant</td>
<td>Network interface</td>
</tr>
<tr>
<td>vmw-hcs-154158-05127-02254-00-1132121-01111-00-112000-00-uag1</td>
<td>Virtual machine</td>
</tr>
<tr>
<td>vmw-hcs-154158-05127-02254-00-1132121-01111-00-112000-00-uag2</td>
<td>Virtual machine</td>
</tr>
</tbody>
</table>
```
You need to obtain the IP addresses of the NICs for the gateway configuration on which you enabled RADIUS two-factor authentication which correspond to the subnet which has network visibility to the RADIUS server, and specify those IP addresses as allowed clients in your RADIUS server configuration.

**Important** To avoid any disruption in connectivity between your RADIUS server and the pod after an update, for each gateway that you configured with RADIUS settings, ensure that the IP addresses of the four (4) NICs that are described below are specified as allowed clients in your RADIUS server's configuration. Even though only half of the NICs are active during ongoing pod operations, they switch when the pod is updated. After a pod update, the other half of the NICs become active and the pre-update NICs go idle until the next pod update, when they switch back again. If you have not added all of the NIC IP addresses, both the active and idle ones, to your RADIUS server configuration, the RADIUS server will refuse connection requests from the post-pod-update now-active set of NICs, and the login process for end users using that gateway will break.

To obtain the gateway's NIC IP addresses to add to the RADIUS server configuration:

1. Obtain from your network administrator the information about which of the pod's subnets has network visibility to the RADIUS server (management, tenant, or dmz).
2. Log in to the Microsoft Azure portal for your subscription and locate the gateway's resource group.
3. For the NICs that correspond to the subnet that your network administrator says has visibility to the RADIUS server, click on each NIC and copy its IP address.
4. Add those NIC IP addresses to your RADIUS server client configuration file so that those NICs are allowed clients for the RADIUS server that you configured in the settings for that gateway.
The following line is an illustration of a portion of the client configuration lines for the NICs with IP addresses on the pod's tenant subnet for an internal gateway where the network administrator configured the RADIUS server inside the same VNet as the pod and with accessibility from the pod's tenant subnet. The pod's tenant subnet was configured as 192.168.25.0/22 when this pod was deployed. When the pod is initially deployed, the NIC1 and NIC2 are active and NIC3 and NIC4 are idle. However, all four of those NICs are added to the RADIUS server configuration to ensure that after the pod updates, when NIC3 and NIC4 become active and NIC1 and NIC2 go idle, the RADIUS server will continue to accept connections from this gateway. You must use the appropriate syntax for your own RADIUS server.

```plaintext
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
}
```

How to Add the Pod External Gateway’s Load Balancer IP Address as an Allowed Client for Requests

When the RADIUS server is located outside of the pod's VNet, for the external gateway on which you specified that RADIUS server, you must add the external gateway's Azure load balancer resource's public IP address as an allowed client in that RADIUS server configuration. You can obtain that load balancer IP address by using the Microsoft Azure portal and locating the load balancer resource in the gateway's resource group.

1. Log in to the Microsoft Azure portal for your subscription and locate the gateway's resource group.

2. In the gateway's resource group, click on the load balancer resource. It has a name in the pattern vmw-hcs-podID-uag-lb. Its IP address is listed in its overview information.
Add the gateway’s load balancer IP address to your RADIUS server client configuration file so that the gateway’s load balancer is an allowed client for the RADIUS server that you configured in the settings for that gateway. The following line is an illustrating example. You must use the appropriate syntax for your own RADIUS server.

```plaintext
client MYPODUAGEXTLBIP {
    ipaddr = 52.191.236.223
    secret = myradiussecret
}
```

Delete a Gateway Configuration from a Horizon Cloud Pod

To delete a gateway configuration from a Horizon Cloud pod deployed in Microsoft Azure, use the **Delete** action in the pod’s details page. As an example, after the pod is deployed, you might decide you want to set up that gateway type all over again with a new configuration. For that scenario, you first delete the existing gateway configuration from the pod and then edit the pod to set up the gateway again.

**Caution**

- Deleting the gateway configuration will immediately end all the user sessions that are connected to that gateway.
- Deleting the gateway is an irreversible action. You cannot recover the specific deleted gateway configuration. You can later edit the pod to add a new gateway configuration in place of the deleted one.
As described in Chapter 7 Introduction to Horizon Cloud Pods in Microsoft Azure, a pod can have an external gateway configuration or an internal one or both. You choose the specific type to delete from the Delete action. If you want to delete both gateway configurations from the pod, you must delete each one at a time.

**Important** During the time the system is changing the pod's configuration until it is finished, the following limitations apply:

- You cannot perform administration tasks on the pod. As an example, the Edit button in the pod detail's page will become unavailable until the changes to the pod are completed.
- End users who do not have connected sessions to their desktops or remote applications served by the pod and who attempt to connect cannot do so.
- End users who have connected sessions served by a gateway on the pod that you are not deleting will have those active sessions disconnected. No data loss will occur. After the configuration changes are complete, those users can reconnect using that remaining gateway.

**Tip** The console is dynamic. It will only make available in the user interface those workflows and toggles and fields that make sense and are appropriate based on the current configuration of the pod and the configuration of your overall environment.

**Procedure**

1. In the console, navigate to the Capacity page and click on the pod to open its details page.
2. Click the appropriate action for the gateway type you want to delete from the pod.
   - **Delete > External UAG**, to delete the pod's external gateway configuration.
   - **Delete > Internal UAG**, to delete the pod's internal gateway configuration.
3. Confirm the deletion.

**Results**

The system begins the process of deleting the gateway's resources in Microsoft Azure.

**Note** If you delete an external Unified Access Gateway configuration that was deployed into a resource group that you created, when the deletion process is completed, some non-pod artifacts might remain, such as the storage account for diagnostic logs and two images from which the Horizon Cloud deployer originally created the Connector VM and Unified Access Gateway VMs. If you want to, you can manually delete those artifacts after the deletion process is completed.

**What to do next**

Keep in mind that starting with pod manifest 2298.0, the pod must have at least one gateway configuration for supported operations. If you leave a pod of manifest 2298.0 or later without a gateway configuration, that pod is in an unsupported configuration. If you deleted the pod's sole
gateway configuration for a pod at manifest 2298.0 or later, you must add a gateway configuration to have the pod in a supported configuration. See Add a Gateway Configuration to a Deployed Horizon Cloud Pod.

Overview of Using Multiple Tenant Subnets with Your Horizon Cloud Pod for Your Farms and VDI Desktop Assignments

By configuring your pod with additional tenant subnets, you are able to specify using those subnets for your farms and VDI desktop assignments. Instead of having all farm and desktop VMs connected to the pod’s tenant subnet, you can specify for each farm and VDI desktop assignment the specific subnet or subnets to which you want their VMs connected. Without having additional VM subnets configured on the pod, all of your farm and VDI desktop VMs get connected to your pod’s tenant subnet by default. This feature to edit a pod to add multiple tenant subnets is available for pod manifests of 2298.0 or later.

Note These tenant subnets are also known as VM subnets. In the documentation and in the Horizon Cloud Administration Console, you might see reference to both names.

The additional VM subnets can be in the same VNet as the pod (the pod manager VMs) or can be in separate VNets that are peered with the VNet in which the core pod resides. When using peered VNets, those peered VNets must be in the same subscription and Microsoft Azure region as the pod.

Important When you add these additional VM subnets to your pod, you are responsible for adding the Network Security Groups (NSGs) using the Microsoft Azure portal to provide network isolation for them. The Horizon Cloud Edit Pod workflow does not create such NSGs for you.

When you use the pod deployer to create the pod in the first place, you specify a tenant subnet in the pod deployment wizard. That tenant subnet is known as the primary VM subnet. In the console, the pod detail’s page’s Networking section contains the information about the pod’s tenant subnets — both the primary one and any added ones. The following screenshot illustrates a pod that has not had any additional tenant subnets added to it yet. In this case, the pod was deployed using named subnets. The subnet named tenant was selected in the pod deployment wizard for the pod’s primary VM subnet. All of the core pod VMs, the gateway VMs, and the base image VMs have connections to this primary VM subnet.
This screenshot illustrates that same pod after two VM subnets are added to it — tenant5 and tenant6.

Operations that Happen as the Additional Subnets are Added

After you click Save & Exit in the Edit Pod workflow to add selected subnets, the system runs some background tasks that update the pod manager VMs and gateway VMs so that they can communicate over the added subnets with the farm VMs and desktop VMs that will eventually be attached to those subnets. If that update completes without errors, the added subnets are set to READY state. If an error occurs, the subnets are set to ERROR state.

This screenshot illustrates the added subnet in READY state.
If a subnet shows as ERROR, you can use the Redeploy failed networks action to retry the system tasks. On the pod's details page, click ... > Redeploy failed networks > .

**Removing Added VM Subnets from the Pod's Configuration**

If there are no farms or VDI desktop assignments using a VM subnet, you can use the Edit Pod workflow to remove the subnet from the pod's configuration. Start the Edit Pod workflow, unselect those subnets from the displayed list, and save your changes.

**Note** Removing the primary VM subnet from the pod is not supported. That subnet is the pod's required tenant subnet.

**About Using the VM Subnets for Farms and VDI Desktop Assignments**

**Important** Currently, you can use these VM subnets for VDI desktop assignments only when your environment is configured for using single-pod broker with your pods in Microsoft Azure. Use of multiple VM subnets with Pods in Microsoft Azure - Create a VDI Multi-Cloud Assignment, which are the system-default type of VDI desktop assignments when your tenant is configured with Universal Broker is not currently supported.

When the subnets are in READY state, you can use them in the definitions of farms and VDI desktop assignments. The farm VMs and VDI desktop VMs will get connected to the subnets that you specify in their definitions.

- You can specify these VM subnets for your farms and VDI desktop assignments both when creating them and when editing them.
- When you specify more than one VM subnet for a farm or VDI desktop assignment, the farm's or assignment's VMs are load balanced across the specified subnets.

**Note** When you create a farm or desktop assignment with these VM subnets, you have the option to select the pod's primary VM subnet (the pod's tenant subnet) along with the added VM subnets.

- In the current release, after you have assigned a subnet to a farm or desktop assignment, you cannot later unassign that subnet from the farm or desktop assignment.

**VM Subnet Status**

The colored icons on the pod detail's page indicates the status of these subnets. In the console, hover over the icon to see the status label.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PENDING</td>
<td>After you run the Edit Pod workflow to add a new tenant subnet, the subnet starts out in PENDING status while the system background tasks run. The time for this status is typically brief.</td>
</tr>
<tr>
<td>READY</td>
<td>If all operations related to the tenant subnet are successful, the indicator shows READY status.</td>
</tr>
</tbody>
</table>
### Status and Description

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR</td>
<td>If any operation related to the subnet fails, the indicator shows ERROR status.</td>
</tr>
<tr>
<td>DELETING</td>
<td>After you run the Edit Pod workflow to remove a tenant subnet, its indicator shows DELETING status while the system background tasks are in progress.</td>
</tr>
</tbody>
</table>

---

**Editing Your Horizon Cloud Pod to Make Use of Multiple Tenant Subnets for Farms and VDI Desktop Assignments**

To configure your pod with multiple tenant subnets, you use the Edit Pod workflow. These subnets are also called VM subnets. This feature where you can use multiple tenant subnets with your pods in Microsoft Azure is available for pod manifests of 2298.0 or later. You add these subnets to the pod's configuration so that you can use them for the VMs in your farms and VDI desktop assignments.

For an overview of the multiple tenant subnets feature, see [Overview of Using Multiple Tenant Subnets with Your Horizon Cloud Pod for Your Farms and VDI Desktop Assignments](#).

**Note** The maximum of additional tenant subnets that is supported for adding to the pod is thirty-nine (39). Therefore, the number of tenant subnets supported for the pod as a whole is forty — one primary tenant subnet and 39 additional subnets.

**Prerequisites**

Verify that the tenant subnets you want to add to the pod are already created in the Microsoft Azure portal. These subnets can be in the same VNet as the pod (the pod manager VMs) or can be in different VNets. If they are in different VNets, those VNets must be peered with the pod’s VNet. When using peered VNets, those peered VNets must be in the same subscription and Microsoft Azure region as the pod.

Verify that the tenant subnets are empty. Ensure that no other resource is attached to these subnets.

**Important** When you add these additional VM subnets to your pod, you are responsible for adding the Network Security Groups (NSGs) using the Microsoft Azure portal to provide network isolation for them. The Horizon Cloud Edit Pod workflow does not create such NSGs for you.

**Procedure**

1. Start the Edit Pod workflow from the pod's details page by clicking **Edit**.
2. Move to the **Pod Details** step and locate the **Networking** section.
   
   This section displays the pod's current network configuration. The **VM Subnet - Additional** area displays the VNets found in the pod's subscription. The icons next to each VNet indicate the number of subnets that are already connected to the pod.
3. Expand the VNet that has the subnets that you want to add to the pod.
   
   The set of subnets in the VNet are displayed. If you expand the VNet that is also used by the pod, the pod's primary VM subnet has an indicator next to it and it is already selected.
4 Select the subnets you want to add.

The following screenshot illustrates that a subnet named tenant is the pod's primary tenant subnet, and two additional subnets are selected for adding to the pod (tenant5 and tenant6).

5 Click Save & Exit.

Results

As described in Overview of Using Multiple Tenant Subnets with Your Horizon Cloud Pod for Your Farms and VDI Desktop Assignments, the system's background tasks run to make the necessary pod configuration changes. When those tasks successfully complete, the subnets appear in the READY state on the pod's details page.
What to do next

- Use the Microsoft Azure portal to add Network Security Groups (NSGs) for these subnets to provide network isolation for them. The Horizon Cloud Edit Pod workflow does not create such NSGs for you.

- With the VM subnets successfully added to the pod, you can start using them with your farms and VDI desktop assignments.

Change, Modify, and Update the Subscription Information Associated with Deployed Horizon Cloud Pods

In some circumstances, you might find you need to change, modify, or update the Microsoft Azure subscription information that is associated with the pods deployed in those subscriptions. Similarly, if you used the feature to deploy an external gateway using a subscription separate from the pod's subscription, you might find you need to change that subscription information.

You use the Manage Subscription workflow in the Horizon Cloud Administration Console to change, modify, or update the subscription information that is stored in your Horizon Cloud environment. The Manage Subscription workflow is also used to add new subscription information into your environment, as well as to delete subscription information that is no longer associated with any pods and that you wish to remove completely from being visible in Horizon Cloud.

How might you find yourself needing to change, modify, or update the Microsoft Azure subscription information that is associated with the deployed pods? Imagine that you created the subscription's application key to have it expire in one year and now the time is close to day 360. Before the final day 365 passes and the key expires, you would first need to use the Microsoft Azure portal to create a new key for the subscription and then immediately change the stored subscription information in the Horizon Cloud Administration Console to start using the new key.

When the subscription information on both sides matches — the Microsoft Azure portal side and the Horizon Cloud Administration Console side — the subscription information stored in your Horizon Cloud environment remains viable for use with the pods already deployed in that subscription.

You update the subscription information used by a pod or by its external gateway — when that gateway is deployed in a separate subscription — from the Capacity page's Resources tab. For a description of the subscription information fields, see Deploying Horizon Cloud Pods into Microsoft Azure from the Capacity Page.

Procedure

1. In the console, navigate to the Capacity page and click Resources.

   The following screenshot illustrates the Resources tab with two named subscriptions listed. Each name is a hyperlink. Clicking the hyperlink name opens a window in which you can change the stored information.
2 Click the displayed subscription name of the subscription you want to change to use new values.

When you click a hypertext name of the set for Microsoft Azure subscription information, the Manage Subscription window opens with the **Edit** action selected by default.
3 Type in new values for the ones you want to change to match the values you set for the subscription in the Microsoft Azure portal.

You can change the Subscription Name, Application ID, and Application Key. Even though the Application Key field has the icon to view the key, the key stays hidden. To type in a new subscription name, click Edit next to the Subscription Name menu in the Manage Subscription window.

**Note** The Subscription ID and Domain ID values cannot be updated.

4 Click Confirm.

Results

The new values are saved and stored in your Horizon Cloud environment.

**Horizon Cloud — Deleting, Editing, and Adding Microsoft Azure Subscription Information**

You use the Manage Subscription workflow in the Horizon Cloud Administration Console to edit or delete the Microsoft Azure subscription information that is stored in your Horizon Cloud environment. You can also use this workflow to add Microsoft Azure subscription information that you want stored in Horizon Cloud prior to deploying a pod into that subscription's capacity.
In addition to using your Microsoft Azure subscription information during the pod deployment process, Horizon Cloud must use your Microsoft Azure subscription information to run and manage the pods you have deployed into your subscription's capacity in the Microsoft Azure cloud. The subscription information that you specify in the pod deployment wizard is saved to your Horizon Cloud environment. The information is stored as a configuration setting, using a name that you specify. The Manage Subscription workflow provides for adding, editing, and deleting these stored subscription configurations.

**Manage Subscription - Microsoft Azure**

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
</tr>
<tr>
<td>Edit</td>
</tr>
<tr>
<td>Delete</td>
</tr>
</tbody>
</table>

**Subscription Name**

**Note** When there are no existing stored Microsoft Azure subscriptions, only the Add choice is available in the Action menu.

**How Do I Launch the Manage Subscription Workflow?**

You can launch the overall Manage Subscription workflow from either the Manage action on the console's Capacity page's Resources tab or from the Getting Started page. The following screenshot illustrates the location of the Manage action in the Capacity page.

You can also launch the workflow by clicking the name of a subscription that is listed on the Resources tab. Clicking a specific name will open the Manage Subscription window with that name selected by default in the Subscription Name field and the other fields prefilled with the information stored for that name.

**Note** When you open Manage Subscription by clicking a specific name, the Edit choice is pre-selected in the Action menu. The system assumes when you click on a specific item, you intend to update that specific configuration.
Editing an Existing Subscription

When you have changed the subscription information in the Microsoft Azure portal that Horizon Cloud relies on using with the deployed pods, you must update the corresponding information pieces in the configuration saved in Horizon Cloud. Only when the subscription information on both sides matches — the Microsoft Azure portal side and the Horizon Cloud Administration Console side — can the subscription information stored in your Horizon Cloud environment remain viable for use with the pods already deployed in that subscription. As an example, when you change the application ID for the subscription on the Microsoft Azure side, then you would log in to Horizon Cloud and use the Edit action of the Manage Subscription workflow to update the saved configuration's Application ID field to match.

For the editing steps, see Change, Modify, and Update the Subscription Information Associated with Deployed Horizon Cloud Pods.

Deleting an Existing Subscription

In addition to editing, the workflow also provides for deleting a stored configuration when all of the pods that were associated with that subscription name have been deleted. Deleting a stored configuration prevents that subscription name from appearing in the pod deployment wizard the next time you start to deploy a pod. Deleting such no-longer-used subscription names is useful when you have been doing trials or proof-of-concepts from the Horizon Cloud environment, where you are repeatedly deploying, then deleting, then re-deploying new pods and you want to remove the subscription information saved from the previous deployments.

To delete a named set of subscription information:

1. On the Capacity page's Resources tab, click the name of the subscription that you want to delete from Horizon Cloud. The following screenshot illustrates the clickable names sub1 and sub2.

2. In the Manage Subscription window that opens, verify the subscription name you clicked is the one you want to delete and select Delete in the Action menu. The following screenshot illustrates selection of the Delete action for the subscription information saved under the name sub2.
Note  If the subscription name has any pods associated with it, a message displays saying that you cannot delete it. Only subscription names that have zero pods associated with them can be deleted.

3  Click Confirm.

For the use case where you have deleted all of your pods that you had deployed into Microsoft Azure cloud and you want to delete all of the stored subscription information, navigate to the Getting Started page and use its Manage > Manage Subscriptions action to open the Manage Subscription window and delete the named sets of information.
Adding New Subscription Information

The Manage Subscription workflow also provides for adding a new set of subscription information and saving it to your Horizon Cloud environment outside of the pod deployment wizard. This use case is helpful when people on your team have distinct responsibilities — such as when one person on your team is responsible for adding all of the subscription information using specific while another person on your team is responsible for actually deploying the pods. The first person can add all of the information into Horizon Cloud prior to the pod deployment process.

**Important** When you are entering new information, you must ensure the subscription information you enter meets the subscription requirements described in Prerequisites for Running the Pod Deployment Wizard, especially that the service principal has the role permissions it needs. If the information does not meet the subscription requirements, when this named set of subscription information is selected in workflows such deploying a new pod, those workflows might fail.

To add a new set of subscription information and save it in Horizon Cloud:

1. On the Capacity page's Resources tab, click Manage.

   ![Capacity page with Manage highlighted](image)

   **Note** If you are adding a new subscription in the Getting Started page, click Manage > Manage Subscriptions.

2. In the Manage Subscription window, verify the Action is set to Add.

3. In Subscription Name, type a name that you want to use for this set of saved subscription information. The console will use this name in its pages and workflows that involve subscriptions. The name must start with a letter and contain only letters, dashes, and numbers.

4. Specify the Microsoft Azure subscription information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment</td>
<td>Select the cloud environment associated with your subscription, for example:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Azure - Commercial</strong>, for the standard global Microsoft Azure cloud regions</td>
</tr>
<tr>
<td></td>
<td>- <strong>Azure - China</strong>, for the Microsoft Azure in China cloud</td>
</tr>
<tr>
<td>Subscription ID</td>
<td>Enter your cloud capacity subscription ID (in UUID form). This subscription ID must be valid for the environment you selected. For Microsoft Azure, you can obtain this UUID from your Microsoft Azure portal's Subscriptions area.</td>
</tr>
</tbody>
</table>
Table: Microsoft Azure RDMA for Horizon Cloud

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Directory ID</strong></td>
<td>Enter your Microsoft Azure AD Directory ID (in UUID form). For Microsoft Azure, you can obtain this UUID from your Microsoft Azure Active Directory properties in the Microsoft Azure portal.</td>
</tr>
<tr>
<td><strong>Application ID</strong></td>
<td>Enter the application ID (in UUID form) associated with the service principal you created in the Microsoft Azure portal. Creating an application registration and its associated service principal in your Microsoft Azure Active Directory is a prerequisite.</td>
</tr>
<tr>
<td><strong>Application Key</strong></td>
<td>Enter the key value for the service principal's authentication key that you created in the Microsoft Azure portal. Creating this key is a prerequisite.</td>
</tr>
</tbody>
</table>

5 Click **Confirm**.

**Examine a Subscription's Current Usage of Your Microsoft Azure Limits Using the Horizon Cloud Administration Console**

Horizon Cloud monitors your pods' usage of your subscription's limits. The Microsoft Azure limits are also known as quotas. The Dashboard page displays health warning information when the usage gets close to reaching the maximum limits on your subscription. You can examine the current usage for a given subscription from the pod details page of any of that subscription's pods.

When you register with Microsoft Azure for a subscription, you sign up for a particular amount of capacity in terms of Microsoft Azure limits. Types of these limits are things like VMs per subscription and cores per subscription. Each of your pods uses quota from the pod’s associated subscription’s Microsoft Azure limits.

**Procedure**

1 In the console, navigate to **Settings > Capacity**, and open the details page for any of the pods in that subscription.
2 In the pod details page, locate the **Subscription Limits** field and click on the hyperlinked value to see the subscription's usage of various Microsoft Azure limits.

Results

If you see a high percentage of limits reported for a subscription, and the details show it is nearing close to the maximum number of cores or VMs from the various types, you can increase the number of cores allotted for that subscription in Microsoft Azure. You use the Microsoft Azure portal to increase the subscription's quotas for the various resources in the Microsoft Azure environment. Log into the portal and navigate to **Subscriptions**. Select the subscription name and then click **Usage + quotas** to see the subscription's usage levels. From that page, click **Request Increase** to get higher quotas for that subscription.

Updating Your Horizon Cloud Pod

VMware updates the Horizon Cloud software components periodically to include new features, improvements for service supportability and resiliency, user-experience improvements, and bug fixes. VMware typically updates the in-cloud management environment on a weekly basis and updates the software components used in a deployed pod on a roughly quarterly basis. When VMware updates the software components used in a deployed pod, the manifest number for the pod's software goes to a higher number. If there are improvements considered important for pod serviceability and support operations, VMware will make a new manifest available even if the
timing within a quarter of the previous manifest version. The normal update process takes place without incurring any system downtime.

**Important** If the pod is already integrated with the cloud-hosted Workspace ONE Access using the old Linux connector version 2017.12.1.0, you should update the connector to the latest supported version before updating the pod. To choose the connector version that is supported by this Horizon Cloud release, see the VMware Product Interoperability Matrixes at [https://www.vmware.com/resources/compatibility/sim/interop_matrix.php](https://www.vmware.com/resources/compatibility/sim/interop_matrix.php). Then update your existing connector by following the steps for your chosen connector version found in the VMware Workspace ONE Access documentation. After you have completed updating your connector, then update your pod.

Updating your deployed pod means appropriately moving your pod's current infrastructure components to a higher software manifest level. The infrastructure components are primarily the pod manager VMs and any Unified Access Gateway VMs that are configured for the pod. For example, a pod update can include updates for the pod management software or for the Unified Access Gateway software or for both.

You can use the Capacity page to see which pods have updates available for them. Navigate to **Settings > Capacity**. The pod's Status column will show the pending icon instead of the green dot, the pod's version number is a hyperlink instead of static text, and when your cursor hovers over that version number, a tooltip indicates an update is available. The following screenshot illustrates the behavior described in the preceding sentence.

![Capacity Page Screenshot](image)

You can see the update details for a specific pod on its details page. When an update is available, an on-screen message describing the update appears.
Note  After you have updated a pod from prior releases to later ones, you can then update the agent-related software in the pod’s already published images, farms, and VDI desktop assignments to the same agent version level that comes with the updated pod version. The agent-related update is done in a process separate from updating the pod itself. For the steps on how to update the agent-related software after the pod is updated, see Update Agent Software for RDSH Images in Horizon Cloud, Update Agent Software for Dedicated VDI Desktop Assignments, and Update Agent Software for Images Used by Floating VDI Desktop Assignments.

This Horizon Cloud pod update process is patterned after a software industry technique known as blue-green deployment.
The existing to-be-updated pod components are considered the blue components. Shortly after VMware releases a new pod manifest, the VMware Horizon Service Operations team runs some pre-checks and then designates your Horizon Cloud customer account as available to use the new manifest version. At the point in time when that new manifest version is designated in your customer account, the service builds a green set of components for the pod in your Microsoft Azure subscription. This green set is a parallel environments of the existing blue components.

**Note** Not all of the pod update process adheres exactly to a software industry blue-green deployment pattern. As an example, in the pod update process, when the newer instances are created alongside the existing ones, the newer ones are powered up and remain running until the pod has completed migrating to the new instances. Also, after the deployer validates the pod is successfully running on the newer components, the older VMs are deleted instead of remaining in an idle state.

**End-to-End Process**

Starting from when the VMware Operations team designates your customer account to use the new manifest version, the end-to-end sequence is:

1. The service creates a jump box resource group in the pod's subscription and deploys a jump box VM. This jump box VM orchestrates the creation of the green set of components.

2. The green set of components is created alongside the blue components, in the same resource groups. In the pod management resource group, the green set of pod manager VMs and their associated artifacts like NICs and disks are created. In the pod's gateway-related resource groups, the green set of Unified Access Gateway VMs are their associated artifacts are created. These green VMs are started and kept running until this entire end-to-end sequence is completed. The jump box VM and its resource group are deleted when the green components are successfully built and running.

**Important** Starting from this sequence point until the last step of the sequence, there are a duplicate number of VMs running: both the blue VMs and the green VMs. Therefore, it is prudent for you to schedule the update workflow to switch to the new pod software as soon as you see the notification banner that the update is available to move to, and schedule it for a day and time earlier rather than later.

This process does not cause any downtime, and the parallel VMs do not affect the pod's operations. Unless the system encounters errors that only you can resolve in your Microsoft Azure environment, no actions are required from you at this point. If the service encounters any issues in deploying the green components, it detects whether the remedy for those issues is within your control. If the service determines that you can remedy the issues, a notification appears in the administrative console. Because the remedy is in your control and cannot be resolved by VMware, if you get a notification of update errors, you must complete the actions to resolve them and then contact VMware support to continue the pod update process. For details about the types of issues that you can remedy, see [Cores Needed for](#)
Upgrading a Horizon Cloud Pod in Microsoft Azure and Remedies for Typical Pod Update Errors. If the service determines an issue can be resolved by the VMware Operations team, it alerts the VMware Operations team, which will resolve the issue without any actions from you.

3 On the pod's details page, a banner appears that says an update is available to move to and you can schedule the day and time for making the switch.

4 Next, you must schedule the update to move the pod from using its current blue VMs and components to the green ones. You schedule this update from the pod's summary page, by selecting Update > Schedule Updates. You set a day and time for the service to switch the pod to using the new green components. The service deploys a jump box VM to configure the scheduler in the pod, and then deletes the jump box VM until the scheduled day and time.

Important Before the update runs, remove any management locks in Microsoft Azure that you might have set on any of the pod's virtual machines (VMs). Any VMs with names that have a portion like vmw-hcs-podID, where podID is the pod's ID value, belong to the pod. Microsoft Azure provides an ability to use the Microsoft Azure portal to lock resources to prevent changes to them. Such management locks can be applied on an entire resource group or on individual resources. If you or your organization has applied management locks on the pod's VMs, those locks must be removed before the update runs. Otherwise, the update process will not successfully complete. You can locate the pod's ID value in the pod's details page from the Capacity page.

You determine the convenient time for the update to take place. Typically, the update itself, or the migration from the existing version to the new version, takes about ten minutes. As a best practice, schedule the update at a time when the environment is least busy. After the update is scheduled, the console displays the scheduled time in a top banner. You can reschedule the time for the update at any time prior to the scheduled time, if required by your organization's needs.

Important When you schedule the update in the pod's details page, you are prompted for a date and time. This time is local to your browser time zone.
At your selected day and time, the service again deploys a jump box VM to orchestrate the
switch for the pod to use the green VMs and components. The green components become
the current blue components. The process takes from five to fifteen minutes to complete,
with the longer times for pods that have both an external and internal Unified Access
Gateway configuration. The process migrates the data and configuration from your existing
to-be-updated pod's infrastructure to the new.

During the migration, the following limitations apply:

- You cannot perform administrative tasks on the pod that is undergoing the update.
- End users who do not have connected sessions to their virtual desktops or remote
  applications served by the updating pod and who attempt to connect cannot do so.
- End users who have connected sessions served by the updating pod will have those
  active sessions disconnected. After the migration is complete, those users can reconnect.
  No data loss will occur, unless you have used the Immediately option for the timeout
  handling in the farms and VDI desktop assignments.

Caution  Users with connected sessions to desktops or remote applications served by farms
and VDI desktop assignments with Logoff Disconnected Sessions set to Immediately will be
immediately disconnected and those disconnected sessions are also logged off immediately.
In those conditions, any in-progress user work is lost.

To avoid loss of in-progress end user data for this scenario, before the migration process
starts, adjust the Logoff Disconnected Sessions setting in the farms and VDI desktop
assignments to a time value that will give those users time to save their work. Then after the
update is finished, you can change the setting back to what it was before.
After everything is migrated to the new environment and the pod is successfully running on the new instances, the system deletes the blue VMs from the pod's resource groups, and the jump box resource group and its contents. Some artifacts, such as the NICs for the previous Unified Access Gateway instances, remain to preserve configuration values that are needed for the next pod update.

**After the End-to-End Process is Complete**

When the migration to the green components finishes, you can perform administrative tasks on the pod. To see the software version that a pod is currently running, select **Settings > Capacity** and click the pod to open its summary page. The page displays the current software version running. Click the software version number to see associated release information.

**Post-Update**

**Important** If your configured Radius server is deployed in same VNet, then after the migration to the new infrastructure elements, you must update the settings on your Radius server to accept the new private IP addresses for the new internal Unified Access Gateway VMs. This is a one-time requirement for the first update on the pod, and does not have to be repeated for that pod's future updates.

**Important** Starting with the September 2019 quarterly service release, the pod architecture is updated to support the ability to have high availability (HA). Even when the high availability feature is not enabled, the new HA-capable architecture includes a Microsoft Azure load balancer in front of the pod's manager VM. After you update your pod to manifest 1600, if your pod was configured for direct connections, you should remap your DNS settings to point to pod manager's Azure load balancer IP address that will be newly displayed in the updated pod's details page. Until you update the DNS mapping, even though those direct user connections will still work, they won't have the high availability fail over for an HA-enabled pod if the active-broker manager VM goes down. For this use case, you map an FQDN to the IP address in the **Pod Manager Load Balancer IP** field that is displayed on the pod's details page, as described in [Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs](#). Prior to pod manifest 1600, that IP was the one assigned to the pod's manager VM's NIC on the tenant subnet. Starting with pod manifest 1600 or later, the pod's IP address to map is the private IP address of the Microsoft Azure load balancer used for the pod's manager VMs. For existing pods that are updated to this release's manifest version, if you had configured a DNS name to point to the tenant appliance IP address for a pod of manifest 1493.1 or earlier, you should remap your DNS settings to point to the IP address displayed for the **Pod Manager Load Balancer IP** label in the updated pod's details page.
Cores Needed for Upgrading a Horizon Cloud Pod in Microsoft Azure and Remedies for Typical Pod Update Errors

When Horizon Cloud encounters errors in the pod update process that block its progress and which you can remedy, those errors are surfaced to you in the administrative console so that you can take the actions required to resolve them. The surfaced progress-blocking errors are under your control in your Microsoft Azure environment. Because the remedy is in your control and cannot be resolved by VMware, if you see notification of update errors in the console, you must complete the actions to resolve them and then contact VMware support to continue the pod update process.

*Updating Your Horizon Cloud Pod* describes how the update process works for a pod deployed in Microsoft Azure. Generally speaking, the update process follows a blue/green pattern, where the existing to-be-updated pod resources in the pod's main resource group and gateway-related resource groups are the blue components. The first step of the process is creation of a jump box resource group in your subscription, and deployment of a jump box VM in that resource group. That jump box VM then orchestrates the creation of a parallel set of pod VMs in your subscription, within the pod's existing resource groups. This parallel set are the green components in the blue/green pattern. The green components include VMs that are parallel to the ones in the pod's main resource group and gateway-related resource groups, such as the pod manager VMs and Unified Access Gateway VMs. These VMs are started and remain running alongside the to-be-updated pod's VMs (the blue set's VMs) until the end-to-end update process is finished. The end-to-end update process finishes only after you use the console to schedule the update and that scheduled activity runs and completes the switch of the pod from using the blue VMs to the green VMs. When the pod is using the green VMs, the blue VMs are stopped and removed, and the jump box VM and its resources are deleted.

Creating the green VMs cannot complete successfully if your Microsoft Azure environment cannot accommodate creating those parallel green VMs alongside the existing pod VMs. A typical key reason this occurs is when the pod's associated Microsoft Azure subscription does not have enough quota left to instantiate the jump box VM and the green VMs. Another reason that building out the green VMs can encounter errors is if your pod is currently offline. At the time you schedule the update in the console, Horizon Cloud deploys the jump box VM so that it can keep track of the schedule and be ready to kick off the migration of the pod to the newer components at the time you scheduled. If the pod's associated Microsoft Azure subscription does not have enough quota left to instantiate the jump box VM and keep it running through the time period from your scheduled time and when the switchover to the green VMs is finished, an update error is flagged for notification in the console.

For a description of the various system activities in the end-to-end pod update process, see *Updating Your Horizon Cloud Pod*.

**Update-Blocking Errors that can Typically Occur**

These are the update-blocking errors that can typically occur and which you can remedy in your Microsoft Azure environment.

**Subscription does not have the capacity available to instantiate the jump box VM.**
The update process is designed to instantiate a jump box VM in the pod's subscription when the system builds out the green components, when you use the scheduler to schedule the update, and at the scheduled time to orchestrate the switch from blue to green components. This jump box VM orchestrates the work to get the new components ready and run the actual migration process. Along with your current quota usage by your existing pods' VMs that are using the same subscription, your subscription's quota needs to allow for an additional VM of the Standard_F2 VM specification, 2 cores (vCPUs). This quota requirement is in addition to the VM types and cores required for creating the parallel green VMs.

**Subscription does not have enough of the appropriate cores (vCPUs) or VM sizes available to instantiate all of the VMs for the parallel green VMs.**

When the green components are built out, for each VM in your current pod, another VM gets created. As a result, you will have a duplicate number of pod manager VMs and Unified Access Gateway VMs from the time the green components are built out until the switch from the blue components to green components occurs at the time you scheduled in the console. To accommodate creating these green VMs, your subscription's quota levels for cores (vCPUs) from the relevant Microsoft VM families must be enough to encompass the parallel green VMs along with the quota you have already used from that subscription for its existing associated pods. See the quota and cores table below for the necessary cores for the various VM types and usages.

**Pod is currently offline, or is not currently able to communicate with Horizon Cloud.**

On the Capacity page, verify that the to-be-updated pod is reporting online status. Log in to the Microsoft Azure portal and check if the pod manager VM and its Unified Access Gateway VMs (if your pod has those) are running. If a VM is not running, power it on. For details about the resource groups in which those VMs are located, see Resource Groups Created For a Pod Deployed In Microsoft Azure.

**Quota and Cores Needed For the Time from Deploying the Green VMs to When the Switch to the Green Pod is Completed**

If you are notified about an update error due to lack of available cores, use the following table to see the additional quota you need. For the various VM types used in the current blue pod, the table at the end of this topic describes the quota used by those types, the additional quota needed when the green pod VMs are created, and the total quota needed for running both blue and green VMs from when the green VMs are created until the switch to the green VMs completes. For details about the VM family types and cores used by a pod, see the VM requirements for a pod documentation topic in the Deployment Guide.
### VM Types and Their Cores

<table>
<thead>
<tr>
<th>VM Type</th>
<th>Description</th>
<th>Total Quota for Running Blue VMs and Green VMs Until Switch to Green is Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard_D4_v3 VM type, 4 cores each</td>
<td>This VM type is used for the pod manager VMs.</td>
<td><strong>For a pod with a single manager VM</strong>&lt;br&gt;Your quota must allow for the 4 cores of the existing (blue) manager VM plus an additional 4 cores for the parallel green manager VM. Eight (8) cores to cover this usage.</td>
</tr>
<tr>
<td><strong>Note</strong> If the Standard_D4_v3 type is not available in your Microsoft Azure region, your pod is typically using Standard_D3_v2 VM type. That type also uses 4 cores.</td>
<td></td>
<td><strong>For a pod with high availability enabled, that has two manager VMs</strong>&lt;br&gt;Your quota must allow for the 8 cores of the existing (blue) manager VMs (2 VMs of 4 cores each) plus an additional 8 cores for the parallel green manager VMs. Sixteen (16) cores to cover this usage.</td>
</tr>
</tbody>
</table>

### Depending on what you chose when deploying the pod:
- **Standard_A4_v2 VM type (has 4 cores)**<br>This VM type is used for the Unified Access Gateway VMs in your pod's gateway configurations. The number of cores your subscription needs to support depends on which gateway types are configured on your pod.<br>
- **Standard_F8s_v2 (has 8 cores)**

**For a pod with only an external gateway**<br>That external gateway has two Unified Access Gateway VMs, therefore 2 VMs times the number of cores they have each. For the green set, your quota must allow for that total number of cores of the existing (blue) Unified Access Gateway VMs plus an additional duplicate number cores for the parallel green Unified Access Gateway VMs.
- For example, if your VMs are the Standard_A4_v2 with 4 cores each, you need 2 times 4 times 2 equals 16 cores to cover this usage.<br>- If your VMs are a VM size with 8 cores each, you need 2 times 8 times 2 equals 32 cores to cover that usage.<br>

**For a pod with only an internal gateway**<br>That gateway has two Unified Access Gateway VMs, therefore 2 VMs times the number of cores they have each. For the green set, your quota must allow for that total number of cores of the existing (blue) Unified Access Gateway VMs plus an additional duplicate number cores for the parallel green Unified Access Gateway VMs.<br>- For example, if your VMs are the Standard_A4_v2 with 4 cores each, you need 2 times 4 times 2 equals 16 cores to cover this usage.<br>- If your VMs are a VM size with 8 cores each, you need 2 times 8 times 2 equals 32 cores to cover that usage.<br>

**For a pod with both types of gateways**<br>That gateway has four Unified Access Gateway VMs, so 4 VMs times the number of cores they each have. For the green set, your quota must allow for 4
### VM Types and Their Cores

<table>
<thead>
<tr>
<th>VM Type</th>
<th>Description</th>
<th>Total Quota for Running Blue VMs and Green VMs Until Switch to Green is Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard_F2 VM, 2 cores</td>
<td>This VM is used for the jump box VM.</td>
<td>times the cores of the existing (blue) Unified Access Gateway VMs plus times two again for the parallel green Unified Access Gateway VMs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For example, if your VMs are the Standard_A4_v2 with 4 cores each, you need 4 times 4 times 2 equals 32 cores to cover this usage.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- If your VMs are a VM size with 8 cores each, you need 4 times 8 times 2 equals 64 cores to cover that usage.</td>
</tr>
</tbody>
</table>

### Backup and Restore Service for Horizon Cloud Pods in Microsoft Azure

Horizon Cloud pods deployed in Microsoft Azure of manifest version 1101 or later automatically participate in the Horizon Cloud backup and restore service. Manifest version 1101 was first made available in the Horizon Cloud December 2018 release.

**Note** If you do not want a pod to participate in the backup and restore service, please file a VMware support request (SR) to request disabling the feature for that pod.

#### Backups

The service takes daily backups of the following items for each pod: the pod's manager virtual machine (VM), Unified Access Gateway settings, Network Security Groups (NSGs), and key vaults. No other resources are backed up. The system retains up to seven (7) backups. The backups are saved in your Microsoft Azure subscription in a separate resource group, which has a name in the pattern `vmw-hcs–podID–recovery`. The `podID` is the pod's ID identifier that is listed in the pod's details, accessed from the administrative console's Capacity page.

Your Microsoft Azure subscription incurs a disk storage cost for the retained backups. Each disk is approximately 32 GB, so when the maximum of seven backups is reached, the incurred cost consists of 7 times the 32 GB disk storage cost applicable in your subscription's Microsoft Azure region.

If the system fails to take a daily backup, you will see a notification in the console. The VMware team is also alerted when the system fails to take the backup and will attempt to remedy and get backups resumed without any action from you.
Restores

To have a pod restored to one of the last 7 restore points, you make the request by filing a VMware SR. The VMware support team will advise you about the procedures as part of providing this overall service. The system's recovery process can recover the pod to the configuration that the backups hold in the last 7 restore points. After the system's recovery process, the VMware team will assist you to get the pod closer to its latest working state. After the pod is restored, some settings and configurations in the restored environment will require your input and for you to perform some actions in the environment. The VMware team will work with you during the post-restore reconfiguration steps to complete the process.

**Important** Because the backups are stored in a resource group in your Microsoft Azure subscription, if that resource group is lost, no restore is possible for the associated pod.

For pods of manifest 1600 and later, the pod architecture includes the Microsoft Azure Postgres database. This Microsoft Azure Postgres database is not backed up by the Horizon Cloud backup and restore service because the Microsoft Azure Postgres database is a Microsoft Azure managed service. If the pod's Microsoft Azure Postgres database is deleted, no restore is possible for that pod.

Change the Horizon Cloud Pod's NTP Setting

You can change the NTP settings for a pod deployed in Microsoft Azure by using the **Edit** action on the pod's details page.

**Procedure**

1. In the console, navigate to **Settings > Capacity** and click the pod's name to open its details page.
2. In the pod's details page, click **Edit**.
3. In the Edit Pod window, edit the settings in the **NTP Servers** field.
4. Click **Save & Exit** to save the new settings to the system.

Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs

Use this workflow when your scenario is integrating the Workspace ONE Access Connector appliance with the pod. The primary use of this workflow is for that integration, so that the Workspace ONE Access connector will trust SSL connections to the pod manager VMs. That is how integration of these pods with Workspace ONE Access works. The Workspace ONE Access Connector talks to the pod manager VMs through the Microsoft Azure load balancer that is in front of those appliances. Even though there might be some rare, atypical scenarios in which
some types of organizations would look to put an SSL certificate directly onto the pod manager VMs, those situations are uncommon and most organizations would not fall into those situations.

**Important** If your deployment does not involve the Workspace ONE Access Connector integrating with your pods, and your end users are pointing their clients and browsers to the FQDN that is for the pod's gateway configuration, these steps do not apply to that scenario. For that scenario, there is an entirely Replace a Gateway's SSL Certificate with a New One, Such as For a New Expiration Date or to Use a Different FQDN, For a Horizon Cloud Pod in Microsoft Azure. Performing the steps below will not change the SSL certificate that is on the gateway configurations. If your use case involves replacing the SSL certificate that is configured on one or more of the pod's gateway configurations, see instead Replace a Gateway's SSL Certificate with a New One, Such as For a New Expiration Date or to Use a Different FQDN, For a Horizon Cloud Pod in Microsoft Azure. You can examine the FQDN information displayed in the pod details page's gateway-related sections to check if you told your end users to point their clients or browsers to a gateway-related FQDN.

To learn about scenarios where the pod manager VMs get configured with SSL certificates, read about Overview of Configuring SSL Certificates on the Horizon Cloud Pod's Manager VMs, Primarily For Use By the Workspace ONE Access Connector. The primary use case is when you are integrating your pod with the Workspace ONE Access connector so that end users can access their pod-provisioned resources using Workspace ONE Access. To read about that integration workflow at Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access.

**Note** When you click Save in the steps below, Horizon Cloud will use those certificate files to configure the certificate on those VMs. This activity takes less than a minute.

The steps below are performed in the Horizon Cloud Administration Console.
Prerequisites

Before you start this workflow, verify that you have the required items described in Prerequisites for Running the Horizon Cloud Administration Console's Upload Pod Certificate Workflow to Configure SSL Certificates on the Horizon Cloud Pod's Manager VMs. Especially ensure that you have three certificate files that the console's workflow requires and that they meet the criteria described on that linked page.

Caution  Uploading and saving incorrect or improperly formed SSL certificate files to the pod can result in loss of access to the pod. To avoid inability to recover the pod, if you earlier notified VMware Support that you do not want the pod to participate in the backup and restore service that is provided by default for Horizon Cloud pods in Microsoft Azure, before you upload an SSL certificate to the pod, contact VMware Support to turn on the backup service for the pod to ensure a backup is available in case you lose access to the pod after uploading the certificate files. See Backup and Restore Service for Horizon Cloud Pods in Microsoft Azure for information about the default backup and restore service. If your pod manifest version is lower than 1101, contact VMware Support to update your pod so that it can participate in the backup and restore service.

Procedure

1  Select Settings > Capacity.

2  Open the pod's summary page by clicking the pod's name.

3  Click … > Upload Pod Certificate.

   The Upload Pod Certificate window opens. The following screenshot is an example of the window.

   ![Upload Pod Certificate Window](image)

   - CA Certificate File
   - SSL Certificate File
   - SSL Key File

4  For each of the certificate files listed in the Upload Pod Certificate window, click Select and navigate to where you have the file available to upload.
5 When the window shows that all of the certificate files are listed, click **Save**.

The following screenshot is an illustration of the window with all certificate files listed before saving them to the system.

---

**Results**

Horizon Cloud uses the certificate files to configure pod's manager VMs with your SSL certificate. This activity takes several seconds. You can verify the status in the pod's summary page.

---

**Overview of Configuring SSL Certificates on the Horizon Cloud Pod's Manager VMs, Primarily For Use By the Workspace ONE Access Connector**

For production systems, a key use case for configuring an SSL certificate on the Horizon Cloud pod's manager VMs is that of integrating Workspace ONE Access with the pod. The Workspace ONE Access connector has to be able to trust SSL connections to the pod manager VMs. That is how integration of these pods with Workspace ONE Access works. For this specific use case of integrating with the Workspace ONE Access connector, the pod needs SSL certificates to be set directly on the pod's manager VMs.

A key part of integrating Workspace ONE Access with a Horizon Cloud pod in Microsoft Azure is configuring the Workspace ONE Access connector to synchronize the Horizon Cloud Virtual Apps Collection that you set up in Workspace ONE Access to use the pod-provisioned desktops and remote applications. The Workspace ONE Access connector needs to communicate with the pod manager VMs to do that synchronization. Therefore the pod needs to present a valid SSL certificate so that the Workspace ONE Access connector will trust it. For more information about this integration, see **Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access**.
Relationship of the Pod Detail Page's Pod Manager Load Balancer IP Address Field to the Workspace ONE Access Connector's SSL Certificate Requirements

A key piece of information that you will need to create a valid trusted SSL certificate that can be configured on the pod manager VMs is the numerical IP address displayed in the pod detail page next to the label **Pod Manager Load Balancer IP**. The following screenshot is an illustration of where the **Pod Manager Load Balancer IP** label is displayed in the deployed pod's details page.

The trusted SSL certificate must be based on the fully qualified domain name (FQDN) that you map in your DNS server to the IP address that is displayed in that field. This mapping is needed so that an end user's client that is configured to use that FQDN can get a trusted connection to the pod.

Now, what is that numerical IP address related to? It is a private IP address from the pod's tenant subnet. The pod resource that IP address is associated with depends on whether the pod has manifest version 1600 or later, or has a manifest version earlier than 1600.

**Pods of manifest version 1600 or later**

For pods of manifest 1600 of later, the displayed numerical IP address shown for the label **Pod Manager Load Balancer IP** is the numerical private IP address for the pod's Azure load balancer resource. The pod architecture for pods of manifest 1600 or later includes a pod Azure load balancer with a private IP address from the pod's tenant subnet. That pod Azure load balancer is the point for the SSL communication to the pod manager VMs. As described in , when the high availability feature is enabled for that pod, it has two manager VMs behind that Azure load
balancer. In this case, when you click **Upload Certificate** in the administrative console to upload the SSL certificate files, Horizon Cloud performs the configuration on the active manager VM and then copies the certificate configuration to the other manager VM. When the high availability feature is not enabled for the pod, it has a single manager VM behind that Azure load balancer. When you click **Upload Certificate** in the console, Horizon Cloud configures the certificate on that manager VM.

The following screenshot depicts how the private IP address of the pod's Azure load balancer is the same IP address that is displayed next to that **Pod Manager Load Balancer IP** label in the pod's details page in the console for the preceding example.

**Pods of earlier manifest versions than 1600**

For pods of manifests earlier than 1600, the displayed numerical tenant IP address shown for the label **Pod Manager Load Balancer IP** is the numerical private IP address from the pod's tenant subnet that is associated with the tenant NIC on the pod manager VM. The pod architecture for earlier manifest versions have a single pod manager VM. The manager VM's private IP address on the tenant subnet is the point for the SSL communication to that manager VM. When you click **Upload Certificate** in the console, Horizon Cloud configures the certificate on that manager VM.

**How to Configure SSL Certificates on the Pod's Manager VMs**

You use the administrative console to configure the SSL certificates on the pod manager VMs. For the detailed steps, see [Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs](#). For the prerequisites before running those steps, see [Prerequisites for Running the Horizon Cloud Administration Console's Upload Pod Certificate Workflow to Configure SSL Certificates on the Horizon Cloud Pod's Manager VMs](#).

**Atypical Scenarios That Would Need SSL Certificates Configured on the Pod's Manager VMs**

Although these scenarios might be appropriate for proof-of-concepts, they are discouraged for production use. For production systems, you should leverage the Horizon Cloud features of internal and external gateway configurations that support end-user connections to their pod-provisioned resources. For end-user connections internal to your corporate network, such as
over a VPN, you should have an internal Unified Access Gateway configuration on the pod. For end-user connections over the Internet, you should have an external Unified Access Gateway configuration on the pod. For steps on adding those configurations to your pod, see Add a Gateway Configuration to a Deployed Horizon Cloud Pod.

Table 7-5. Atypical Scenarios That Would Require SSL Certificates Configured on the Pod Manager VMs

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod deployed with only the external gateway configuration, and no internal Unified Access Gateway configuration</td>
<td>In this scenario, while your end users over the Internet reach their pod-provisioned resources through the deployed external gateway configuration, there is no parallel internal gateway configuration for your users internal to your corporate network to use to reach their pod-provisioned resources. Without an internal Unified Access Gateway configuration, those internal users would have to point their client connections to reach the pod directly. To reach the pod directly means to point the client to the IP address displayed next to the Pod Manager Load Balancer IP label in the pod’s details page, or to an FQDN that you map to that displayed IP address in your DNS.</td>
</tr>
</tbody>
</table>
| Pod deployed without any gateway configuration whatsoever (zero Unified Access Gateway VMs) | In this scenario, all end user connections to pod-provisioned resources would have to use one of the operating-system-specific Horizon Clients to reach the pod directly. To reach the pod directly means to point the client to the IP address displayed next to the Pod Manager Load Balancer IP label in the pod’s details page, or to an FQDN that you map to that displayed IP address in your DNS.  

**Attention** Unlike when using one of the operating-system-specific Horizon Clients, when you point a browser to the pod directly, that browser connection will behave as an untrusted connection even when you have configured an SSL certificate on the pod’s manager VMs using the Upload Certificate action in the console. Typing the pod’s FQDN directly into a browser makes the browser connect using the HTML Access (Blast) connection type, and due to the way HTML Access (Blast) works, the browser will display the typical untrusted certificate error when it makes the connection direct to the pod. To avoid that displayed untrusted certificate error, the pod would need gateways configured so that you can have those browser connections go through the appropriate gateway configuration: an external gateway configuration for your end users sitting outside of your corporate network and an internal gateway configuration for your end users sitting inside your corporate network. If you do not want to expose your FQDN to the Internet, use an internal gateway configuration. The internal gateway configuration uses a Microsoft internal load balancer to which end users who are internal to your corporate network can point their connections. See Add a Gateway Configuration to a Deployed Horizon Cloud Pod.
Prerequisites for Running the Horizon Cloud Administration Console's Upload Pod Certificate Workflow to Configure SSL Certificates on the Horizon Cloud Pod's Manager VMs

Before you run the Upload Pod Certificate workflow, verify that you have satisfied these prerequisites. You must have the certificate-related files as described below to satisfy the Upload Pod Certificate window's criteria and allow the workflow to successfully complete.

- In your DNS server, map a fully qualified domain name (FQDN) to the IP address that is displayed in the pod's details page and which is labeled as **Pod Manager Load Balancer IP**. You can navigate to the pod's details page from the Capacity page and clicking on the pod's name. For the meaning of the IP address that is displayed next to the label **Pod Manager Load Balancer IP**, see Overview of Configuring SSL Certificates on the Horizon Cloud Pod's Manager VMs, Primarily For Use By the Workspace ONE Access Connector.

- Obtain a valid trusted SSL certificate based on that FQDN. That SSL certificate must be the following format needed for you to provide it into the console's Upload Pod Certificate window. Because the console's Upload Pod Certificate workflow requires specific elements, you must ensure that this SSL certificate adheres to the following characteristics:
  - Three separate files for uploading into the Upload Pod Certificate window:
    - A `CA.crt` file for the CA certificate.
    - A `SSL.crt` file for your CA-signed SSL certificate.
    - A `.key` file for the RSA private key, labeled **SSL Key File** in the window.

The following screenshot is an illustration of how the Upload Pod Certificate window looks where you provide those three files.
Ensure the CA certificate file and the SSL certificate files for this upload are in PEM format, which is a BASE64-encoded DER representation of an X.509 certificate. They must both have a .crt extension. When looking at their contents, these two files should look similar to the following example.

```
-----BEGIN CERTIFICATE-----
MIIFejCCA2KgAwIBAgIDAIi/MA0GCSqG
...............
-----END CERTIFICATE-----
```

Ensure the private key is without a password or passphrase associated with it. The .key file looks like the following example:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAoJmURboiFut+R34CNFibb9fjtI+cpDarUzqe8oGKFzEE/jmj
...............
-----END PRIVATE KEY-----
```

Before running the Upload Pod Certificate workflow, if you earlier notified VMware Support that you do not want the pod to use the default Horizon Cloud pod backup and restore service, you should contact VMware Support to turn on the backup service for the pod. Because uploading and saving incorrect or improperly formed SSL certificate files to the pod can result in loss of access to the pod, ensuring a backup is available is highly recommended in case you lose access to the pod after uploading the certificate files. See Backup and Restore Service for Horizon Cloud Pods in Microsoft Azure for information about the default backup and restore service. If your pod manifest version is lower than 1101, contact VMware Support to update your pod so that it can participate in the backup and restore service.

For steps used to configure the SSL certificate on the pod's manager VMs, see Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs.

**DNS Requirements for a Horizon Cloud Pod in Microsoft Azure**

For the pod deployment process to deploy your pod successfully into Microsoft Azure, you must configure your firewalls to allow the active pod manager to access the Domain Name Service (DNS) addresses it needs. In addition, your DNS must resolve specific names as described in this topic. In addition to the main pod deployment, when you are deploying the external gateway in
its own VNet, that VNet's subnet must meet the same DNS requirements as the separate pod VNet's management subnet, as described in this topic.

**Important** The pod deployment process uses a jump box VM. This jump box VM has ports and protocol requirements for the pod deployment process, as well as for configuring settings for the pod's Unified Access Gateway VMs when you are deploying a Unified Access Gateway configuration for the pod. See [Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates](#).

Deploying the external gateway into its own VNet also uses its own jump box VM, separate from the pod's. That jump box VM has its own ports and protocol requirements for the gateway deployment process. See [When the External Gateway is Deployed in its Own VNet: Ports and Protocols Required by the External Gateway Configuration's Jump Box During Gateway Deployments and Updates](#).

After a pod is successfully deployed, specific ports and protocols are required for ongoing Horizon Cloud operations. The specific ports and protocols required depends on whether the pod is at the manifest version for the September 2019 release, or is at a previous manifest version.

- For a pod created after the September 2019 release or updated to that release's manifest version or later, see [Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later](#). Such pods have manifest versions of 1593 or later.

- For a pod created before the September 2019 release and not yet updated to that release's manifest version, see [Ports and Protocols Requirements for a Horizon Cloud Pod Deployed Prior to the September 2019 Release](#). Such pods have manifest versions of 1493.1 or earlier.

- **DNS Requirements for the Overarching Pod Deployment Process, Pod Updates, and Ongoing Operations**
- **Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates**
- **When the External Gateway is Deployed in its Own VNet: Ports and Protocols Required by the External Gateway Configuration's Jump Box During Gateway Deployments and Updates**


DNS Requirements for the Overarching Pod Deployment Process, Pod Updates, and Ongoing Operations

You must ensure the following DNS names are resolvable and reachable from the management and tenant subnets using the specific ports and protocols as indicated in the following table. Horizon Cloud uses specific outbound ports to securely download the pod software into your Microsoft Azure environment and so that the pod can connect back to the Horizon Cloud control plane. You must configure your network firewall, network security group (NSG) rules, and proxy servers such that the active pod manager has the ability to contact the DNS addresses on the ports that it requires. Otherwise, the pod deployment process will fail.

**Important**

- When you are using the feature to deploy the external gateway into its own VNet, the management subnet in that VNet must meet the same DNS requirements as stated in the table below for the management subnet in the pod's VNet. The external gateway VNet's back-end subnet and DMZ subnet do not have specific DNS requirements.

- When you are deploying the pod with either an external gateway, an internal gateway, or both, you must upload a certificate that the pod deployer will configure in those gateway configurations. If the certificate or certificates that you supply for this purpose use CRLs (Certificate Revocation Lists) or OCSP (Online Certificate Status Protocol) settings that refer to specific DNS names, then you must ensure outbound Internet access on the VNet to those DNS names is resolvable and reachable. During configuration of your supplied certificate in the Unified Access Gateway gateway configuration, the Unified Access Gateway software will reach out to those DNS names to check the certificate's revocation status. If those DNS names are not reachable, pod deployment will fail during its Connecting phase. These names are highly dependent on the CA that you used to obtain the certificates, and therefore are not in VMware's control.

Your Welcome to Horizon Service email will indicate which regional control plane instance your tenant account was created in. Due to a known issue that existed when the welcome email was sent to you, the email you received might display the system string names used for the regions instead of human-friendly names. If you see a system string name in your welcome email, you can use the following table to relate what is shown in your email with the regional control plane DNS names.

**Table 7-6. Regions in Your Welcome Email Mapped to Regional Control Plane DNS Names**

<table>
<thead>
<tr>
<th>Your welcome email says</th>
<th>Regional DNS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>cloud.horizon.vmware.com</td>
</tr>
<tr>
<td>EU_CENTRAL_1 or Europe</td>
<td>cloud-eu-central-1.horizon.vmware.com</td>
</tr>
<tr>
<td>AP_SOUTHEAST_2 or Australia</td>
<td>cloud-ap-southeast-2.horizon.vmware.com</td>
</tr>
<tr>
<td>PROD1_NORHTCENTRALUS2_CP1 or USA-2</td>
<td>cloud-us-2.horizon.vmware.com</td>
</tr>
<tr>
<td>PROD1_NORTHEUROPE_CP1 or Europe-2</td>
<td>cloud-eu-2.horizon.vmware.com</td>
</tr>
</tbody>
</table>
Table 7-6. Regions in Your Welcome Email Mapped to Regional Control Plane DNS Names (continued)

<table>
<thead>
<tr>
<th>Your welcome email says</th>
<th>Regional DNS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROD1_AUSTRALIAEAST_CP1 or Australia-2</td>
<td>cloud-ap-2.horizon.vmware.com</td>
</tr>
<tr>
<td>Japan</td>
<td>cloud-jp.horizon.vmware.com</td>
</tr>
</tbody>
</table>

Table 7-7. Pod Deployment and Operations DNS Requirements

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>One of the following names, depending on which regional Horizon Cloud control plane instance is specified in your Horizon Cloud tenant account. The regional instance is set when the account is created, as described in Onboarding to Horizon Cloud for Microsoft Azure, Horizon On-Premises, and Horizon on VMware Cloud on AWS.</td>
<td>443</td>
<td>TCP</td>
<td>Regional Horizon Cloud control plane instance</td>
</tr>
<tr>
<td></td>
<td>- cloud.horizon.vmware.com</td>
<td></td>
<td></td>
<td>- United States: cloud.horizon.vmware.com, cloud-us-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-us-2.horizon.vmware.com</td>
<td></td>
<td></td>
<td>- Europe: cloud-eu-central-1.horizon.vmware.com, cloud-eu-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-ap-southeast-2.horizon.vmware.com</td>
<td></td>
<td></td>
<td>- Japan: cloud-jp.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-ap-2.horizon.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- cloud-jp.horizon.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>softwareupdate.vmware.com</td>
<td>443</td>
<td>TCP</td>
<td>VMware software package server. Used for downloading updates of the agent-related software used in the system's image-related operations.</td>
</tr>
</tbody>
</table>
Table 7-7. Pod Deployment and Operations DNS Requirements (continued)

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>One of the following names, depending on which of the regional DNS names apply to your account.</td>
<td>443</td>
<td>TCP</td>
<td>Horizon Cloud content delivery server. On the management subnet, this site is used for downloading the VHDs (virtual hard disks) for the pod’s manager and Unified Access Gateway VMs. Also used for the VHD for the gateway connector VM, in the case where the external gateway is in its own VNet) hydra-softwarelib-cdn.azureedge.net corresponds to regional instances for cloud.horizon.vmware.com, cloud-eu-central-1.horizon.vmware.com, cloud-ap-southeast-2.horizon.vmware.com. hydra-softwarelib-cdn.azureedge.net corresponds to regional instances for cloud-us-2.horizon.vmware.com, cloud-eu-2.horizon.vmware.com, cloud-ap-2.horizon.vmware.com, cloud-jp.horizon.vmware.com.</td>
</tr>
</tbody>
</table>
Table 7-7. Pod Deployment and Operations DNS Requirements (continued)

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>packages.microsoft.com</td>
<td>443 and 11371</td>
<td>TCP</td>
<td>Microsoft software package server. Used to securely download the Microsoft Azure Command Line Interface (CLI) software.</td>
</tr>
<tr>
<td>Management</td>
<td>azure.archive.ubuntu.com</td>
<td>80</td>
<td>TCP</td>
<td>Ubuntu software package server. Used by the pod-related Linux-based VMs for Ubuntu operating system updates.</td>
</tr>
<tr>
<td>Management</td>
<td>api.snapcraft.io</td>
<td>443</td>
<td>TCP</td>
<td>Ubuntu software package server. Used by the pod's Linux-based VMs for Ubuntu operating system updates.</td>
</tr>
<tr>
<td>Management</td>
<td>archive.ubuntu.com</td>
<td>80</td>
<td>TCP</td>
<td>Ubuntu software package server. Used by the pod's Linux-based VMs for Ubuntu operating system updates.</td>
</tr>
<tr>
<td>Management</td>
<td>changelogs.ubuntu.com</td>
<td>80</td>
<td>TCP</td>
<td>Ubuntu software package server. Used by the pod's Linux-based VMs for tracking Ubuntu operating system updates.</td>
</tr>
<tr>
<td>Management</td>
<td>security.ubuntu.com</td>
<td>80</td>
<td>TCP</td>
<td>Ubuntu software package server. Used by the pod's Linux-based VMs for security-related Ubuntu operating system updates.</td>
</tr>
</tbody>
</table>
Table 7-7. Pod Deployment and Operations DNS Requirements (continued)

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Management    | One of the following, depending on which Microsoft Azure cloud you are deploying your pod into:  
  - Microsoft Azure (global): login.microsoftonline.com  
  - Microsoft Azure Germany: login.microsoftonline.de  
  - Microsoft Azure China: login.chinacloudapi.cn  
  - Microsoft Azure US Government: login.microsoftonline.us |      | TCP      | This web address is generally used by applications to authenticate against Microsoft Azure services. For some descriptions in the Microsoft Azure documentation, see OAuth 2.0 authorization code flow, Azure Active Directory v2.0 and the OpenID Connect protocol, and National clouds. The National clouds topic describes how there are different Azure AD authentication endpoints for each Microsoft Azure national cloud. |
| Management    | One of the following, depending on which Microsoft Azure cloud you are deploying your pod into:  
  - Microsoft Azure (global): management.azure.com  
  - Microsoft Azure Germany: management.microsoftazure.de  
  - Microsoft Azure China: management.chinacloudapi.cn  
Table 7-7. Pod Deployment and Operations DNS Requirements (continued)

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Management    | One of the following, depending on which Microsoft Azure cloud you are deploying your pod into:  
  - Microsoft Azure (global): graph.windows.net  
  - Microsoft Azure Germany: graph.cloudapi.de  
  - Microsoft Azure China: graph.chinacloudapi.cn  
  - Microsoft Azure US Government: graph.windows.net | 443  | TCP      | Access to the Azure Active Directory (Azure AD) Graph API, which is used for the pod's programmatic access to Azure Active Directory (Azure AD) through OData REST API endpoints. |
| Management    | One of the following, depending on which Microsoft Azure cloud you have deployed your pod into:  
  - Microsoft Azure (global): *.blob.core.windows.net  
  - Microsoft Azure Germany: *.blob.core.cloudapi.de  
  - Microsoft Azure China: *.blob.core.chinacloudapi.cn  
  - Microsoft Azure US Government: *.blob.core.usgovcloudapi.net | 443  | TCP      | Used for the pod's programmatic access to the Azure Blob Storage. Azure Blob Storage is a service for storing large amounts of unstructured object data, such as text or binary data. |
| Management    | One of the following, depending on which Microsoft Azure cloud you have deployed your pod into:  
  - Microsoft Azure (global): *.vault.azure.net  
  - Microsoft Azure Germany: *.vault.microsoftazure.de  
  - Microsoft Azure China: *.vault.azure.cn  
  - Microsoft Azure US Government: *.vault.usgovcloudapi.net | 443  | TCP      | Used for the pod's ability to programatically work with the Azure Key Vault cloud service. Azure Key Vault is a cloud service that provides a secure store for secrets. |
<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>If your firewall or network security group (NSG) supports the use of service tags, one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Global Azure SQL service tag: Sql</td>
</tr>
<tr>
<td></td>
<td>- Region-specific SQL service tag for the Azure region where the pod is deployed: Sql.region, such as Sql.WestUS.</td>
</tr>
<tr>
<td></td>
<td>If your firewall or network security group (NSG) does not support the use of service tags, you can use the hostname of the database. This name follows the pattern *.postgres.database.azure.com.</td>
</tr>
<tr>
<td></td>
<td>Port 5432, Protocol TCP, Purpose Used for pod communication to the Microsoft Azure PostgreSQL database server.</td>
</tr>
<tr>
<td>Management</td>
<td>One of the following names, depending on which regional Horizon Cloud control plane instance is specified in your Horizon Cloud tenant account. The regional instance is set when the account is created, as described in Onboarding to Horizon Cloud for Microsoft Azure, Horizon On-Premises, and Horizon on VMware Cloud on AWS.</td>
</tr>
<tr>
<td></td>
<td>- connector-azure-us.vmwarehorizon.com</td>
</tr>
<tr>
<td></td>
<td>- connector-azure-eu.vmwarehorizon.com</td>
</tr>
<tr>
<td></td>
<td>- connector-azure-aus.vmwarehorizon.com</td>
</tr>
<tr>
<td></td>
<td>- connector-azure-jp.vmwarehorizon.com</td>
</tr>
</tbody>
</table>
|               | Port 443, Protocol TCP, Purpose Regional instance of the Universal Broker service  
- United States: connector-azure-us.vmwarehorizon.com  
- Europe: connector-azure-eu.vmwarehorizon.com  
- Australia: connector-azure-aus.vmwarehorizon.com  
- Japan: connector-azure-jp.vmwarehorizon.com
Table 7-7. Pod Deployment and Operations DNS Requirements (continued)

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant</td>
<td>One of the following names, depending on which of the regional DNS names apply to your account:</td>
<td>443</td>
<td>TCP</td>
<td>Horizon Cloud content delivery server. On the tenant subnet, this site is used by the system's automated Import Image process for downloading the installer for the agent-related software. d1mes20qfad06k.cloudfront.net corresponds to regional instances for cloud.horizon.vmware.com, cloud-eu-central-1.horizon.vmware.com, cloud-ap-southeast-2.horizon.vmware.com. hydra-softwarelib-cdn.azureedge.net corresponds to regional instances for cloud-us-2.horizon.vmware.com, cloud-eu-2.horizon.vmware.com, cloud-ap-2.horizon.vmware.com, cloud-jp.horizon.vmware.com.</td>
</tr>
<tr>
<td>Tenant</td>
<td>Depending on which regional Horizon Cloud control plane is specified in your Horizon Cloud account:</td>
<td>443</td>
<td>TCP</td>
<td>Cloud Monitoring Service (CMS)</td>
</tr>
<tr>
<td></td>
<td>North America:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>kinesis.us-east-1.amazonaws.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>query-prod-us-east-1.cms.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Europe:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>kinesis.eu-central-1.amazonaws.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>query-prod-eu-central-1.cms.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Australia:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>kinesis.ap-southeast-2.amazonaws.com</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 7-7. Pod Deployment and Operations DNS Requirements (continued)

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>query-prod-ap-southeast-2.cms.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Japan:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>kinesis.ap-northeast-1.amazonaws.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>query-prod-ap-northeast-1.cms.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates

As described in the Horizon Cloud Deployment Guide, a jump box VM is used in the initial creation of a pod and during subsequent software updates on the pod’s environment. After a pod is created, the jump box VM is deleted. Then, when a pod is being updated, the jump box VM is re-created to run that update process and is deleted when the update has completed. Such updates include when a pod is edited to add a Unified Access Gateway configuration.

Note A pod that is either deployed new in Microsoft Azure starting with the September 2019 release or which is updated to the September 2019 release manifest level and has high availability enabled will have two manager VMs. The following paragraphs use the plural word VMs to indicate the jump box VM must communicate with all of the pod’s manager VMs, whether the pod has only one or has two.

During those processes, that jump box VM communicates with:

- The pod’s manager VMs using SSH to the manager VMs’ port 22. As a result, during the pod deployment process and pod update process, the requirement that communication between the jump box VM and the manager VMs’ port 22 must be met. The manager VMs’ port 22 must be allowed between the jump box VM as a source and the manager VMs as a destination.

- The Unified Access Gateway VMs using HTTPS to those VMs’ port 9443, in the case where a pod is deployed with, or edited to add, a Unified Access Gateway configuration. As a result, during the pod deployment process and pod update process, when the pod configuration includes Unified Access Gateway, the requirement that communication between the jump box VM and the Unified Access Gateway VMs’ port 9443 must be met. The Unified Access Gateway VMs’ port 9443 must be allowed between the jump box VM as a source and the Unified Access Gateway VMs as a destination.

Because these VMs are assigned IP addresses dynamically, the network rules to allow this communication should use:

- The management subnet CIDR as both the source and destination, with destination port 22, source port any, and protocol TCP.
The management subnet CIDR as both the source and destination, with destination port 9443, source port any, and protocol TCP, when a Unified Access Gateway configuration is involved.

**Note**  Ongoing pod operations do not require availability of port 22 on the pod's manager VMs. However, if you make a support request to VMware and the support team determines the way to debug that request is to deploy a jump box VM for SSH communication to your pod's manager VMs, then you will have to meet this port requirement during the time the VMware support team needs the port for debugging your issue. The VMware support team will inform you of any requirements, as appropriate for any support situation.

**When the External Gateway is Deployed in its Own VNet: Ports and Protocols Required by the External Gateway Configuration's Jump Box During Gateway Deployments and Updates**

As described in the *Horizon Cloud Deployment Guide*, a jump box VM is used in the initial creation of the external gateway in its own VNet and during subsequent software updates on that gateway. After the external gateway is created in its own VNet, the jump box VM is deleted. Then, when that external gateway is being updated, the jump box VM is re-created to run that update process and is deleted when the update has completed. Such updates include when a pod is edited to add an external gateway in its own VNet.

During those processes, that jump box VM communicates with:

- During those processes, that jump box VM communicates with the gateway connector VM using SSH to that connector VM's port 22. As a result, during the gateway deployment process and update process, the requirement that communication between the jump box VM and the connector VMs' port 22 must be met. The connector VMs' port 22 must be allowed between the jump box VM as a source and the connector VMs as a destination.

- The Unified Access Gateway VMs using HTTPS to those VMs' port 9443. As a result, during the pod deployment process and pod update process, when the pod configuration includes Unified Access Gateway, the requirement that communication between the jump box VM and the Unified Access Gateway VMs' port 9443 must be met. The Unified Access Gateway VMs' port 9443 must be allowed between the jump box VM as a source and the Unified Access Gateway VMs as a destination.

Because these VMs are assigned IP addresses dynamically, the network rules to allow this communication should use:

- The management subnet CIDR as both the source and destination, with destination port 22, source port any, and protocol TCP.
The management subnet CIDR as both the source and destination, with destination port 9443, source port any, and protocol TCP.

**Note** Ongoing pod operations do not require availability of port 22 on the gateway connector's VM. However, if you make a support request to VMware and the support team determines the way to debug that request is to deploy a jump box VM for SSH communication to that gateway's connector VM, then you will have to meet this port requirement during the time the VMware support team needs the port for debugging your issue. The VMware support team will inform you of any requirements, as appropriate for any support situation.

### Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later

For ongoing Horizon Cloud operations, a pod that is either deployed new in Microsoft Azure starting with the September 2019 release and later, or which is updated to the September 2019 release level, has specific port and protocol requirements that are different from a pod that was deployed previously. Pods deployed new or updated to the September 2019 release have manifest versions of 1600 or later.

**Important** In addition to the ports and protocols described here, you must meet DNS requirements. For details, see [DNS Requirements for a Horizon Cloud Pod in Microsoft Azure](#).

### Ports and Protocols Required by Key Pod Components for Ongoing Operations

In addition to the DNS requirements, the ports and protocols in the following tables are required for the pod to operate properly for ongoing operations after deployment.

In the tables below, the term manager VM refers to the pod's manager VM. In the Microsoft Azure portal, this VM has a name that contains a part like `vmw-hcs-podID`, where `podID` is the pod's UUID, and a node part.

**Important** A pod that is enabled for high availability has two manager VMs. A pod that has high availability switched on has only one manager VM. In the tables below, wherever you see the term manager VM, it applies to all of the manager VMs in your high-availability-enabled pod unless otherwise indicated.

All pods at the September 2019 release's manifest version or later have a pod Microsoft Azure load balancer. The table rows that involve the pod's load balancer apply for all pods at the manifest level of 1600 or later.
<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Ports</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager VM</td>
<td>Pod’s other manager VM</td>
<td>4101</td>
<td>TCP</td>
<td>For a pod that is enabled with high availability, this traffic is JMS routing between the manager VMs.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Unified Access Gateway VMs</td>
<td>944</td>
<td>HTTPS</td>
<td>This port is used by the pod manager VM over the management subnet to configure settings in the pod’s Unified Access Gateway configuration. This port requirement applies when initially deploying a pod with a Unified Access Gateway configuration and when editing a pod to add a Unified Access Gateway configuration or update settings for that Unified Access Gateway configuration.</td>
</tr>
<tr>
<td>Pod’s Microsoft Azure load balancer</td>
<td>Manager VM</td>
<td>808</td>
<td>HTTP</td>
<td>Health checks of the VMs in the load balancer’s backend pool. When a pod at this release’s manifest version is not enabled with high availability, the load balancer has one manager VM in its backend pool.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Domain controller</td>
<td>389</td>
<td>TCP, UDP</td>
<td>LDAP services. Server that contains a domain controller role in an Active Directory configuration. Registering the pod with an Active Directory is a requirement.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Global catalog</td>
<td>326</td>
<td>TCP</td>
<td>LDAP services. Server that contains global catalog role in an Active Directory configuration. Registering the pod with an Active Directory is a requirement.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Domain controller</td>
<td>88</td>
<td>TCP, UDP</td>
<td>Kerberos services. Server that contains a domain controller role in an Active Directory configuration. Registering the pod with an Active Directory is a requirement.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>DNS server</td>
<td>53</td>
<td>TCP, UDP</td>
<td>DNS services.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>NTP server</td>
<td>123</td>
<td>UDP</td>
<td>NTP services. Server that provides NTP time synchronization.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>True SSO Enrollment Server</td>
<td>3211</td>
<td>TCP</td>
<td>True SSO Enrollment Server. Optional if you are not using True SSO Enrollment Server capabilities with your pods.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Workspace ONE Access service</td>
<td>443</td>
<td>HTTPS</td>
<td>Optional if you are not using Workspace ONE Access with the pod. Used to create a trust relationship between the pod and the Workspace ONE Access service. Ensure that the pod can reach the Workspace ONE Access environment you are using, either on-premises or the cloud service, on port 443. If you are using the Workspace ONE Access cloud service, see also the list of Workspace ONE Access service IP addresses to which the Workspace ONE Access Connector and the pod must have access in the VMware Knowledge Base article 2149884.</td>
</tr>
</tbody>
</table>
Table 7-8. Pod Operations Ports and Protocols (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transient Jump box VM</td>
<td>Manager VM</td>
<td>22</td>
<td>TCP</td>
<td>As described above in Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates, a transient jump box is used during pod deployment and pod update processes. Even though ongoing processes do not require these ports, during pod deployment and pod update processes, this jump box VM must communicate with the manager VMs using SSH to the manager VM's port 22. For details about the cases for which the jump box VM needs this communication, see Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates.</td>
</tr>
<tr>
<td>Transient Jump box VM</td>
<td>Unified Access Gateway VMs</td>
<td>944</td>
<td>HTTPS</td>
<td>This port is used by the jump box VM over the management subnet to configure settings in the pod's Unified Access Gateway configuration. This port requirement applies when initially deploying a pod with a Unified Access Gateway configuration and when editing a pod to add a Unified Access Gateway configuration to a pod.</td>
</tr>
</tbody>
</table>

Note: A pod that is at manifest version 1600 or later and has the high availability feature enabled on it, will have two manager VMs. The preceding paragraph uses the plural word VMs to indicate the jump box VM must communicate with all of the pod's manager VMs, whether the pod has only one or has two.

Gateway Connector VM Ports and Protocols Requirements

This table applies to the gateway's connector VM that is used when you have deployed the external gateway in a separate VNet. In addition to the DNS requirements, the ports and protocols in the following table are required for the external gateway to operate properly for ongoing operations after deployment.

In the table below, the term connector VM refers to the gateway's connector VM which manages the connection between the cloud management plane and the external gateway. In the Microsoft Azure portal, this VM has a name that contains a part like vmw-hcs-ID, where ID is the gateway's deployer ID, and a node part.
Table 7-9. Pod Operations Ports and Protocols

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector VM</td>
<td>DNS server</td>
<td>53</td>
<td>TCP/UDP</td>
<td>DNS services.</td>
</tr>
<tr>
<td>Connector VM</td>
<td>NTP server</td>
<td>123</td>
<td>UDP</td>
<td>NTP services. Server that provides NTP time synchronization.</td>
</tr>
<tr>
<td>Transient Jump box VM</td>
<td>Connector VM</td>
<td>22</td>
<td>TCP</td>
<td>As described above in Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates, a transient jump box is used during deployment of the external gateway and during update processes. Even though ongoing processes do not require these ports, during deployment and update processes, this jump box VM must communicate with the connector VM using SSH to the connector VMs' port 22.</td>
</tr>
</tbody>
</table>

Unified Access Gateway VM Ports and Protocols Requirements

In addition to the DNS and above primary ports and protocols requirements, the ports and protocols in the following tables are related to the gateways that you have configured on the pod to operate properly for ongoing operations after deployment.

For connections using a high-availability-enabled pod configured with Unified Access Gateway instances, traffic must be allowed from the pod’s Unified Access Gateway instances to targets as listed in the table below. During pod deployment, a Network Security Group (NSG) is created in your Microsoft Azure environment for use by the pod’s Unified Access Gateway software.

Table 7-10. Port Requirements for Traffic from the Pod’s Unified Access Gateway Instances

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Access Gateway</td>
<td>Pod’s Microsoft Azure load balancer</td>
<td>8443</td>
<td>TCP</td>
<td>Login authentication traffic. The traffic from the Unified Access Gateway instances reaches the pod’s manager VM through the pod’s load balancer.</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>4172</td>
<td>TCP/UDP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>22443</td>
<td>TCP/UDP</td>
<td>Blast Extreme By default, when using Blast Extreme, client-drive redirection (CDR) traffic and USB traffic is side-channeled in this port. If you prefer instead, the CDR traffic can be separated onto the TCP 9427 port and the USB redirection traffic can be separated onto the TCP 32111 port.</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>9427</td>
<td>TCP</td>
<td>Optional for client driver redirection (CDR) and multimedia redirection (MMR) traffic.</td>
</tr>
</tbody>
</table>
Table 7-10. Port Requirements for Traffic from the Pod’s Unified Access Gateway Instances (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>32111</td>
<td>TCP</td>
<td>Optional for USB redirection traffic.</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Your RADIUS instance</td>
<td>1812</td>
<td>UDP</td>
<td>When using RADIUS two-factor authentication with that Unified Access Gateway configuration. The default value for RADIUS is shown here.</td>
</tr>
</tbody>
</table>

Ports and Protocols Required by Universal Broker

To support the use of Universal Broker for the brokering of end-user assignments from a pod, you must configure port 443 as described in the following table. The active pod manager establishes a persistent WebSocket connection with the Universal Broker service through port 443 and receives connection requests from the Universal Broker service through a randomly selected port.

Table 7-11. Port Requirements for Universal Broker

<table>
<thead>
<tr>
<th>Source</th>
<th>Source Port</th>
<th>Target</th>
<th>Target Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active pod manager</td>
<td>Randomly selected from available ports</td>
<td>Universal Broker service</td>
<td>443</td>
<td>HTTPS initially, then WebSocket</td>
<td>Establishes a persistent WebSocket connection with the Universal Broker service</td>
</tr>
</tbody>
</table>

End-User Connection Traffic Ports and Protocols Requirements

For detailed information about the various Horizon Clients that your end users might use with your Horizon Cloud pod, see the Horizon Client documentation page at https://docs.vmware.com/en/VMware-Horizon-Client/index.html. Which ports must be opened for traffic from the end users’ connections to reach their pod-provisioned virtual desktops and remote applications depends on the choice you make for how your end users will connect:

**When you choose the deployer option for having an external gateway configuration in the pod’s own VNet**

The deployer deploys Unified Access Gateway instances in your Microsoft Azure environment, along with a Microsoft Azure load balancer resource to those instances in that
load balancer's backend pool. That load balancer communicates with those instances' NICs on the DMZ subnet, and is configured as a public load balancer in Microsoft Azure. The diagram Figure 7-1. Illustration of the Horizon Cloud Pod Architecture for a Pod with High Availability Enabled and Configured with Both External and Internal Unified Access Gateway Configurations depicts the location of this public load balancer and the Unified Access Gateway instances. When your pod has this configuration, traffic from your end users on the Internet goes to that load balancer, which distributes the requests to the Unified Access Gateway instances. For this configuration, you must ensure that those end-user connections can reach that load balancer using the ports and protocols listed below. Post-deployment, the external gateway's load balancer is located in the resource group named vmw-hcs-podID-uag, where podID is the pod's UUID.

When you choose the deployer option for having an internal Unified Access Gateway configuration

An internal gateway configuration is deployed into the pod's own VNet by default. The deployer deploys Unified Access Gateway instances in your Microsoft Azure environment, along with a Microsoft Azure load balancer resource to those instances in its backend pool. That load balancer communicates with those instances' NICs on the tenant subnet, and is configured as an internal load balancer in Microsoft Azure. The diagram Figure 7-1. Illustration of the Horizon Cloud Pod Architecture for a Pod with High Availability Enabled and Configured with Both External and Internal Unified Access Gateway Configurations depicts the location of this internal load balancer and the Unified Access Gateway instances. When your pod has this configuration, traffic from your end users in your corporate network goes to that load balancer, which distributes the requests to the Unified Access Gateway instances. For this configuration, you must ensure that those end-user connections can reach that load balancer using the ports and protocols listed below. Post-deployment, the internal gateway's load balancer is located in the resource group named vmw-hcs-podID-uag-internal, where podID is the pod's UUID.

When you choose the deployer options either for having an external gateway configuration in its own VNet and not the pods, or the option to use its own subscription (which is a special sub-case of using its own VNet because VNets do not span subscriptions)

The deployer deploys Unified Access Gateway instances in your Microsoft Azure environment, along with a Microsoft Azure load balancer resource to those instances in that load balancer's backend pool. That load balancer communicates with those instances' NICs on the DMZ subnet, and is configured as a public load balancer in Microsoft Azure. The diagram Figure 7-2. Illustration of the External Gateway's Architecture Elements When the External Gateway is Deployed into Its Own VNet, Separate from the Pod's VNet depicts the location of this public load balancer and the Unified Access Gateway instances in the gateway's own VNet. When your pod has this configuration, traffic from your end users on the Internet goes to that load balancer, which distributes the requests to the Unified Access Gateway instances. For this configuration, you must ensure that those end-user connections can reach that load balancer using the ports and protocols listed below. Post-deployment, the external gateway's load balancer is located in the resource group named vmw-hcs-ID-uag,
where ID is the value show in the **Deployer ID** field of the pod’s details page. As described in the Administration Guide, you get to the pod’s details page from the console’s Capacity page.

**When you choose to have zero Unified Access Gateway configurations on the pod, such as when you are integrating Workspace ONE Access with the pod or are allowing internal users to connect directly over VPN**

**Attention** In production systems, for internal-user access, the best practice is to use an internal Unified Access Gateway gateway configuration on the pod, and not direct connections to the pod.

When Workspace ONE Access is integrated with the pod, you typically have your end users connect through Workspace ONE Access. When Workspace ONE Access is integrated with a Horizon Cloud pod in Microsoft Azure, you must configure it pointing directly to the pod. No Unified Access Gateway configuration is needed on the pod then, when your end users are connecting to their pod-provisioned resources using Workspace ONE Access. For this configuration, you upload an SSL certificate to the pod’s manager VMs using the pod’s summary page in the console, as described in Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs. Then you complete the steps to integrate Workspace ONE Access with the pod.

Table 7-12. External End User Connections Ports and Protocols when the Pod Configuration has External Unified Access Gateway instances

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic. Can also carry client-drive redirection (CDR), multimedia redirection (MMR), USB redirection, and tunneled RDP traffic. SSL (HTTPS access) is enabled by default for client connections. Port 80 (HTTP access) can be used in some cases. See Understanding What URL Content Redirection Is.</td>
</tr>
<tr>
<td>Client</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Horizon</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>4172</td>
<td>TCP, UDP</td>
<td>PCoIP via PCoIP Secure Gateway on Unified Access Gateway</td>
</tr>
<tr>
<td>Client</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Horizon</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Client</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 7-12. External End User Connections Ports and Protocols when the Pod Configuration has External Unified Access Gateway instances (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>UDP</td>
<td>Blast Extreme via the Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>844</td>
<td>UDP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic (adaptive transport).</td>
</tr>
<tr>
<td>Browser</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>

Table 7-13. Internal End User Connections Ports and Protocols when the Pod Configuration has Internal Unified Access Gateway instances

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic. Can also carry client-drive redirection (CDR), multimedia redirection (MMR), USB redirection, and tunneled RDP traffic. SSL (HTTPS access) is enabled by default for client connections. Port 80 (HTTP access) can be used in some cases. See Understanding What URL Content Redirection Is.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>4172</td>
<td>TCP</td>
<td>PCoIP via PCoIP Secure Gateway on Unified Access Gateway</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Source</td>
<td>Target</td>
<td>Port</td>
<td>Protocol</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------</td>
<td>------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>UDP</td>
<td>Blast Extreme via the Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>844</td>
<td>UDP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic (adaptive transport).</td>
</tr>
<tr>
<td>Browser</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Pod's Microsoft Azure load balancer</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic. The traffic from the clients reaches the pod's manager VMs through the pod's load balancer.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>4172</td>
<td>TCP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>22443</td>
<td>TCP</td>
<td>Blast Extreme</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>32111</td>
<td>TCP</td>
<td>USB redirection</td>
</tr>
</tbody>
</table>
Table 7-14. Internal End User Connections Ports and Protocols when using Direct Pod Connections, Such as Over VPN (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>9427</td>
<td>TCP</td>
<td>Client-drive redirection (CDR) and multimedia redirection (MMR)</td>
</tr>
<tr>
<td>Browser</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>

**Ports and Protocols Requirements for Traffic from the Horizon Agent in the Base VM, VDI Desktop VMs, and Farm RDSH VMs**

The following ports must allow traffic between the Horizon agent-related software that is installed in the base VMs, desktop VMs, and farm RDSH VMs and the pod's manager VMs.
<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon agent in the base imported VM, golden images, desktop VMs, farm RDSH VMs</td>
<td>Manager VM</td>
<td>4001</td>
<td>TCP</td>
<td>Java Message Service (JMS, non-SSL), used by the agent in the VM to communicate with the pod as part of the certificate thumbprint verification and exchange to secure an SSL connection to the pod. After the keys are negotiated and exchanged between the VM and the pod manager, the agent uses port 4002 to create a secured SSL connection. For example, the Reset Agent Pairing action on the Imported VMs page requires communication over port 4001 for that agent pairing workflow between the base imported VM and the pod. <strong>Note</strong> Both ports 4001 and 4002 are required for steady-state operations. There are times when the agent might need to re-key with the pod, so port 4001 must be kept open.</td>
</tr>
<tr>
<td>Horizon agent in the base imported VM, the golden images, desktop VMs, farm RDSH VMs</td>
<td>Manager VM</td>
<td>4002</td>
<td>TCP</td>
<td>Java Message Service (JMS, SSL), used by the agent in these VMs to communicate with the pod using a secured SSL connection.</td>
</tr>
<tr>
<td>FlexEngine agent (the agent for VMware Dynamic Environment Manager) in the desktop or farm RDSH VMs</td>
<td>Those file shares that you set up for use by the FlexEngine agent that runs in the desktop or farm RDSH VMs</td>
<td>445</td>
<td>TCP</td>
<td>FlexEngine agent access to your SMB file shares, if you are using VMware Dynamic Environment Manager capabilities.</td>
</tr>
</tbody>
</table>

As part of the pod deployment process, the deployer creates network security groups (NSGs) on the network interfaces (NICs) on all of the deployed VMs. For details about the rules defined in those NSGs, see [Default Network Security Group Rules for the VMs in a Horizon Cloud Pod Deployed in Microsoft Azure](#).

**Note** Instead of listing DNS names, IP addresses, ports, and protocols in a Horizon Cloud Knowledge Base (KB) article, we have provided them here as part of the core Horizon Cloud documentation.
Ports and Protocols Requirements for a Horizon Cloud Pod Deployed Prior to the September 2019 Release

For ongoing Horizon Cloud operations, a pod that was deployed in Microsoft Azure prior to the September 2019 release has specific port and protocol requirements that are different from a pod that is deployed at the manifest version of the September 2019 release, or which is updated to the September 2019 release’s manifest version. A pod that was deployed prior to the September 2019 release has a manifest version of 1493.1 or earlier.

**Important** In addition to the ports and protocols described here, you must meet DNS requirements. For details, see DNS Requirements for a Horizon Cloud Pod in Microsoft Azure.

Ports and Protocols Required for Ongoing Operations for a Pod of Manifest Version

In addition to the DNS requirements, the ports and protocols in the following tables are required for the pod to operate properly for ongoing operations after deployment.

**Note** In this section's tables, the term manager VM refers to the pod’s manager VM. In the Microsoft Azure portal, this VM has a name that contains a part like `vmw-hcs-podID`, where `podID` is the pod’s UUID, and a node part.

### Table 7-15. Pod Operations Ports and Protocols

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Ports</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager VM</td>
<td>Domain controller</td>
<td>389</td>
<td>TCP</td>
<td>LDAP services. Server that contains a domain controller role in an</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UDP</td>
<td>Active Directory configuration. Registering the pod with an Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Directory is a requirement.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Global catalog</td>
<td>326</td>
<td>TCP</td>
<td>LDAP services. Server that contains global catalog role in an Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8</td>
<td></td>
<td>Directory configuration. Registering the pod with an Active Directory is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>a requirement.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Domain controller</td>
<td>88</td>
<td>TCP</td>
<td>Kerberos services. Server that contains a domain controller role in an</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UDP</td>
<td>Active Directory configuration. Registering the pod with an Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Directory is a requirement.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>DNS server</td>
<td>53</td>
<td>TCP</td>
<td>DNS services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>Manager VM</td>
<td>NTP server</td>
<td>123</td>
<td>UDP</td>
<td>NTP services. Server that provides NTP time synchronization.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>True SSO Enrollment Server</td>
<td>3211</td>
<td>TCP</td>
<td>True SSO Enrollment Server. Optional if you are not using True SSO</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Enrollment Server capabilities with your pods.</td>
</tr>
</tbody>
</table>
### Table 7-15. Pod Operations Ports and Protocols (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Ports</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager VM</td>
<td>Workspac e ONE Access service</td>
<td>443</td>
<td>HTTPS</td>
<td>Optional if you are not using Workspace ONE Access with the pod. Used to create a trust relationship between the pod and the Workspace ONE Access service. Ensure that the pod can reach the Workspace ONE Access environment you are using, either on-premises or the cloud service, on port 443. If you are using the Workspace ONE Access cloud service, see also the list of Workspace ONE Access service IP addresses to which the Workspace ONE Access Connector and the pod must have access in the VMware Knowledge Base article 2149884.</td>
</tr>
<tr>
<td>Transient Jump box VM</td>
<td>Manager VM</td>
<td>22</td>
<td>TCP</td>
<td>As described in Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates, a transient jump box is used during pod deployment and pod update processes. Even though ongoing processes do not require these ports, during pod deployment and pod update processes, this jump box VM must communicate with the pod's manager VM using SSH to the manager VM's port 22. For details about the cases for which the jump box VM needs this communication, see Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates.</td>
</tr>
</tbody>
</table>

Which ports must be opened for traffic from the end users' connections to reach their pod-provisioned virtual desktops and remote applications depends on the choice you make for how your end users will connect:

- When you choose the option for having an external gateway configuration, Unified Access Gateway instances are automatically deployed in your Microsoft Azure environment, along with a Microsoft Azure load balancer resource to those instances in its backend pool. That load balancer communicates with those instances' NICs on the DMZ subnet, and is configured as a public load balancer in Microsoft Azure. The diagram Figure 7-1. Illustration of the Horizon Cloud Pod Architecture for a Pod with High Availability Enabled and Configured with Both External and Internal Unified Access Gateway Configurations depicts the location of this public load balancer and the Unified Access Gateway instances. When your pod has this configuration, traffic from your end users on the Internet goes to that load balancer, which distributes the requests to the Unified Access Gateway instances. For this configuration, you must ensure that those end-user connections can reach that load balancer using the ports and protocols listed below. For the deployed pod, the external gateway's load balancer is located in the resource group named vmw-hcs-pod\ID-uag, where pod\ID is the pod's UUID.

- When you choose the option for having an internal Unified Access Gateway configuration, Unified Access Gateway instances are automatically deployed in your Microsoft Azure environment, along with a Microsoft Azure load balancer resource to those instances in its backend pool. That load balancer communicates with those instances' NICs on the tenant subnet, and is configured as an internal load balancer in Microsoft Azure. The diagram Figure 7-1. Illustration of the Horizon Cloud Pod Architecture for a Pod with High Availability Enabled and Configured with Both External and Internal Unified Access Gateway Configurations depicts the location of this internal load balancer and the Unified Access Gateway instances.
When your pod has this configuration, traffic from your end users in your corporate network goes to that load balancer, which distributes the requests to the Unified Access Gateway instances. For this configuration, you must ensure that those end-user connections can reach that load balancer using the ports and protocols listed below. For the deployed pod, the internal gateway's load balancer is located in the resource group named vmw-hcs-<podID>-uag-internal, where <podID> is the pod's UUID.

When you do not choose either Unified Access Gateway configurations, you can instead have your end users connecting directly to the pod, such as using a VPN. For this configuration, you upload an SSL certificate to the pod's manager VM using the pod's summary page in the administrative console, as described in Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs.

For detailed information about the various Horizon Clients that your end users might use with your Horizon Cloud pod, see the Horizon Client documentation page at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

Table 7-16. External End User Connections Ports and Protocols when the Pod Configuration has External Unified Access Gateway instances

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic. Can also carry client-drive redirection (CDR), multimedia redirection (MMR), USB redirection, and tunneled RDP traffic. SSL (HTTPS access) is enabled by default for client connections. Port 80 (HTTP access) can be used in some cases. See Understanding What URL Content Redirection is.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>4172</td>
<td>TCP UDP</td>
<td>PCoIP via PCoIP Secure Gateway on Unified Access Gateway</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic.</td>
</tr>
</tbody>
</table>
### Table 7-16. External End User Connections Ports and Protocols when the Pod Configuration has External Unified Access Gateway instances (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>UDP</td>
<td>Blast Extreme via the Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>844</td>
<td>UDP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic (adaptive transport).</td>
</tr>
<tr>
<td>Browser</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>

### Table 7-17. Internal End User Connections Ports and Protocols when the Pod Configuration has Internal Unified Access Gateway instances

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic. Can also carry client-drive redirection (CDR), multimedia redirection (MMR), USB redirection, and tunneled RDP traffic. SSL (HTTPS access) is enabled by default for client connections. Port 80 (HTTP access) can be used in some cases. See <a href="#">Understanding What URL Content Redirection Is</a>.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>4172</td>
<td>TCP</td>
<td>PCoIP via PCoIP Secure Gateway on Unified Access Gateway</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic.</td>
</tr>
</tbody>
</table>
Table 7-17. Internal End User Connections Ports and Protocols when the Pod Configuration has Internal Unified Access Gateway instances (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>UDP</td>
<td>Blast Extreme via the Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>844</td>
<td>UDP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic (adaptive transport).</td>
</tr>
<tr>
<td>Browser</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>

Table 7-18. Internal End User Connections Ports and Protocols when using Direct Pod Connections, Such as Over VPN

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Manager VM</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>4172</td>
<td>TCP, UDP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>22443</td>
<td>TCP, UDP</td>
<td>Blast Extreme</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>32111</td>
<td>TCP</td>
<td>USB redirection</td>
</tr>
</tbody>
</table>
Table 7-18. Internal End User Connections Ports and Protocols when using Direct Pod Connections, Such as Over VPN (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target Description</th>
<th>Port</th>
<th>Protocol(s)</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>9427</td>
<td>TCP</td>
<td>Client-drive redirection (CDR) and multimedia redirection (MMR)</td>
</tr>
<tr>
<td>Browser</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>

For connections using a pod configured with Unified Access Gateway instances, traffic must be allowed from the pod's Unified Access Gateway instances to targets as listed in the table below. During pod deployment, a Network Security Group (NSG) is created in your Microsoft Azure environment for use by the pod's Unified Access Gateway software.

Table 7-19. Port Requirements for Traffic from the Pod's Unified Access Gateway Instances

<table>
<thead>
<tr>
<th>Source</th>
<th>Target Description</th>
<th>Port</th>
<th>Protocol(s)</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Access Gateway</td>
<td>Manager VM</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>4172</td>
<td>TCP, UDP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>22443</td>
<td>TCP, UDP</td>
<td>Blast Extreme</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>By default, when using Blast Extreme, client-drive redirection (CDR) traffic and USB traffic is side-channeled in this port. If you prefer instead, the CDR traffic can be separated onto the TCP 9427 port and the USB redirection traffic can be separated onto the TCP 32111 port.</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>9427</td>
<td>TCP</td>
<td>Optional for client driver redirection (CDR) and multimedia redirection (MMR) traffic.</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>32111</td>
<td>TCP</td>
<td>Optional for USB redirection traffic.</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Your RADIUS instance</td>
<td>1812</td>
<td>UDP</td>
<td>When using RADIUS two-factor authentication with that Unified Access Gateway configuration. The default value for RADIUS is shown here.</td>
</tr>
</tbody>
</table>

The following ports must allow traffic from the Horizon agent-related software that is installed in the desktop VMs and farm server VMs.
### Source | Target | Port | Protocol | Purpose
--- | --- | --- | --- | ---
Horizon agent in the desktop or farm server VMs | Manager VM | 4001 | TCP | Java Message Service (JMS, non-SSL), used by the agent in the VM when the agent is not yet paired with the pod. The agent communicates with the pod to get the information it needs to pair with the pod. After the agent is paired, it uses port 4002 to communicate with the pod.
Horizon agent in the desktop or farm server VMs | Manager VM | 4002 | TCP | Java Message Service (JMS, SSL), used by the agent to communicate with the pod when the agent is already paired with the pod.
FlexEngine agent (the agent for VMware Dynamic Environment Manager) in the desktop or farm server VMs | Those file shares that you set up for use by the FlexEngine agent that runs in the desktop or farm server VMs | 445 | TCP | FlexEngine agent access to your SMB file shares, if you are using VMware Dynamic Environment Manager capabilities.

As part of the pod deployment process, the deployer creates network security groups (NSGs) on the network interfaces (NICs) on all of the deployed VMs. For details about the rules defined in those NSGs, see [Default Network Security Group Rules for the VMs in a Horizon Cloud Pod Deployed in Microsoft Azure](#).

**Note** Instead of listing DNS names, IP addresses, ports, and protocols in a Horizon Cloud Knowledge Base (KB) article, we have provided them here as part of the core Horizon Cloud documentation.

### Default Network Security Group Rules for the VMs in a Horizon Cloud Pod Deployed in Microsoft Azure

The purpose of this documentation topic here is to explain to you what you will see after you use Horizon Cloud to create a pod in your Microsoft Azure subscription and you subsequently log in to the Microsoft Azure portal and look at what the pod deployer created there. As part of deploying the pod in Microsoft Azure, the automated deployment process creates a set of network security groups (NSGs) and associates each with specific individual network interfaces (NICs) that are on each of the VMware controlled pod-related virtual machines (VMs). Such pod-related VMs are the pod’s manager VMs, and the VMs that are deployed when the pod is
configured with Unified Access Gateway. Also, during pod deployment-related workflows, such as deploying a pod or adding a gateway configuration to a pod, the temporary jump box also has an NSG in its temporary jump box resource group. The pod deployer associates the appropriate deployer-created NSG with the appropriate NIC, according to the VMware design and architecture for the pod. These NSGs are used at a NIC level to ensure that each NIC on a particular VMware managed appliance can receive the traffic that VMware managed appliance is supposed to receive for standard service and pod operations over the NIC's attached subnet, and to block all traffic that appliance is not supposed to receive. Each NSG contains a set of security rules that define the allowed traffic to and from each NIC.

The NSGs described here are separate from the ones used for the farms and VDI desktops that you create in the pod, and have different usage information. For information about the NSGs used for farms and pools, see About Network Security Groups and Your Farms and About Network Security Groups and Your VDI Desktops.

**Warning** The deployer-created NSG rules described here are configuration requirements of the service. You should never delete or edit any of the Horizon Cloud NSGs that are automatically created and associated with the pod VMs’ NICs. This instruction includes actions such as:

- Copying or moving these NSGs or NSG rules to any subnet used by Horizon Cloud
- Copying or moving these NSGs or NSG rules between the NICs that are associated with the pod VMs.

The NSGs created by Horizon Cloud and the rules inside of them are specific to the particular NICs and VMs to which they are attached, and are expressly for the purposes of those NICs and VMs. Any change to those NSGs or rules, or any attempt to use them for any other purpose — even on the same subnets to which those NICs are attached — will most likely result in disrupting the required network traffic to and from the NICs to which they are attached. That disruption in turn could result in disrupting all pod operations. The lifecycle of these NSGs is managed by Horizon Cloud, and there are specific reasons for each one. Those reasons include:

- The ability for the cloud control plane to communicate with the pod.
- Management of the pod’s infrastructure
- Pod lifecycle operations

Because these deployer-created NSGs are configuration requirements of the service, attempts to change them or move them are considered an unsupported use of Horizon Cloud and a misuse of the service offerings, as described in the Service Level Agreement for VMware Horizon Service.

However, you can create your own NSGs containing your own organization’s rules within resource groups outside of the pod’s resource groups that are auto-created and managed by Horizon Cloud for the pod’s VMs. The rules in your own NSGs must not conflict with Horizon Cloud’s requirements for the management and operations of the pod’s VMs. Such NSGs should be attached to the management, tenant, and DMZ subnets used by the pod. Creating your own NSGs within the resource groups managed by Horizon Cloud will cause failure during deletion actions on the Horizon Cloud managed resource groups if your NSGs in those resource groups are associated with a resource that resides in a different resource group.
As described in the Microsoft Azure documentation, the purpose of a network security group (NSG) is to filter network traffic to and from resources in your Microsoft Azure environment using security rules. Each rule has a set of properties such as source, destination, port, protocol, and so on that determine the traffic allowed for the resources to which the NSG is associated. The NSGs that Horizon Cloud automatically creates and associates with the VMware controlled pod VMs' NICs contain particular rules which Horizon Cloud has determined are needed for the service's management of the pod, for proper running of ongoing pod operations, and for managing the pod's lifecycle. Generally speaking, each rule defined in these NSGs is intended to provide for the pod operations' port traffic that is part and parcel of the service's fulfillment of the standard business purposes of a Horizon Cloud subscription, such as the VDI use cases of delivering virtual desktops to end users. See also Ports and Protocols Requirements for a Horizon Cloud Pod.

The sections below list the NSG rules that Horizon Cloud defines in those NSGs.

- **General Facts About These NSGs**

- **Pod Manager VM's Deployer-Created NSGs**

- **External Unified Access Gateway VMs' Deployer-Created NSGs**

- **Internal Unified Access Gateway VMs' Deployer-Created NSGs**

- **Gateway Connector VM's Deployer-Created NSG When an External Gateway is Deployed in Its Own VNet**

- **Temporary Jump Box VM's Deployer-Created NSG**

**General Facts About These NSGs**

This list applies to all of the deployer-created NSGs that the deployer associates with specific NICs on the pod-related VMs.

- These VMware created NSGs are for the security of the VMware controlled software appliances. When VMware adds new software to your subscription and additional rules are required, those new rules are added to these NSGs.

- In the Microsoft Azure portal, the NSGs have names that contain the pattern vmw-hcs--podUUID, where podUUID is the pod's identifier, except for the NSGs that are for an external gateway configuration that is deployed into its own VNet. In that case, the gateway’s relevant NSGs have names that contain the pattern vmw-hcs--ID, where ID is the deployment ID for that external gateway.

**Note**  For the scenario where the external gateway configuration is deployed into a separate subscription using the option to deploy into an existing resource group that you pre-created in that subscription, the NSG on the gateway connector's VM's management NIC is named in a pattern based on the resource group's name instead of the vmw-hcs--podUUID pattern. As an example, if you named that resource group hcsgateways, then in that resource group, Horizon Cloud creates an NSG named hcsgateways--mgmt--nsg, and associates that NSG with the gateway connector VM's management NIC.
You can locate these identifiers by navigating to the pod's details from the administrative console's Capacity page.

**Note** When you choose to have the pod's external Unified Access Gateway use a custom resource group, the name of the gateway connector VM's deployer-created NSG contains the name of that custom resource group instead of the pattern `vmw-hcs-<ID>`. As an example, if you specify using a custom resource group named `ourhcspodgateway` for your pod's external gateway, the NSG that the deployer creates and associates with the gateway VM's NIC will be named `ourhcspodgateway-mgmt-nsg`.

- The NSGs are located in the same resource group as the VMs and NICs to which they are associated. As an example, the NSGs associated with the NICs on the external Unified Access Gateway VMs are located in the resource group named `vmw-hcs-podUUID-uag` when the external gateway is deployed in the pod's VNet and using a deployer-created resource group. See also Resource Groups Created For a Pod Deployed In Microsoft Azure.

- Horizon Cloud might add new rules or modify these rules as appropriate for ensuring maintainability of the service.

- During a pod update, the NSGs and rules will be retained. They will not be deleted.

- Except for the temporary jump box's NSG rules, the Horizon Cloud rules start at priority 1000, and the priorities go up in increments that are 100 typically. The Horizon Cloud rules end with a rule at priority 3000. For the jump box's NSG rules, the Horizon Cloud rules start at priority 100, and the priorities go up in increments of 1. The Horizon Cloud rules end with a rule at priority 1000.

- The `AllowAzureInBound` rules for source IP address 168.63.129.16 provide for the NSGs accepting incoming communication from the Microsoft Azure platform, as described in the Microsoft Azure documentation topic What is IP address 168.63.129.16. All of the pod-related VMs are VMs in Microsoft Azure. As described in that Microsoft Azure documentation topic, their IP address 168.63.129.16 facilitates various VM management tasks that the Microsoft Azure cloud platform does for all VMs in their cloud. As an example, this IP address facilitates having the VM Agent that is within the VM to communicate with the Microsoft Azure platform to signal that the VM is in a Ready state.

- In the NSGs for the Unified Access Gateway instances, the `AllowPcoipUdpInBound` rules are set for any port because PCoIP traffic is using variable port numbers in the 4173+ range, so that traffic cannot be restricted to a specific set of ports.

- Microsoft Azure creates some default rules automatically in each NSG when it is created. In every NSG that is created, Microsoft Azure creates some inbound and outbound rules at priority 65000 and higher. Such Microsoft Azure default rules are not described in this documentation topic, because they are created by Microsoft Azure automatically. For details on those default rules, see the Microsoft Azure documentation topic Default security rules.
During deployment-related workflows, such as deploying a pod or adding a gateway configuration to a pod, the temporary jump box also has an NSG in its temporary jump box resource group. This NSG is deleted when the jump box's resource group is deleted at the completion of the workflow.

Each rule defined in these NSGs is intended to provide for the pod operations' port traffic that is part and parcel of the service's fulfillment of the standard business purposes of a Horizon Cloud subscription, such as the VDI use cases of delivering virtual desktops to end users. See also Ports and Protocols Requirements for a Horizon Cloud Pod.

When you Editing Your Horizon Cloud Pod to Make Use of Multiple Tenant Subnets for Farms and VDI Desktop Assignments, the rules in the tenant-subnet-related NSGs on the pod manager VMs' and Unified Access Gateway VMs' NICs are updated to include those additional tenant subnets.

Pod Manager VM's Deployer-Created NSGs

The pod manager VM has two NICs, one connected to the management subnet and the other connected to the tenant subnet. The deployer creates a specific NSG for each of those two NICs, and associates each NSG with its appropriate NIC.

- The management NIC has an NSG named in the pattern `vmw-hcs-podUUID-mgmt-nsg`.
- The tenant NIC has an NSG named in the pattern `vmw-hcs-podUUID-tenant-nsg`.

In your Microsoft Azure environment, these NSGs reside in the pod's resource group named in the pattern `vmw-hcs-podUUID`.

**Important** When the pod is using the feature to have its external gateway in a separate VNet (which includes the case where that gateway is using a separate subscription from the pod's subscription), the NSG for the pod manager VM's tenant NIC has an additional inbound rule named `AllowGatewayBrokeringHttpsInBound` for port 8443 TCP with `VirtualNetwork` as the source. The deployer-created NSG rules on the pod manager VM's tenant NIC when the external gateway is in a separate VNet are listed in the third table below.
<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Rule’s Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowSshInBound</td>
<td>22</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>As described in the topic DNS Requirements for a Horizon Cloud Pod in Microsoft Azure, the short-lived jump box VM communicates with a pod manager VM using SSH to the VM's port 22 in the initial creation of a pod and during subsequent software updates on the pod. Also as described in that topic, day-to-day pod operations do not require availability of port 22 on the pod manager VM. However, if during steady-state operations you make a support request to...</td>
</tr>
</tbody>
</table>
Table 7-20. Deployer-Created NSG Rules on the Pod Manager VM’s Management NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Rule’s Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1100</td>
<td>AllowAzureInBound</td>
<td>Any</td>
<td>Any</td>
<td>168.63.129.16</td>
<td>Any</td>
<td>Allow</td>
<td>For the VM to accept incoming communication from the Microsoft Azure platform, as described in the preceding General Facts section and in the Microsoft Azure documentation topic What is IP.</td>
</tr>
</tbody>
</table>
### Table 7-20. Deployer-Created NSG Rules on the Pod Manager VM’s Management NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Rule’s Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1200</td>
<td>AllowHttpSInBound</td>
<td>443</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>For the cloud control plane to securely communicate with the pod manager’s REST API endpoint.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1300</td>
<td>AllowApacheGeodeInBound</td>
<td>10334 - 10335, 41000-41002, 42000-42002</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>These ports are used to replicate user sessions across the pod manager VMs.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1400</td>
<td>AllowTelegrafInBound</td>
<td>9172</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>This rule is planned for use in a future service release.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1500</td>
<td>AllowAgentJmsInBound</td>
<td>4001, 4002</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>This rule is planned for use in a future service release.</td>
</tr>
<tr>
<td>Inbound</td>
<td>3000</td>
<td>DenyAllInBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to limit this NIC’s inbound traffic to the items in the previous rows.</td>
</tr>
<tr>
<td>Direction</td>
<td>Priority</td>
<td>Name</td>
<td>Ports</td>
<td>Protocol</td>
<td>Source</td>
<td>Destination</td>
<td>Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>---------------</td>
<td>---------</td>
<td>----------</td>
<td>-------------</td>
<td>-------------</td>
<td>--------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowHttpInBound</td>
<td>80</td>
<td>TCP</td>
<td>VirtualNetwork</td>
<td>Any</td>
<td>Allow</td>
<td>This rule provides for an atypical scenario in which you might have told your internal end users (on your corporate network, such as over VPN) to make their client connections to an FQDN that you have mapped to the pod's Microsoft Azure load balancer. This scenario is sometimes referred to as direct-pod connection. For the login authentication request to the connection broker in the pod, the Horizon Clients and Horizon web client use port 443. To support easy redirection.</td>
</tr>
<tr>
<td>Direction</td>
<td>Priority</td>
<td>Name</td>
<td>Ports</td>
<td>Protocol</td>
<td>Source</td>
<td>Destination</td>
<td>Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-----------------------</td>
<td>-------------</td>
<td>----------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inbound</td>
<td>1100</td>
<td>AllowAgentntHttpsinBound</td>
<td>3443, 8443</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>Port 3443 inbound to this NIC is used by the App Volumes Agent in the base VMs, desktop VMs, and farm RDSH VMs to access the App Volumes Manager service that runs in the pod manager VM. Port 8443 inbound to this NIC is used by the Unified Access Gateway instances to check with the pod manager</td>
<td></td>
</tr>
</tbody>
</table>

As a convenience for a user who might type HTTP in their client instead of HTTPS, that traffic arrives at port 80 and is automatically redirected to port 443.
Table 7-21. Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1120</td>
<td>AllowUagHttpInBo</td>
<td>8443</td>
<td>TCP</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>This rule is planned for use in a future service release.</td>
</tr>
</tbody>
</table>

VM’s connection broker. The gateway instances use this endpoint to confirm sending new client brokering requests to the pod manager VM.
Table 7-21. Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1200</td>
<td>AllowAgentJmsInbound</td>
<td>4001</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
<td>The Horizon Agents in the base VMs, desktop VMs, and farm RDSH VMs use these ports. Port 4001 is for Java Message Service (JMS, non-SSL), used by the agent in the VM to communicate with the pod as part of the certificate thumbprint verification and exchange to secure an SSL connection to the pod. After the keys are negotiated and exchanged between the VM and the pod manager, the agent uses port 4002 to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4002</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 7-21. Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1210</td>
<td>AllowRoutingJmsInbound</td>
<td>4101</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
<td></td>
</tr>
</tbody>
</table>

*Note* Both 4001 and 4002 are required for steady-state operations. At times, the agent might need to re-key with the pod.

create a secured SSL connection.
Table 7-21. Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1300</td>
<td>AllowAgentUdpInBound</td>
<td>5678</td>
<td>UDP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
<td>Deprecated for pods of manifests 1600 and later. In the service’s September 2019 release, the DaaS agent was incorporated into the Horizon Agent as of pod manifest 1600. Previously, this port 5678 and UDP protocol were used to support use of the DaaS agent.</td>
</tr>
</tbody>
</table>
Table 7-21. Deployer-Created NSG Rules on the Pod Manager VM's Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1400</td>
<td>AllowAzureInBound</td>
<td>Any</td>
<td>Any</td>
<td>168.63.129.16</td>
<td>Any</td>
<td>Allow</td>
<td>For the VM to accept incoming communication from the Microsoft Azure platform, as described in the preceding General Facts section and in the Microsoft Azure documentation topic What is IP address 168.63.129.16.</td>
</tr>
<tr>
<td>Inbound</td>
<td>3000</td>
<td>DenyAllInBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to limit this NIC's inbound traffic to the items in the previous rows.</td>
</tr>
</tbody>
</table>
Table 7-22. When the External Gateway resides in a Separate VNet, Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destinations</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowHttpInBound</td>
<td>80</td>
<td>TCP</td>
<td>VirtualNetwork</td>
<td>Any</td>
<td>Allow</td>
<td>This rule provides for an atypical scenario in which you might have</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>443</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>told your internal end users (on your corporate network, such as over</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>VPN) to make their client connection s to an FQDN that you have</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mapped to the pod’s Microsoft Azure load balancer. This scenario is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sometimes referred to as direct-pod connection. For the login</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>authentication on request to the connection broker in the pod, the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Horizon Clients and Horizon web client use port 443. To support easy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 7-22. When the External Gateway resides in a Separate VNet, Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1100</td>
<td>AllowAgentHttpsInBound</td>
<td>3443</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
<td>Port 3443 inbound to this NIC is used by the App Volumes Agent in the base VMs, desktop VMs, farm RDSH VMs to access the App Volumes Manager service running in the pod manager VM. Port 8443 inbound to this NIC is used by the Unified Access Gateway instances to check with the pod</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8443</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>redirection as a convenience for a user who might type HTTP in their client instead of HTTPS, that traffic arrives at port 80 and is automatically redirected to port 443.</td>
</tr>
</tbody>
</table>
Table 7-22. When the External Gateway resides in a Separate VNet, Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>manager VM's connection broker. The gateway instances use this endpoint to confirm sending new client brokering requests to the pod.</td>
</tr>
</tbody>
</table>


Table 7-22. When the External Gateway resides in a Separate VNet, Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1110</td>
<td>AllowGatewayBreakingHttpsInBound</td>
<td>8443</td>
<td>TCP</td>
<td>VirtualNetwork</td>
<td>Any</td>
<td>Allow</td>
<td>When the pod’s external gateway is deployed in its own VNet separate from the pod, this rule supports the inbound traffic from the external gateway’s Unified Access Gateway instances to check with the pod manager VM’s connection broker. The gateway instances use this endpoint to confirm sending new client brokering requests to the connection broker.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1120</td>
<td>AllowUagHttpsInBound</td>
<td>8443</td>
<td>TCP</td>
<td>ManagementSubnet</td>
<td>Any</td>
<td>Allow</td>
<td>This rule is planned for use in a future service release.</td>
</tr>
</tbody>
</table>
Table 7-22. When the External Gateway resides in a Separate VNet, Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1200</td>
<td>AllowAgent.JmsInBound</td>
<td>4001</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
<td>The Horizon Agents in the base VMs, desktop VMs, and farm RDSH VMs use these ports. Port 4001 is for Java Message Service (JMS, non-SSL), used by the agent in the VM to communicate with the pod as part of the certificate thumbprint verification and exchange to secure an SSL connection to the pod. After the keys are negotiated and exchanged between the VM and the pod manager, the agent uses port 4002 to</td>
</tr>
</tbody>
</table>
Table 7-22. When the External Gateway resides in a Separate VNet, Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1210</td>
<td>AllowRouterJmsInbound</td>
<td>4101</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
<td>When a pod is enabled for high availability (HA), this traffic is JMS routing between the pod manager VMs (node-1 and node-2)</td>
</tr>
</tbody>
</table>

create a secured SSL connection.

Note Both 4001 and 4002 are required for steady-state operations. At times, the agent might need to re-key with the pod.
Table 7-22. When the External Gateway resides in a Separate VNet, Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1300</td>
<td>AllowAgentUdpInBound</td>
<td>5678</td>
<td>UDP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
<td>Deprecated for pods of manifests 1600 and later. In the service’s September 2019 release, the DaaS agent was incorporated into the Horizon Agent as of pod manifest 1600. Previously, this port 5678 and UDP protocol were used to support use of the DaaS agent.</td>
</tr>
</tbody>
</table>
Table 7-22. When the External Gateway resides in a Separate VNet, Deployer-Created NSG Rules on the Pod Manager VM’s Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1400</td>
<td>AllowAzureInBound</td>
<td>Any</td>
<td>Any</td>
<td>168.63.129.16</td>
<td>Any</td>
<td>Allow</td>
<td>For the VM to accept incoming communication from the Microsoft Azure platform, as described in the preceding General Facts section and in the Microsoft Azure documentation topic What is IP address 168.63.129.16.</td>
</tr>
<tr>
<td>Inbound</td>
<td>3000</td>
<td>DenyAllInBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to limit this NIC’s inbound traffic to the items in the previous rows.</td>
</tr>
</tbody>
</table>

External Unified Access Gateway VMs’ Deployer-Created NSGs

Each of the VMs for the external Unified Access Gateway configuration has three (3) NICs, one connected to the management subnet, one connected to the tenant subnet, and one connected to the DMZ subnet. The deployer creates a specific NSG for each of those three NICs, and associates each NSG with its appropriate NIC.

- The management NIC has an NSG named in the pattern `vmw-hcs-ID-uag-management-nsg`.
- The tenant NIC has an NSG named in the pattern `vmw-hcs-ID-uag-tenant-nsg`.
- The DMZ NIC has an NSG named in the pattern `vmw-hcs-ID-uag-dmz-nsg`. 
In your Microsoft Azure environment, these NSGs are named in the pattern `vmw-hcs-\(ID\)-uag` where \(ID\) is the pod's ID as displayed on the pod's details page in the console, unless the external gateway is deployed in its own VNet separate from the pod's VNet. In the case of an external gateway deployed in its own VNet, the \(ID\) is the Deployment ID value shown on the pod's details page.
Table 7-23. Deployer-Created NSG Rules on the External Unified Access Gateway VMs' Management NIC

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowHttpInBound</td>
<td>9443</td>
<td>TCP</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>For the service to configure the gateway's administration settings using its management interface. As described in the Unified Access Gateway product documentation, its management interface is at port 9443/TCP.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1100</td>
<td>AllowAzureInBound</td>
<td>Any</td>
<td>Any</td>
<td>168.63.129.16</td>
<td>Any</td>
<td>Allow</td>
<td>For the VM to accept incoming communication from the Microsoft Azure platform, as described in the preceding General Facts section and in the Microsoft Azure documentation topic What is IP address 168.63.129.16.</td>
</tr>
</tbody>
</table>
Table 7-23. Deployer-Created NSG Rules on the External Unified Access Gateway VMs’ Management NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1200</td>
<td>AllowSshInBound</td>
<td>22</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>For VMware to perform emergency access to the VM if needed for troubleshooting. Permission will be requested from you prior to any emergency access.</td>
</tr>
<tr>
<td>Inbound</td>
<td>3000</td>
<td>DenyAllInBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to limit this NIC’s inbound traffic to the items in the previous rows.</td>
</tr>
<tr>
<td>Outbound</td>
<td>3000</td>
<td>DenyAllOutBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to deny outbound traffic from this NIC.</td>
</tr>
</tbody>
</table>
Table 7-24. Deployer-Created NSG Rules on the External Unified Access Gateway VMs’ Tenant NIC

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowAzureInbound</td>
<td>Any</td>
<td>Any</td>
<td>168.63.129.16</td>
<td>Any</td>
<td>Allow</td>
<td>For the VM to accept incoming communication from the Microsoft Azure platform, as described in the preceding General Facts section and in the Microsoft Azure documentation topic What is IP address 168.63.129.16.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1400</td>
<td>AllowPCoIPudpInBound</td>
<td>Any</td>
<td>UDP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
<td>This rule supports the standard configuration used for Unified Access Gateway working with the Horizon Agent. The Horizon Agents in the desktop and farm VMs send PCoIP data back to the Unified Access Gateway instances using UDP.</td>
</tr>
</tbody>
</table>
Table 7-24. Deployer-Created NSG Rules on the External Unified Access Gateway VMs' Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>3000</td>
<td>DenyAllInBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to limit this NIC's inbound traffic to the items in the previous rows.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outbound</td>
<td>1000</td>
<td>AllowHttpSOutBounded</td>
<td>443 8443</td>
<td>TCP</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>This rule supports the Unified Access Gateway instances communicating with the connection broker in the pod manager VMs for the purpose of new client brokering requests to the pod.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outbound</td>
<td>1100</td>
<td>AllowBlastOutBound</td>
<td>22443</td>
<td>Any</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>This rule supports the use case of a Horizon Client Blast Extreme session to the Horizon Agent in a desktop or farm VM.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 7-24. Deployer-Created NSG Rules on the External Unified Access Gateway VMs' Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>1200</td>
<td>AllowPcoIPOutBound</td>
<td>4172</td>
<td>Any</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>This rule supports the use case of a Horizon Client PCoIP session to the Horizon Agent in a desktop VM.</td>
</tr>
<tr>
<td>Outbound</td>
<td>1300</td>
<td>AllowUsbOutBound</td>
<td>32111</td>
<td>TCP</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>This rule supports the use case of USB redirection traffic. USB redirection is an agent option in the desktop or farm VMs. That traffic uses port 32111 for an end-user client session to the Horizon Agent in a desktop or farm VM.</td>
</tr>
</tbody>
</table>
Table 7-24. Deployer-Created NSG Rules on the External Unified Access Gateway VMs' Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>1400</td>
<td>AllowMmr OutBound</td>
<td>9427</td>
<td>TCP</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>This rule supports the use cases of multimedia redirection (MMR) and client driver redirection (CDR) traffic. These redirections are agent options in the desktop or farm VMs. That traffic uses port 9427, for an end-user client session to the Horizon Agent in a desktop or farm VM.</td>
</tr>
<tr>
<td>Direction</td>
<td>Priority</td>
<td>Name</td>
<td>Ports</td>
<td>Protocol</td>
<td>Source</td>
<td>Destination</td>
<td>Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>------------------</td>
<td>-------</td>
<td>----------</td>
<td>--------</td>
<td>-----------------------</td>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>Outbound</td>
<td>1500</td>
<td>AllowAllOutBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>When running in a VM that supports multiple user sessions, the Horizon Agent chooses different ports to use for the sessions’ PCoIP traffic. Because these ports cannot be determined ahead of time, a NSG rule naming specific ports to allow that traffic cannot be defined ahead of time. Therefore, similar to the rule at priority 1200, this rule supports the use case of multiple Horizon Client PCoIP sessions with such VMs.</td>
</tr>
<tr>
<td>Outbound</td>
<td>3000</td>
<td>DenyAllOutBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the</td>
</tr>
</tbody>
</table>
Table 7-24. Deployer-Created NSG Rules on the External Unified Access Gateway VMs' Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>

deployer to limit this NIC's outbound traffic to the items in the previous rows.
### Table 7-25. Deployer-Created NSG Rules on the External Unified Access Gateway VMs' DMZ NIC

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowHttpInBound</td>
<td>80, 443</td>
<td>TCP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
<td>This rule provides for the external end users' inbound traffic from the Horizon Clients and the Horizon web client to request the login authentication request to the connection broker in the pod. By default, the Horizon Client and Horizon web client use port 443 for this request. To support easy redirection as a convenience for a user who might type HTTP in their client instead of HTTPS, that traffic arrives at port 80 and is automatically redirected to port 443.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1100</td>
<td>AllowBlastInBound</td>
<td>443, 8443</td>
<td>Any</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
<td>This rule supports the Unified Administration of Your Horizon Cloud Tenant Environment and Your Fleet of Onboarded Pods</td>
</tr>
</tbody>
</table>
Table 7-25. Deployer-Created NSG Rules on the External Unified Access Gateway VMs' DMZ NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1200</td>
<td>AllowPcoiPinB</td>
<td>4172</td>
<td>Any</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
<td>This rule supports the Unified Access Gateway instances receiving PCoIP traffic from the external end users' Horizon Clients.</td>
</tr>
</tbody>
</table>

Access Gateway instances receiving the Blast traffic from the external end users' Horizon Clients.
Table 7-25. Deployer-Created NSG Rules on the External Unified Access Gateway VMs' DMZ NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1300</td>
<td>AllowAzureInBound</td>
<td>Any</td>
<td>Any</td>
<td>168.63.129.16</td>
<td>Any</td>
<td>Allow</td>
<td>For the VM to accept incoming communication from the Microsoft Azure platform, as described in the preceding General Facts section and in the Microsoft Azure documentation topic What is IP address 168.63.129.16.</td>
</tr>
<tr>
<td>Inbound</td>
<td>3000</td>
<td>DenyAllInBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to limit this NIC's inbound traffic to the items in the previous rows.</td>
</tr>
</tbody>
</table>

Internal Unified Access Gateway VMs' Deployer-Created NSGs

Each of the VMs for the internal Unified Access Gateway configuration has two (2) NICs, one connected to the management subnet and one connected to the tenant subnet. The deployer creates a specific NSG for each of those two NICs, and associates each NSG with its appropriate NIC.

- The management NIC has an NSG named in the pattern `vmw-hcs-podUID-uag-management-nsg`.
- The tenant NIC has an NSG named in the pattern `vmw-hcs-podUID-uag-tenant-nsg`. 
In your Microsoft Azure environment, these NSGs reside in the pod's resource group named in the pattern `vmw-hcs-podUUID-uag-internal`. 
### Table 7-26. Deployer-Created NSG Rules on the Internal Unified Access Gateway VMs' Management NIC

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowHttpInBound</td>
<td>9443</td>
<td>TCP</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>For the service to configure the gateway's administration settings using its management interface. As described in the Unified Access Gateway product documentation, its management interface is at port 9443/TCP.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1100</td>
<td>AllowAzureInBound</td>
<td>Any</td>
<td>Any</td>
<td>168.63.129.16</td>
<td>Any</td>
<td>Allow</td>
<td>For the VM to accept incoming communication from the Microsoft Azure platform, as described in the preceding General Facts section and in the Microsoft Azure documentation topic What is IP address 168.63.129.16.</td>
</tr>
</tbody>
</table>
Table 7-26. Deployer-Created NSG Rules on the Internal Unified Access Gateway VMs’ Management NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1200</td>
<td>AllowSshInBound</td>
<td>22</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Deny</td>
<td>For VMware to perform emergency access to the VM if needed for troubleshooting. Permission will be requested from you prior to any emergency access.</td>
</tr>
<tr>
<td>Inbound</td>
<td>3000</td>
<td>DenyAllInBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to limit this NIC's inbound traffic to the items in the previous rows.</td>
</tr>
<tr>
<td>Outbound</td>
<td>3000</td>
<td>DenyAllOutBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to deny outbound traffic from this NIC.</td>
</tr>
</tbody>
</table>
Table 7-27. Deployer-Created NSG Rules on the Internal Unified Access Gateway VMs' Tenant NIC

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowAzureInBound</td>
<td>Any</td>
<td>Any</td>
<td>168.63.129.16</td>
<td>Any</td>
<td>Allow</td>
<td>For the VM to accept incoming communication from the Microsoft Azure platform, as described in the preceding General Facts section and in the Microsoft Azure documentation topic What is IP address 168.63.129.16.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1100</td>
<td>AllowHttpInBound</td>
<td>80</td>
<td>TCP</td>
<td>VirtualNetwork</td>
<td>Any</td>
<td>Allow</td>
<td>This rule provides for the internal end users' inbound traffic from the Horizon Clients and the Horizon web client to request the login authentication on request to the connection broker in the pod. By default, the Horizon Client and Horizon web client use port</td>
</tr>
</tbody>
</table>
Table 7-27. Deployer-Created NSG Rules on the Internal Unified Access Gateway VMs' Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1200</td>
<td>AllowBlast InBound</td>
<td>443 8443</td>
<td>Any</td>
<td>VirtualNet work</td>
<td>Any</td>
<td>Allow</td>
<td>443 for this request. To support easy redirection as a convenience for a user who might type HTTP in their client instead of HTTPS, that traffic arrives at port 80 and is automatically redirected to port 443.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1300</td>
<td>AllowPcoIP InBound</td>
<td>4172</td>
<td>Any</td>
<td>VirtualNet work</td>
<td>Any</td>
<td>Allow</td>
<td>This rule supports the Unified Access Gateway instances receiving the Blast traffic from the internal end users' Horizon Clients.</td>
</tr>
</tbody>
</table>
Table 7-27. Deployer-Created NSG Rules on the Internal Unified Access Gateway VMs' Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1400</td>
<td>AllowPcoipUdpInBo</td>
<td>Any</td>
<td>UDP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
<td>This rule supports the standard configuration used for Unified Access Gateway working with the Horizon Agent. The Horizon Agents in the desktop and farm VMs send PCoIP data back to the Unified Access Gateway instances using UDP.</td>
</tr>
<tr>
<td>Inbound</td>
<td>3000</td>
<td>DenyAllInBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to limit this NIC's inbound traffic to the items in the previous rows.</td>
</tr>
</tbody>
</table>
Table 7-27. Deployer-Created NSG Rules on the Internal Unified Access Gateway VMs' Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>1000</td>
<td>AllowHttpOutBound</td>
<td>443</td>
<td>TCP</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>This rule supports the Unified Access Gateway instances communicating with the connection broker in the pod manager VMs for the purpose of new client brokering requests to the pod.</td>
</tr>
<tr>
<td>Outbound</td>
<td>1100</td>
<td>AllowBlastOutBound</td>
<td>22443</td>
<td>Any</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>This rule supports the use case of a Horizon Client Blast Extreme session to the Horizon Agent in a desktop or farm VM.</td>
</tr>
<tr>
<td>Outbound</td>
<td>1200</td>
<td>AllowPcoIPOutBound</td>
<td>4172</td>
<td>Any</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>This rule supports the use case of a Horizon Client PCoIP session to the Horizon Agent in a desktop VM.</td>
</tr>
<tr>
<td>Direction</td>
<td>Priority</td>
<td>Name</td>
<td>Ports</td>
<td>Protocol</td>
<td>Source</td>
<td>Destination</td>
<td>Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>------------------</td>
<td>--------</td>
<td>----------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Outbound</td>
<td>1300</td>
<td>AllowUsb OutBound</td>
<td>32111</td>
<td>TCP</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>This rule supports the use case of USB redirection traffic. USB redirection is an agent option in the desktop or farm VMs. That traffic uses port 32111 for an end-user client session to the Horizon Agent in a desktop or farm VM.</td>
</tr>
<tr>
<td>Outbound</td>
<td>1400</td>
<td>AllowMmr OutBound</td>
<td>9427</td>
<td>TCP</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>This rule supports the use cases of multimedia redirection (MMR) and client driver redirection (CDR) traffic. These redirections are agent options in the desktop or farm VMs. That traffic uses port 9427, for an end-user client session to the Horizon Agent in a desktop or farm VM.</td>
</tr>
</tbody>
</table>
Table 7-27. Deployer-Created NSG Rules on the Internal Unified Access Gateway VMs' Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>1500</td>
<td>AllowAllOutBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</td>
<td>When running in a VM that supports multiple user sessions, the Horizon Agent chooses different ports to use for the sessions' PCoIP traffic. Because these ports cannot be determined ahead of time, a NSG rule naming specific ports to allow that traffic cannot be defined ahead of time. Therefore, similar to the rule at priority 1200, this rule supports the use case of multiple Horizon Client PCoIP sessions with such VMs.</td>
</tr>
<tr>
<td>Outbound</td>
<td>3000</td>
<td>DenyAllOutBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the</td>
</tr>
</tbody>
</table>
Table 7-27. Deployer-Created NSG Rules on the Internal Unified Access Gateway VMs' Tenant NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>

deployer to limit this NIC's outbound traffic to the items in the previous rows.

Gateway Connector VM's Deployer-Created NSG When an External Gateway is Deployed in Its Own VNet

The gateway connector VM has a single NIC. This NIC is attached to the external gateway's VNet's management subnet. The deployer creates a single NSG and associates that NSG specifically with that NIC. By default, the deployer-created NSG for the gateway connector's management NIC has the same rules as the deployer-created NSG for the pod manager VM.
<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Inbound   | 1000     | AllowSshInBound | 22    | Any      | Management subnet | Any         | Allow  | As described in the topic DNS Requirements for a Horizon Cloud Pod in Microsoft Azure, the short-lived jump box VM communicates with this gateway connector VM using SSH to the VM's port 22 during its initial creation and during subsequent software updates on the pod. Also as described in that topic, day-to-day pod operations do not require availability of port 22 on the gateway connector VM. However, if during steady-state operations you make a support
Table 7-28. Deployer-Created NSG Rules on the External Gateway’s Connector VM’s Management NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1100</td>
<td>AllowAzureInBound</td>
<td>Any</td>
<td>Any</td>
<td>168.63.129.16</td>
<td>Any</td>
<td>Allow</td>
<td>For the VM to accept incoming communication from the Microsoft Azure platform, as described in the preceding General Facts section and in the Microsoft Azure documentation topic</td>
</tr>
</tbody>
</table>

request to VMware and the support team determines the way to troubleshoot that request is to deploy a jump box VM for SSH communication to the gateway connector VM, this NSG rule supports that use case. Permission will be requested from you prior to any emergency access.
Table 7-28. Deployer-Created NSG Rules on the External Gateway’s Connector VM’s Management NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1200</td>
<td><strong>AllowHttpInBound</strong></td>
<td>443</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>For the cloud control plane to securely communicate with the gateway connector’s REST API endpoint.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1300</td>
<td><strong>AllowApacheGeodeInBound</strong></td>
<td>10334 - 10335, 41000-41002, 42000-42002</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>These ports are used to replicate user sessions across the pod manager VMs and the gateway connector VM.</td>
</tr>
<tr>
<td>Inbound</td>
<td>1400</td>
<td><strong>AllowTelegrafInBound</strong></td>
<td>9172</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>This rule is planned for use in a future service release.</td>
</tr>
</tbody>
</table>
Table 7-28. Deployer-Created NSG Rules on the External Gateway’s Connector VM’s Management NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1500</td>
<td>AllowAgentJmsInBound</td>
<td>4001, 4002</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>This rule is planned for use in a future service release.</td>
</tr>
<tr>
<td>Inbound</td>
<td>3000</td>
<td>DenyAllInBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to limit this NIC’s inbound traffic to the items in the previous rows.</td>
</tr>
</tbody>
</table>

Temporary Jump Box VM’s Deployer-Created NSG

During deployment-related workflows, such as deploying a pod or adding a gateway configuration to a pod, the temporary jump box also has an NSG in its temporary jump box resource group. This NSG is deleted when the jump box’s resource group is deleted at the completion of the workflow.
Table 7-29. Deployer-Created NSG Rules on the Jump Box VM's Management NIC

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>100</td>
<td>AllowSSHI_nBound</td>
<td>22</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Allow</td>
<td>As described in the topic DNS Requirements for a Horizon Cloud Pod in Microsoft Azure, ongoing pod operations do not require inbound traffic to the short-lived jump box VM's port 22. However, if during steady-state operations you make a support request to VMware and the support team determines the way to troubleshoot that request is to deploy a jump box VM for SSH communication to your pod's manager VM, this NSG rule supports that use case.</td>
</tr>
</tbody>
</table>
## Table 7-29. Deployer-Created NSG Rules on the Jump Box VM’s Management NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>100</td>
<td>AllowSSH Outbound</td>
<td>22</td>
<td>TCP</td>
<td>Management subnet</td>
<td>Management subnet</td>
<td>Allow</td>
<td>For the jump box VM to perform its designed functions of configuring the other service-deployed VMs as required by the service.</td>
</tr>
<tr>
<td>Outbound</td>
<td>101</td>
<td>AllowHttp Outbound</td>
<td>443</td>
<td>TCP</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>For the jump box VM to download specific externally located software components, such as the Microsoft Azure CLI (Command Line-Interface). The jump box uses this software to perform its designed functions of configuring the other service-deployed VMs.</td>
</tr>
</tbody>
</table>
Table 7-29. Deployer-Created NSG Rules on the Jump Box VM's Management NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>102</td>
<td>AllowHttp Outbound</td>
<td>80</td>
<td>TCP</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>For the jump box VM to download specific externally located software components, such as the Ubuntu software updates for the pod's Linux-based VMs. The jump box uses this software to perform its designed functions of configuring the other service-deployed VMs.</td>
</tr>
</tbody>
</table>
Table 7-29. Deployer-Created NSG Rules on the Jump Box VM's Management NIC (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Name</th>
<th>Ports</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>103</td>
<td>AllowUag Outbound</td>
<td>9443</td>
<td>TCP</td>
<td>Management subnet</td>
<td>Management subnet</td>
<td>Allow</td>
<td>For the service to configure the gateway's administration settings using its management interface. As described in the Unified Access Gateway product documentation, its management interface is at port 9443/TCP.</td>
</tr>
<tr>
<td>Outbound</td>
<td>104</td>
<td>AllowDns Outbound</td>
<td>53</td>
<td>Any</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</td>
<td>For the jump box VM to reach DNS services.</td>
</tr>
<tr>
<td>Outbound</td>
<td>1000</td>
<td>DenyAllOutBound</td>
<td>Any</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Added by the deployer to limit this NIC's outbound traffic using TCP to the items in the previous rows.</td>
</tr>
</tbody>
</table>

Resource Groups Created For a Pod Deployed In Microsoft Azure

As part of the process of deploying a Horizon Cloud pod using your Microsoft Azure capacity, a set of resource groups are automatically created in your Microsoft Azure subscription. This topic describes those resource groups and their purpose. You can see these resource groups when you log in to your Microsoft Azure environment using the Microsoft Azure portal. If you deploy...
the pod's external gateway into its own subscription, the resource groups that support that
gateway are created in that subscription.

In the tables in the following sections, the podID refers to the pod's unique identifier. You can find
a pod's identifier displayed in the pod's details page, navigating from the Horizon Cloud Chapter
4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types. The poolID
refers to the unique identifier for a farm or VDI desktop assignment. The Deployment-ID refers to
the unique identifier related to an external gateway when it is deployed using its own VNet,
separate from the pod's VNet.

Resource groups that contain VMs also contain the resources associated with those VMs, such as
the VMs' network interfaces (NICs), network security groups (NSGs), and similar artifacts. Log in
to the Microsoft Azure portal and navigate to the resource group to see the artifacts it contains.
For details about the default rules in the NSGs that the pod deployer creates for the pod VMs'
NICs, see Default Network Security Group Rules for the VMs in a Horizon Cloud Pod Deployed in
Microsoft Azure.

Some resource groups are per pod, while others are created in your Microsoft Azure subscription
to contain resources that are used with all of the pods deployed using the same Microsoft Azure
subscription. Such cross-pod resource groups are created when the first pod is deployed using
that subscription.

**Note**

- Starting with the March 2020 service release, the Horizon Cloud deployer provides for
deploying the external Unified Access Gateway configuration into an existing resource group
that you create, instead of one automatically created by the deployer. This option is available
only when you use a separate subscription for that external Unified Access Gateway
configuration. In this scenario, that resource group's naming is controlled by you and your
organization, and does not follow the pattern described here.

- Starting with the October 2020 service release, the Horizon Cloud deployer provides for
applying custom Azure resource tags on the resource groups that the deployer creates
during the pod deployment and gateway deployment processes. This feature is available
when running the workflow to deploy a new pod or when running the workflow to edit a pod
to add a new gateway configuration.

**Per-Pod Resource Groups Created By Horizon Cloud**

When custom Azure resource tags are specified in the pod deployment wizard, the deployer
applies those specified tags to the following resource groups during the pod deployment
process:

- vmw-hcs-podID-jumpbox
- vmw-hcs-podID
- vmw-hcs-podID-base-vms
- vmw-hcs-podID-recovery
When deploying a gateway configuration, you can optionally choose to have the deployer apply the same Azure resource tags that are specified for the pod or specify different custom resource tags. In either case, the deployer will apply the same set of custom resource tags to the resource groups for both types of gateways.

When creating a farm or VDI desktop assignment, you can specify custom Azure resource tags. The Azure resource tags specified in the farm or assignment creation wizards are applied to the resource groups for those farms or VDI desktop assignments when they are created.

<table>
<thead>
<tr>
<th>Resource Group</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmw-hcs-podID-jumpbox</td>
<td>Contains the transient jump box VM and its associated resources that Horizon Cloud uses when deploying a pod or updating an existing pod. When the deployment process or update process is completed, Horizon Cloud deletes the jump box VM and its associated resources from this resource group.</td>
</tr>
<tr>
<td>vmw-hcs-podID</td>
<td>Contains the pod manager VMs and their associated resources.</td>
</tr>
<tr>
<td>vmw-hcs-podID-uag</td>
<td>Created when the pod has an external Unified Access Gateway configuration. Contains the Unified Access Gateway VMs and their associated resources.</td>
</tr>
<tr>
<td>vmw-hcs-podID-uag-internal</td>
<td>Created when the pod has an internal Unified Access Gateway configuration. Contains the Unified Access Gateway VMs and their associated resources.</td>
</tr>
<tr>
<td>vmw-hcs-podID-base-vms</td>
<td>Contains the base image VMs created either by running the Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it with Horizon Cloud or Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud, and those VMs’ associated resources. After an image VM is published to Horizon Cloud — also known as sealing the image — the VM continues to reside in this resource group along with its associated resources.</td>
</tr>
<tr>
<td>vmw-hcs-podID-poolID</td>
<td>Contains the VMs for a farm or VDI desktop assignment and those VMs’ associated resources. Each time a farm or VDI desktop assignment is created, this resource group is created for it. For every farm or VDI desktop assignment in the pod is one of these resource groups.</td>
</tr>
<tr>
<td>vmw-hcs-podID-recovery</td>
<td>Contains the storage-related and snapshot-related artifacts that support the Horizon Cloud Backup and Restore Service for Horizon Cloud Pods in Microsoft Azure.</td>
</tr>
</tbody>
</table>
Resource Groups Created By Horizon Cloud That Are Specific To an External Gateway Deployed in its Own VNet

When deploying a gateway configuration, you can optionally choose to have the deployer apply the same Azure resource tags that are specified for the pod or specify different custom resource tags. In this scenario where the external gateway is deployed in its own VNet and Azure resource tags are specified in the deployment wizard, the deployer:

- Applies the custom Azure resource tags that are specified for the pod itself to the `vmw-hcs-Deployment-ID-jumpbox` and `vmw-hcs-Deployment-ID` resource groups.
- Applies either the resource tags specified for the pod itself or different ones specified for the gateway to the `vmw-hcs-Deployment-ID-nnnnnnnn-nnnn-uag` resource group.

<table>
<thead>
<tr>
<th>Resource Group</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vmw-hcs-Deployment-ID-jumpbox</code></td>
<td>Contains the transient jump box VM and its associated resources that Horizon Cloud uses when deploying an external gateway in its own VNet, or updating that gateway. When the deployment process or update process is completed, Horizon Cloud deletes the jump box VM and its associated resources from this resource group.</td>
</tr>
<tr>
<td><code>vmw-hcs-Deployment-ID</code></td>
<td>Contains the gateway connector VM and its associated resources.</td>
</tr>
<tr>
<td><code>vmw-hcs-Deployment-ID-nnnnnnnn-nnnn-uag</code></td>
<td>Created when the pod has an external Unified Access Gateway configuration. Contains the Unified Access Gateway VMs and their associated resources. The value <code>nnnnnnnn-nnnn</code> is a unique identifier that corresponds with what is known as the gateway set ID in the Horizon Cloud control plane.</td>
</tr>
</tbody>
</table>

Cross-Pod Resource Groups Created By Horizon Cloud

These cross-pod resource groups are created when the first pod is deployed using that subscription. If custom Azure resource tags are specified in the deployment wizard when the first pod is deployed into the subscription, the pod deployer applies those same custom tags to these resource groups when the deployer creates them.
### Resource Group

<table>
<thead>
<tr>
<th>Resource Group</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmw-hcs-images-region</td>
<td>Contains the Horizon Cloud pre-configured VHD files used for configuring a pod’s VMs for the pods deployed in a particular Microsoft Azure region (region). When you deploy the initial pod in a Microsoft Azure region, this region-specific resource group is created. Horizon Cloud uses the resources in this resource group for the subsequent pods deployed into that same region.</td>
</tr>
<tr>
<td>vmw-hcs-diagnostics</td>
<td>Used for the Horizon Cloud diagnostic storage account that contains the pod deployment log files for your subscription’s pods.</td>
</tr>
</tbody>
</table>

---

**Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access**

By integrating your pod in Microsoft Azure with the cloud-hosted Workspace ONE Access environment, you can give your end users the ability to authenticate to their entitled pod-provisioned desktops and applications from a single unified catalog in Workspace ONE Access. You must deploy a Workspace ONE Access connector that bridges your Workspace ONE Access environment with the pod. This connector gives you the ability to synchronize the end-user entitlements from the pod to Workspace ONE Access.

**Tip**

- The former name of Workspace ONE Access was VMware Identity Manager™. The former name of the connector was the VMware Identity Manager™ connector. You might continue to see references to the former name in the product, documentation, and KB articles, especially if you are using older connector versions.

- See the VMware Digital Workspace Tech Zone for an excellent write-up describing the integration between Horizon Cloud and Workspace ONE Access.

- The Workspace ONE Access documentation uses the term entitlements when it describes the connector’s synchronization from the pod to Workspace ONE Access. In Horizon Cloud, an assignment represents the combination of a resource and entitlement. In the Horizon Cloud Administration Console, adding a user to an assignment entitles that user to the assignment’s pod-provisioned resource, such as when you Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure.

Workspace ONE Access is an Identity as a Service (IDaaS) offering that provides application provisioning, a self-service catalog, conditional access controls, and single sign-on (SSO) for SaaS, web, cloud, and native mobile applications. Workspace ONE Access handles the authentication of users to access those items that you have configured for them in the Workspace ONE Access catalog. Horizon Cloud customers typically use the cloud-hosted Workspace ONE Access, hosted by VMware.
For an overview of this integration from the perspective of the Workspace ONE Access environment, see the Providing Access to VMware Horizon Cloud Service Desktops and Applications overview. You configure desktops and remote application assignments for your users and groups in the Horizon Cloud Administration Console as usual. After you complete the steps to integrate your pod with your Workspace ONE Access environment, you sync the pod's assignment information to Workspace ONE Access. Then you can see the desktops and applications in the Workspace ONE Access administration console and your end users can authenticate to their assigned resources from Workspace ONE Access. You can set up a regular sync schedule to sync the assignment information from Horizon Cloud to your Workspace ONE Access environment.

**Note**  The screenshots in the Workspace ONE Access documentation might look different from the user interface elements you see in your specific Workspace ONE Access environment.

**High-Level View of the Key Components**

Integration of a pod in Microsoft Azure with Workspace ONE Access involves the following key concepts.

- The pod deployed in Microsoft Azure
- Your Workspace ONE Access tenant environment
- A valid SSL certificate uploaded onto the pod's manager VMs. This SSL certificate allows the Workspace ONE Access connector to trust connecting to the pod when the Workspace ONE Access connector synchronizes the entitlements and pod-provisioned resources for the Horizon Cloud Virtual Apps Collection in Workspace ONE Access.
- A Workspace ONE Access connector is installed and settings put into place to sync to Workspace ONE Access the information about these resources:
  - The Active Directory users and groups
  - The pod's assignments (the pod-provisioned resources and the entitlements to those resources)
- Configuration settings in the Horizon Cloud Administration Console to set up the SAML artifact that allows Workspace ONE Access to perform the SAML communication with the pod.

**Overview of the Integration Process**

The following list is a high-level summary of the end-to-end steps to enable your end users to authenticate to their pod-provisioned desktops and applications using Workspace ONE Access. Prior to these steps, you must have the pod already deployed in Microsoft Azure and have your Workspace ONE Access environment. If you want to integrate with a cloud-hosted Workspace
ONE Access environment and you do not already have that tenant, you can initiate setting up a Workspace ONE Access cloud tenant using the Horizon Cloud Administration Console's Identity Management page. For details, see Identity Management Page in the Horizon Cloud Administration Console.

1 In your DNS server, map the pod manager's Azure load balancer IP address to a fully qualified domain name (FQDN), such as mypod1.example.com. You can locate this IP address in the pod's details page. See Overview of Configuring SSL Certificates on the Horizon Cloud Pod's Manager VMs, Primarily For Use By the Workspace ONE Access Connector for an illustration of where to locate that IP address within the pod's details page.

**Note** Prior to the July 2020 quarterly service release, this IP address had the label Tenant appliance IP address on the pod's details page. The current label is Pod Manager Load Balancer IP. Pods of recent manifests include a Microsoft Azure load balancer deployed for the pod manager instance by default, and the current label reflects that pod architecture. Even though pods of manifests lower than 1600 do not have a Microsoft Azure load balancer deployed for their pod manager VM, the IP address you need to use for this pairing task is the IP displayed next to that label in the pod's details page.

2 Obtain a trusted SSL certificate based on that FQDN. For details on what is needed, see the following topics:
   - Overview of Configuring SSL Certificates on the Horizon Cloud Pod's Manager VMs, Primarily For Use By the Workspace ONE Access Connector
   - Prerequisites for Running the Horizon Cloud Administration Console's Upload Pod Certificate Workflow to Configure SSL Certificates on the Horizon Cloud Pod's Manager VMs

**Note** The certificate file formats required for uploading an SSL certificate to the pod are different than the PEM file format used by the pod gateway configurations.

3 Upload that SSL certificate as described in Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs.

**Important** If the pod does not have an SSL certificate on it that is configured as described to present to the Workspace ONE Access connector attempting to connect to it, the connector's attempt to connect to the pod to sync the entitlements and resources will fail because the connector will not make an untrusted network connection. The pod's SSL certificate must be trusted by the Workspace ONE Access connector for it to successfully connect with the pod. Until you have uploaded an SSL certificate that meets the criteria onto the pod, you will be unable to successfully integrate Workspace ONE Access with the pod.
4 Obtain a Workspace ONE Access environment, by subscribing to the cloud-hosted version to have a Workspace ONE Access tenant in the cloud.

**Note** If you set up a Workspace ONE Access tenant using the console's Identity Management page, the Workspace ONE Access tenant is associated with your Horizon Cloud customer record as part of that process. Pods that already exist for the same Horizon Cloud customer record can then be integrated with that tenant by deploying the Workspace ONE Access connector. In the following steps, make note of the connector-related details.

5 Deploy Workspace ONE Access according to the Workspace ONE Access guidelines for the deployment model you are using.

If you are using the cloud-hosted Workspace ONE Access, you must install the Workspace ONE Access connector appliance in your Active Directory network. Read all of the connector-related prerequisites starting with the section below titled **What You Need Before You Begin the Integration Steps**.

**Important** You must also ensure that the authoritative time source you configure in that connector matches the NTP server that is configured for the pod. If the time sources do not match, syncing issues can occur. The pod’s details page shows the pod’s configured NTP server. You can open the pod’s details page as described in Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types.

6 Ensure that you meet the Workspace ONE Access prerequisites for integration, as documented in the Workspace ONE Access product documentation appropriate for your situation. See the section below titled **What You Need Before You Begin the Integration Steps**.

**Important** In addition to the prerequisites listed below in this documentation topic, you must also ensure that your configured Workspace ONE Access environment meets the prerequisites for integration with Horizon Cloud resources, as described in the Workspace ONE Access documentation.

<table>
<thead>
<tr>
<th>Workspace ONE Access environment</th>
<th>Link to Workspace ONE Access Prerequisites in the Workspace ONE Access Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud-hosted</td>
<td><a href="#">Prerequisites for Integration</a> of Workspace ONE Access with Horizon Cloud</td>
</tr>
</tbody>
</table>
7 Enable the desktops from your Horizon Cloud environment to the Workspace ONE Access environment, as documented in the Workspace ONE Access product information appropriate for your situation.

**Important** In the Workspace ONE Access screen for entering the Horizon Cloud tenant information, in the **Host** field in that screen, you specify the FQDN that you mapped in your DNS server to the pod manager's Azure load balancer IP address. This FQDN must be the one on which the SSL certificate that you uploaded to the pod is based, as described in **Overview of Configuring SSL Certificates on the Horizon Cloud Pod's Manager VMs, Primarily For Use By the Workspace ONE Access Connector**, **Prerequisites for Running the Horizon Cloud Administration Console's Upload Pod Certificate Workflow to Configure SSL Certificates on the Horizon Cloud Pod's Manager VMs**, and **Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs**.

In the Configure Horizon Cloud Tenant in Workspace ONE Access topics that are linked below, the final step in those procedural topics describes how to sync the information about the entitlements from your Horizon Cloud environment. However, do not perform that sync step until after you complete step 5 below of configuring your pod for Workspace ONE Access access.

<table>
<thead>
<tr>
<th><strong>Workspace ONE Access environment</strong></th>
<th><strong>Link to Desktop Enablement Information in the Workspace ONE Access Documentation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud-hosted</td>
<td>Configure Horizon Cloud Tenant in VMware Workspace ONE Access.</td>
</tr>
</tbody>
</table>

8 Enter the settings that allow your configured Workspace ONE Access environment to be used as an identity management provider for the pod. See **Configure a Horizon Cloud Pod in Microsoft Azure for Workspace ONE Access**.

9 In your Workspace ONE Access environment, sync the entitled desktops and applications to Workspace ONE Access. In the Workspace ONE Access administration console, navigate to the Virtual Apps Configuration page for the collection you created in Step 4 and click **Sync**.

10 Verify end-user access to desktops and applications by logging in to Workspace ONE Access as an end user and launching a desktop and application from the catalog. See **Confirm End-User Access to Desktop Assignments in Workspace ONE Access**.

After you have verified the integration is working, you can optionally enforce end users to authenticate and access their desktops and applications through Workspace ONE Access. See **Enforce Having End Users Go Through Workspace ONE Access to Access Their Horizon Cloud Entitled Desktops and Applications**.
What You Need Before You Begin the Integration Steps

To fully complete the integration process end to end through to the step of verifying end-user access to the pod-provided desktops or RDS-based remote applications using Workspace ONE Access, ensure that you have the following items.

- As described in Overview of Configuring SSL Certificates on the Horizon Cloud Pod's Manager VMs, Primarily For Use By the Workspace ONE Access Connector and Prerequisites for Running the Horizon Cloud Administration Console's Upload Pod Certificate Workflow to Configure SSL Certificates on the Horizon Cloud Pod's Manager VMs, you need an entry in your DNS server that maps the pod manager's Azure load balancer IP address to a fully qualified domain name (FQDN). You want the FQDN that you will be using in the SSL certificate to resolve to the IP address that is displayed on the pod's details page in the Horizon Cloud Administration Console next to the Pod Manager Load Balancer IP label. As an example, let's say you have the pod that is illustrated in the screenshot below and you want to use an FQDN of mypod-a.example.com as the FQDN of that pod for the purposes of the Workspace ONE Access connection to the pod.

<table>
<thead>
<tr>
<th>MontereyStores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod Status</td>
</tr>
</tbody>
</table>

### Summary

<table>
<thead>
<tr>
<th>System Activity</th>
<th>User Activity</th>
<th>Audit Logs</th>
</tr>
</thead>
</table>

### Properties

- Pod ID
- Location: Beverly, MA, United States
- Subscription
- Subscription Limits: 40%
- Pod Manager Load Balancer IP: 192.168.21.4
- Pod Type
- Subscription
- Version No.
- Management Subnet

For this example, in your DNS, you would map mypod-a.example.com to that depicted IP address of 192.168.21.4.
As you perform the steps in the Workspace ONE Access screen for entering the Horizon Cloud tenant information, you specify this FQDN for the Host field in that Workspace ONE Access screen.

- A fully configured pod that has a trusted and valid SSL certificate that you uploaded to the pod itself using the pod details page. For details about uploading the certificate, see Configure SSL Certificates Directly on the Pod Manager VMs, Such As When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs.
- Configured VDI desktop assignments, session desktop assignments, or remote application assignments for the pod.
- Access to your organization's configured Workspace ONE Access tenant environment. Your Workspace ONE Access environment must be configured with trusted certificates.

When using the cloud-hosted Workspace ONE Access, a Workspace ONE Access connector appliance is required for integrating your pod with that tenant. This connector sends the information about user and group entitlements to the virtual desktops and applications to your Workspace ONE Access tenant. You must install the Workspace ONE Access connector appliance in your Active Directory network. Follow the steps as documented in the Workspace ONE Access Cloud Documentation, also available from this documentation page, and see the description of this deployment scenario and subtopics. For the connector version that is required for this release, see the VMware Product Interoperability Matrixes at https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Verify that the connector's configured authoritative time source matches the NTP server that is configured for the pod.

**Note** If you have an existing integration and VMware Workspace ONE® Access™ connector appliance, a best practice is to update the connector before updating the pod to the latest pod software level.

- Verify your configured Workspace ONE Access environment meets all of the prerequisites for integration with Horizon Cloud resources, as described in the Workspace ONE Access documentation.

<table>
<thead>
<tr>
<th>Cloud-hosted</th>
<th>Prerequisites for Integration</th>
</tr>
</thead>
</table>

**Procedure**

1. **Configure a Horizon Cloud Pod in Microsoft Azure for Workspace ONE Access**

   To integrate a pod in Microsoft Azure with Workspace ONE Access, you must configure the pod with the appropriate Workspace ONE Access information. You use the Horizon Cloud Administration Console to configure this information.
2 **Confirm End-User Access to Desktop Assignments in Workspace ONE Access**

After you integrate your Horizon Cloud environment with your Workspace ONE Access environment, you can confirm that end users have remote access to their virtual desktops.

### Configure a Horizon Cloud Pod in Microsoft Azure for Workspace ONE Access

To integrate a pod in Microsoft Azure with Workspace ONE Access, you must configure the pod with the appropriate Workspace ONE Access information. You use the Horizon Cloud Administration Console to configure this information.

#### Prerequisites

Verify that an SSL certificate based on that FQDN is uploaded to the pod itself, as described in Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs. That SSL certificate must be based on the FQDN that you mapped to the pod manager's Azure load balancer IP address in your DNS server, as described in step 4 of Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access.

Verify that your Workspace ONE Access environment is configured use that FQDN, for synchronizing the pod-provisioned end-user resources and entitlements to Workspace ONE Access.

Verify that you have the following information:

- The SAML identity provider (IdP) metadata URL from your Workspace ONE Access environment. You obtain the environment's SAML IdP metadata URL using the Workspace ONE Access administration console and navigating to Catalog > Settings > SAML Metadata. When you click the **Identity Provider (IdP) metadata** link on that page, your browser's address bar displays the URL, typically in the form `https://WS1AccessFQDN/SAAS/API/1.0/GET/metadata/idp.xml`, where `WS1AccessFQDN` is the fully qualified domain name (FQDN) of your Workspace ONE Access environment. For details, see the Workspace ONE Access product information appropriate for your situation:

<table>
<thead>
<tr>
<th>Workspace ONE Access environment</th>
<th>Configure SAML Authentication Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud-hosted</td>
<td>Configure SAML Authentication in the Horizon Cloud Tenant</td>
</tr>
</tbody>
</table>

- The FQDN that you tell your end users to make their connections to, for connecting to Horizon Cloud.

#### Procedure

1 In the Horizon Cloud Administration Console, navigate to **Settings > Identity Management** and click **New**.
2 Configure the following options.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Workspace ONE Access Metadata URL</td>
<td>Type your Workspace ONE Access environment’s SAML IdP metadata URL, typically of the form <a href="https://WS1AccessFQDN/SAAS/API/1.0/GET/metadata/idp.xml">https://WS1AccessFQDN/SAAS/API/1.0/GET/metadata/idp.xml</a> where WS1AccessFQDN is the FQDN of your Workspace ONE Access environment.</td>
</tr>
<tr>
<td>Timeout SSO Token</td>
<td>Type the amount of time, in minutes, after which you want the SSO token to time out. The prefilled, system-default value is zero (0).</td>
</tr>
<tr>
<td>Location</td>
<td>Select one of your locations to filter the Pod drop-down to the set of pods associated with that location.</td>
</tr>
<tr>
<td>Pod</td>
<td>Select the pod for which this configuration applies.</td>
</tr>
<tr>
<td>Data Center</td>
<td>The drop-down displays a numeric related to the Horizon Cloud pod software version. Keep the default.</td>
</tr>
<tr>
<td>Client Access FQDN</td>
<td>Type the FQDN that you tell your end users to make their connections to, for connecting to Horizon Cloud.</td>
</tr>
<tr>
<td>Workspace ONE Redirection</td>
<td>When you also have the configuration to force end-user access to go through Workspace ONE Access, you can set this toggle to YES to have the end users’ clients automatically redirect to their Workspace ONE Access environment. You can read about setting the options to force end-user access to go through Workspace ONE Access in Configure the Option to Force End-User Access to Use Workspace ONE Access. With the automatic redirection configured to YES, in the end-user clients, when the client attempts to connect to Horizon Cloud and you have configured forced authentication through Workspace ONE Access, the client is automatically redirected to the Workspace ONE Access environment that is integrated with the pod. When the toggle is set to NO, automatic redirection is not enabled. When automatic redirection is not enabled and forced access is configured, the clients display an informational message to the user instead. For more details, see Enforce Having End Users Go Through Workspace ONE Access to Access Their Horizon Cloud Entitled Desktops and Applications. Note: You can enable Workspace ONE Access redirection for only one of the identity management providers that are configured here. If the toggle is already set to YES for another configuration and you try to set the toggle to YES, an error message is displayed.</td>
</tr>
</tbody>
</table>

3 Click Save.

Results

A status of green indicates that the configuration is successful.
What to do next

In your Workspace ONE Access environment, sync the entitled desktops and applications to Workspace ONE Access. In the Workspace ONE Access administration console, navigate to Catalog > Virtual Apps until you are on the Virtual Apps Configuration page. Click Sync to sync the Horizon Cloud collection.

**Important**

- Each time resources or entitlements change in Horizon Cloud, a sync is required to propagate the changes to Workspace ONE Access.

- You must also ensure that the authoritative time source you configure in that connector matches the NTP server that is configured for the pod. If the time sources do not match, syncing issues can occur. The pod's details page shows the pod's configured NTP server. You can open the pod's details page from the Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types.

Confirm End-User Access to Desktop Assignments in Workspace ONE Access

After you integrate your Horizon Cloud environment with your Workspace ONE Access environment, you can confirm that end users have remote access to their virtual desktops.

**Prerequisites**

Configure the methods of access you want to provide to end users for accessing their desktops through Workspace ONE Access.

Ensure that the entitled desktops are synced from the integrated Horizon Cloud pod to your Workspace ONE Access environment. In the Workspace ONE Access administration console, navigate to the Virtual Apps Configuration page and sync the Horizon Cloud collection.

**Procedure**

1. Use your organization’s Workspace ONE Access URL to log in to Workspace ONE Access.
2. Launch entitled Horizon Cloud desktops and remote applications from the portal.

Configure True SSO for Use with Your Horizon Cloud Environment

After you have registered an Active Directory domain with your Horizon Cloud environment, you can configure True SSO for it. True SSO is a feature that integrates with Workspace ONE Access to allow users to single sign-on to the virtual Windows desktops and applications served by Horizon Cloud without needing to also enter their Active Directory credentials into the Windows operating system. When True SSO is configured for your environment, the end users authenticate by logging into Workspace ONE Access. After that authentication, the users are
able to launch their entitled desktops or applications without a prompt for Active Directory credentials.

Configuring True SSO for use with your environment is a multi-step process. At a high-level, the steps are:

1. Set up the infrastructure required for True SSO to operate, which involves:
   a. Installing and configuring a Windows Server Certificate Authority (CA) to be an enterprise CA. The procedures in this section are for Windows Server 2012 R2. Very similar steps can be followed on Windows Server 2008 R2.
   b. Setting up a certificate template on the CA.
      \[**Important**\] Use only ASCII characters in the names of your True SSO templates. Due to a known issue, if your True SSO template names contain non-ASCII or high-ASCII characters, you cannot successfully configure True SSO with your Horizon Cloud environment.
   c. Downloading the Horizon Cloud pairing bundle from the Horizon Cloud Administration Console's Active Directory page. The pairing bundle is used when setting up the Enrollment Server.
   d. Setting up the Enrollment Server.
      \[**Important**\] After setting up the Enrollment Server, make sure you meet the port requirements for the Enrollment Server described in DNS Requirements for a Horizon Cloud Pod in Microsoft Azure.

2. Adding the Enrollment Server information to the Horizon Cloud Administration Console's Active Directory page.

When the configuration is complete, the enterprise CA and Enrollment Server work together to issue short-lived certificates that are used to log the users in to their entitled desktops and applications. The Horizon Cloud pod asks the Enrollment Server for a certificate for a specific entitled user. The Enrollment Server contacts the CA to generate the requested certificate and then returns the certificate to the Horizon Cloud pod.

**Prerequisites**

Before configuring True SSO, you must have at least one Workspace ONE Access environment configured. Complete the steps described in Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access.

**Procedure**

1. **Install and Configure a Windows Server 2012 R2 Certificate Authority**

   You can set up a Windows Server 2012 Certificate Authority (CA) using the Service Manager wizard.
2  **Set Up a Certificate Template on the CA**
You must configure the certificate template on the CA. The certificate template is the basis for the certificates that the CA generates.

3  **Download the Horizon Cloud Pairing Bundle**
You need this pairing bundle to complete the Enrollment Server setup steps when you are configuring your Horizon Cloud environment for True SSO. You download the pairing bundle from the Horizon Cloud Administration Console's Active Directory page.

4  **Set up the Enrollment Server**
The Enrollment Server (ES) is a Horizon Cloud component that you install on a Windows Server machine as the last step in setting up infrastructure for True SSO. By deploying the Enrollment Agent (Computer) certificate onto the server, you are authorizing this ES to act as an Enrollment Agent and generate certificates on behalf of users.

5  **Complete Configuring True SSO for your Horizon Cloud Environment**
After the Enrollment Server is set up, you enter the information in the Horizon Cloud Administration Console's Active Directory page.

**Results**
After completing the steps, your environment is configured with True SSO.

**Install and Configure a Windows Server 2012 R2 Certificate Authority**
You can set up a Windows Server 2012 Certificate Authority (CA) using the Service Manager wizard.

The following are standard steps to set up a Microsoft CA. They are detailed here in a simple form suitable for use in a lab environment, but for a real production system it is recommended that you follow industry best practice for CA configuration.

If you need further guidance about setting up a CA, please check out the standard Microsoft technical references: Active Directory Certificate Services Step-by-Step Guide and Install a Root Certification Authority.

**Note**  The procedures in this topic are for Windows Server 2012 R2. Very similar steps can be followed on Windows Server 2008 R2.

**Procedure**

1  On the Server Manager Dashboard, click **Add Roles and Features** to open the wizard, and then and click **Next**.

2  On the Select Installation Type page, select Role-based or feature-based installation and click **Next**.

3  On the Server Selection page, leave defaults and click **Next**.
4 On the Server Roles page:
   a Select Active Directory Certificate Services.
   b In the dialog, select Include management tool (if applicable) and click Add Features.
   c Click Next.
5 On the Features page, click Next.
6 On the AD CS page, click Next.
7 On the Role Services page, select Certification Authority and click Next.
8 On the Confirmation page, select Restart the destination server automatically is required and click Install.
   Installation Progress displays. When the installation is complete, a URL link displays, allowing you to configure the newly installed CA as “Configure Active Directory Certificate Services” on the destination server.
9 Click on the configuration link to launch the configuration wizard.
10 On the Credentials page, enter user credentials from Enterprise Admin group and click Next.
11 On the Role Services page, select CA and click Next.
12 On the Setup Type page, select Enterprise CA and click Next.
13 On the CA Type page, select Root or Subordinate CA as appropriate (in this example it is a Root CA) and click Next.
14 On the Private Key page, select Create a new private key and click Next.
15 On the Cryptography page, enter information as follows.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic Provider</td>
<td>RSA#Microsoft Software Key Storage Provider</td>
</tr>
<tr>
<td>Key Length</td>
<td>4096 (or another length if you prefer)</td>
</tr>
<tr>
<td>Hash Algorithm</td>
<td>SHA256 (or another SHA algorithm if you prefer)</td>
</tr>
</tbody>
</table>
16 On the CA Name page, configure as preferred or accept defaults and click Next.
17 On the Validity Period page, configure as preferred and click Next.
18 On the Certificate Database page, click Next.
19 On the Confirmation page, review the information and click Configure.
20 Complete the configuration process by performing the following tasks (run all commands from the command prompt).

a  Configure CA for non-persistent certificate processing

```bash
certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

b  Configure CA to ignore offline CRL errors

```bash
certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
```

c  Restart the CA service

```bash
net stop certsvc
net start certsvc
```

21 Set up a certificate template on the CA by following the steps in Set Up a Certificate Template on the CA.

Set Up a Certificate Template on the CA

You must configure the certificate template on the CA. The certificate template is the basis for the certificates that the CA generates.

Prerequisites

Complete the steps described in Install and Configure a Windows Server 2012 R2 Certificate Authority.

Procedure

1  Create a new Universal Security Group.

Creating this group allows you to have a single Security Group to which you can assign the permissions required for issuing certificates on behalf of users. All the computers where VMware Enrollment Servers are installed can inherit those permissions by becoming a member of this group.

a  Click Start and type dsa.msc.

The Active Directory Users and Computers window displays.

b  In the tree, right-click the Users folder for the domain controller and select New > Group.

The New Object - Group window displays.

c  In the Group Name field, enter a name for the new group. For example, TrueSSO Enrollment Servers.
d Set the following values.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group scope</td>
<td>Universal</td>
</tr>
<tr>
<td>Group type</td>
<td>Security</td>
</tr>
</tbody>
</table>

e Click OK.

The new group appears in the tree in the Active Directory Users and Computers window.

f Right-click the group and select **Properties**.

g On the Member Of tab, add every computer on which you will be installing an Enrollment Server, and then click **OK**.

h Restart every computer on which you will be installing an Enrollment Server.

2 Configure the certificate template.

a Select **Control Panel > Administrative Tools > Certificate Authority**.

b In the tree, expand the local CA name.

c Right-click on the Certificate Templates folder and select **Manage**.

The Certificate Templates Console displays.

d Right-click on the Smartcard Logon template and select **Duplicate Template**.

The Properties of New Template window displays.
e Enter information on the tabs of the window as described below.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compatibility</td>
<td>■ Select the <strong>Show resulting changes</strong> check box.</td>
</tr>
<tr>
<td></td>
<td>■ Certification Authority - Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>■ Certificate recipient - Windows 7 / Server 2008 R2</td>
</tr>
<tr>
<td>General</td>
<td><strong>Important</strong> Use only ASCII characters in the names of your True SSO templates. Due to a known issue, if your True SSO template names contain non-ASCII or high-ASCII characters, you cannot successfully configure True SSO with your Horizon Cloud environment.</td>
</tr>
<tr>
<td></td>
<td>■ Template display name - Name of your choice. For example, True SSO Template.</td>
</tr>
<tr>
<td></td>
<td>■ Template name - Name of your choice. For example, True SSO Template.</td>
</tr>
<tr>
<td></td>
<td>■ Validity period - 1 hours</td>
</tr>
<tr>
<td></td>
<td>■ Renewal period - 0 weeks</td>
</tr>
<tr>
<td>Request Handling</td>
<td>■ Purpose - Signature and smartcard logon</td>
</tr>
<tr>
<td></td>
<td>■ Select the <strong>For automatic renewal of smart card certificates</strong> ... check box</td>
</tr>
<tr>
<td></td>
<td>■ Select the <strong>Prompt the user during enrollment</strong> radio button</td>
</tr>
<tr>
<td>Cryptography</td>
<td>■ Provider Category - Key Storage Provider</td>
</tr>
<tr>
<td></td>
<td>■ Algorithm name - RSA</td>
</tr>
<tr>
<td></td>
<td>■ Minimum key size - 2048</td>
</tr>
<tr>
<td></td>
<td>■ Select the <strong>Requests can use any provider available</strong> ... radio button</td>
</tr>
<tr>
<td></td>
<td>■ Request hash - SHA256</td>
</tr>
<tr>
<td>Subject Name</td>
<td>■ Select the <strong>Build from this Active Directory Information</strong> radio button</td>
</tr>
<tr>
<td></td>
<td>■ Subject name format - Fully distinguished name</td>
</tr>
<tr>
<td></td>
<td>■ Select the <strong>User principal name (UPN)</strong> check box</td>
</tr>
<tr>
<td>Server</td>
<td>Select the <strong>Do not store certificates and requests in the CA database</strong> check box</td>
</tr>
<tr>
<td>Issuance Requirements</td>
<td>■ Require the following for enrollment - Select <strong>This number of authorized signatures</strong> and enter 1.</td>
</tr>
<tr>
<td></td>
<td>■ Policy type required in signature - Application policy</td>
</tr>
<tr>
<td></td>
<td>■ Application policy - Certificate Request Agent</td>
</tr>
<tr>
<td></td>
<td>■ Require the following for enrollment - Valid existing certificate</td>
</tr>
<tr>
<td>Security</td>
<td>In the upper part of the tab, select the new group you created. Then in the lower part of the tab, select <strong>Allow</strong> for Read and Enroll permissions.</td>
</tr>
</tbody>
</table>

f Click **OK**.

3 Issue the template for True SSO.

a Right-click again on the Certificate Templates folder and select **New > Certificate Template to Issue**.

     The Enable Certificate Templates window displays.

b Select TrueSsoTemplate and click **OK**.
4  Issue the Enrollment Agent template.
   a  Right-click again on the Certificate Templates folder and select **New > Certificate Template to Issue**.
      The Enable Certificate Templates window displays.
   b  Select the Enrollment Agent computer and click **OK**.
      
      **Note**  This template must have the same security settings as the template issued in the previous step.

      The CA is now set up and configured with a certificate template suitable for use with True SSO.

5  Download the Horizon Cloud pairing bundle by following the steps in **Download the Horizon Cloud Pairing Bundle**.

**Download the Horizon Cloud Pairing Bundle**

You need this pairing bundle to complete the Enrollment Server setup steps when you are configuring your Horizon Cloud environment for True SSO. You download the pairing bundle from the Horizon Cloud Administration Console’s Active Directory page.

The pairing bundle contains a certificate file for each one of the Horizon Cloud pods deployed in Microsoft Azure for your Horizon Cloud environment. For the pods for which you want to configure True SSO, you upload those pods’ certificate files to the Enrollment Server. When you have one pod, the bundle contains one certificate file in CRT format. When you have more than one pod, the bundle contains multiple CRT files, one per pod. The name of each CRT file follows the pattern:

```
podID_truesso.crt
```

where `podID` is the pod's ID that is displayed in the pod's summary page.

**Procedure**

1  In the console, navigate to **Settings > Active Directory**.

2  In the True SSO Configuration area, obtain the `pairing_bundle.7z` file by clicking **Download Pairing Token**.

3  Save the file to a location where you can extract its contents.

4  For the pods for which you want to configure True SSO, extract the pods' CRT files from the pairing bundle to a location where you can retrieve them when you are setting up the Enrollment Server.

   The pairing bundle contains a certificate file for each pod in your environment. Each CRT file name follow the pattern `podID_truesso.crt`, where `podID` is the pod's ID value.

5  Set up the Enrollment Server by following the steps in **Set up the Enrollment Server**.
Set up the Enrollment Server

The Enrollment Server (ES) is a Horizon Cloud component that you install on a Windows Server machine as the last step in setting up infrastructure for True SSO. By deploying the Enrollment Agent (Computer) certificate onto the server, you are authorizing this ES to act as an Enrollment Agent and generate certificates on behalf of users.

Prerequisites

Verify that you have completed the steps in Install and Configure a Windows Server 2012 R2 Certificate Authority, Set Up a Certificate Template on the CA, and Download the Horizon Cloud Pairing Bundle.

Procedure

1. Install the Enrollment Server.
   a. Download the EnrollmentServer.exe file from the My VMware site. The file name should be similar to VMware-HorizonCloud-TrueSSOEnrollmentServer-x86_64-7.3.0-xxxxx.exe.
   b. Confirm that the system is running Windows Server 2008 R2, 2012 R2, or 2016, and that it has a minimum of 4GB memory.
   c. Run the installer and follow the wizard.

2. Deploy the Enrollment Agent (Computer) Certificate.
   a. Open the Microsoft Management Console (MMC).
   b. On the File menu, click Add/Remove Snap-in.
   c. Under Available snap-ins, double-click Certificates.
   d. Select Computer account and click Next.
   e. Select Local computer and click Finish.
   f. On the Add or Remove Snap-ins dialog, click OK.
   g. In the MMC, right-click the Personal folder under Certificates and select All Tasks > Request New Certificates.
   h. In the Certificate Enrollment dialog, select the check box for the Enrollment Agent (Computer) and click Enroll.

3. Import the pods' certificate CRT files extracted from the pairing_bundle.7z file, for those pods with which you want to configure True SSO.

   The pairing bundle contains a certificate file for each pod in your environment. Each CRT file name follow the pattern podID_truesso.crt, where podID is the pod's ID value.
   a. In the MMC, right-click the Certificates sub-folder under the VMware Horizon Cloud Enrollments Server Trusted Roots folder and select All Tasks > Import.
   b. Click Next.
c Navigate to the location where you extracted the certificate files from the pairing_bundle.7z bundle.

When you have only one pod, the bundle contains only one CRT file. When you have more than one pod, the bundle contains a CRT file for each pod.

d Import the certificate file or files, depending on how many pods you are configuring.

e Click Next, then click Finish.

4 Complete the remaining configuration steps described in Complete Configuring True SSO for your Horizon Cloud Environment.

**Complete Configuring True SSO for your Horizon Cloud Environment**

After the Enrollment Server is set up, you enter the information in the Horizon Cloud Administration Console's Active Directory page.

**Prerequisites**

Complete the previous step Set up the Enrollment Server.

Verify that you have met the port and protocol requirements for the pod's manager VMs and Enrollment Server network traffic, as described in DNS Requirements for a Horizon Cloud Pod in Microsoft Azure. If the appropriate ports are not allowing traffic, pairing of the Enrollment Server will fail.

**Procedure**

1 In the console, navigate to Settings > Active Directory.

2 Click Add next to True SSO Configuration.

   The True SSO Config dialog displays.

   **Note** Because you already configured the Enrollment Server you can ignore the Download Pairing Token link in this dialog.

3 Enter the fully-qualified domain name (FQDN) of your enrollment server in the Primary Enrollment Server field and click the Test Pairing button next to the field.

   The other required fields are auto-populated.

4 Click Save

5 To configure a Secondary Enrollment Server for high-availability, do the following.

   a Repeat the process described in Set up the Enrollment Server on a second machine.

   b Edit the True SSO configuration and add the second ES address in the Secondary Enrollment Server field, and then test the pairing.

   c Save the configuration again.
Results
The configuration information now appears on the Active Directory page under True SSO Configuration.

End User Connections to Desktops and Applications Provided by Your Horizon Cloud Environment
These topics provide information about areas related to your end users' connections to their entitled desktops and remote applications.

When Using PCOIP URLs and a Pod with an Internal Gateway Configuration
As described in Chapter 7 Introduction to Horizon Cloud Pods in Microsoft Azure, a Horizon Cloud pod in Microsoft Azure can be configured with an internal gateway configuration, using Unified Access Gateway instances. For the internal gateway type, even though HTML Access (Blast protocol) configures its external URL to be your provided FQDN, the PCOIP URL uses IP addresses instead. This behavior makes for a difference between the external gateway and internal gateway types with respect to PCOIP:

- External gateway type: the PCOIP URL is set to the public IP of the external gateway configuration's load balancer resource.
- Internal gateway type: the PCOIP URL first attempts to resolve your provided FQDN using DNS to an IP address, and then uses that as the PCOIP URL. If the PCOIP URL cannot resolve your provided FQDN, the PCOIP URL instead uses the private IP address of the internal gateway configuration's internal load balancer resource.

Now, your network environment might be such that the internal gateway configuration's load balancer is not the first endpoint in an end-user connection attempt. As an example, you might have an additional endpoint or load balancer that you have set up to redirect to the internal gateway configuration's load balancer. In the certificate you uploaded to the internal Unified Access Gateway gateway configuration when you deployed or edited the pod, you likely have made that certificate match the FQDN or IP addresses of that first endpoint in your networking setup. You likely did that because you expect your end-user clients to access your network environment starting with that first endpoint. If your network environment matches this description, where your end-user clients first access an endpoint that is not the internal gateway configuration's load balancer as their first endpoint, you must ensure your DNS mapping provides for the PCOIP URL to match for your end-user clients to properly authenticate against your provided certificate.

Enable Time Zone Redirection for RDS Desktop and RDS-Based Application Sessions
If a farm's RDSH VM is in one time zone and the end user is in another time zone, by default, when the user connects to their RDS session-based desktop, the desktop displays time that is in
the time zone of the farm’s RDSH VM. You can enable the Time Zone Redirection group policy setting to make the session-based desktop display time in the local time zone. This policy setting applies to remote application sessions as well.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.
  

- Verify that the Horizon RDS ADMX files are added to your Active Directory. For an example of these steps from the VMware Horizon product documentation, see the Add the ADMX Template Files to Active Directory documentation topic located in the VMware Horizon product documentation.

- Familiarize yourself with the group policy settings. In that same VMware Horizon documentation, see RDS Device and Resource Redirection Settings.

Procedure

1. On the Active Directory server, open the Group Policy Management Console.
2. Expand your domain and Group Policy Objects.
3. Right-click the GPO that you created for the group policy settings and select Edit.
5. Enable the setting Allow time zone redirection.

Multiple-Monitor Support for Desktops and Remote Applications Provided By a Horizon Cloud Pod in Microsoft Azure

This topic describes specific support for using multiple monitors with the end-user entitled resources provisioned by a Horizon Cloud pod in Microsoft Azure.

For general and extensive details about using monitors and screen resolution in the Horizon Client used by end users, see Monitors and Screen Resolution.

Note Due to the number of variables in your end users’ environments that can affect their graphical user experience — such as network conditions, bandwidth consumption, workload intensity, and so on — testing is recommended so that you can identify the usability, cost, and performance mix which best meet your specific business requirements.

The configurations in the following table are for a typical knowledge worker workload, such as a combination of office productivity applications, streaming media in a browser, and Internet use. Your experience might vary due to VM size, display protocol you are using, screen resolution, workload, and other factors.
Table 7-30. Supported Configurations for RDSH VMs

<table>
<thead>
<tr>
<th>VM Type</th>
<th>Graphics By</th>
<th>Workload</th>
<th>Monitor Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-GPU-backed RDSH VM</td>
<td>Microsoft Hyper-V display adapter</td>
<td>Basic, not requiring advanced graphics features or HD video playback</td>
<td>Single 4K display</td>
</tr>
<tr>
<td>GPU-backed NV-Series RDSH VM</td>
<td>NVIDIA GRID GPU</td>
<td>Graphics intensive or requiring advanced graphics features</td>
<td>Single 4K display</td>
</tr>
<tr>
<td></td>
<td>For driver details, see:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-gpu#nv-series">https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-gpu#nv-series</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 7-31. Supported Configurations for VDI Desktop VMs

<table>
<thead>
<tr>
<th>VM Type</th>
<th>Graphics By</th>
<th>Workload</th>
<th>Monitor Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-GPU-backed VDI desktop VM</td>
<td>VMware Display Adapter</td>
<td>Basic, not requiring advanced graphics features or HD video playback</td>
<td>Single 2560x1440 display Two 1920x1080 displays</td>
</tr>
<tr>
<td></td>
<td>Note This driver is not the VMware ESX display driver. Microsoft software rendering is used for advanced graphics features.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPU-backed VDI desktop VM</td>
<td>NVIDIA GRID GPU</td>
<td>Graphics intensive or requiring advanced graphics features</td>
<td>Up to four 4K displays</td>
</tr>
<tr>
<td></td>
<td>For driver details, see:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-gpu#nv-series">https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-gpu#nv-series</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Horizon Cloud — Support of Media Optimization for Microsoft Teams

You can use the Horizon remote experience feature for Media Optimization for Microsoft Teams with the virtual desktops and remote apps that are provisioned from your cloud-connected pods. As described in the document *VMware Horizon Configuring Remote Desktop Features in Horizon*, this feature provides for Teams media processing to take place on the client machine instead of in the virtual desktop.
For pods in Microsoft Azure, use of this feature requires pod manifest 2298.0 or later and Horizon Agents Installer (HAI) version of 20.2 or later. As of August 11, 2020, you can use the latest 2006 version of the Horizon Clients to obtain use of this feature with virtual desktops provisioned from those pods. The details of this feature used with the 2006 Horizon Clients can be found in the *VMware Horizon Configuring Remote Desktop Features in Horizon* document’s Configuring Media Optimization for Microsoft Teams.

### Access Desktops and Applications

After you create desktop and application assignments, end users can access desktops and applications using the Horizon Client or a browser using Horizon HTML Access capabilities. If you have integrated your environment with your VMware Workspace ONE® Access™ environment, you can optionally enforce end-user access to go through that environment.

### Log In to Desktops or RDS-Based Remote Applications Using the Horizon Client

When your end users connect to Horizon Cloud using the Horizon Client, they can work with their assigned desktops or remote applications.

These steps describe using Horizon Client for the first time to connect to a desktop provided by a Horizon Cloud pod.

**Important** If you are assigning URL redirection to your end users, they must install their Horizon Client with the URL Content Redirection feature enabled for them to take advantage of that feature. The client must be installed using the command line to enable URL Content Redirection in the client. As a starting point to learn about this area, see these topics in the Horizon Client documentation:

- Installing Horizon Client for Windows from the Command Line
- Clicking URL Links That Open Outside of Horizon Client

### Prerequisites

- Familiarize yourself with the most up-to-date information regarding VMware Horizon Clients. For example, to check for up-to-date Horizon Client support information, see the VMware Product Interoperability Matrixes at [https://www.vmware.com/resources/compatibility/sim/interop_matrix.php](https://www.vmware.com/resources/compatibility/sim/interop_matrix.php) and to see the respective documentation, see the Horizon Client documentation page at [https://docs.vmware.com/en/VMware-Horizon-Client/index.html](https://docs.vmware.com/en/VMware-Horizon-Client/index.html).

- From your organization's DNS information, obtain the fully qualified domain name (FQDN) that your organization has associated in its domain name system (DNS) for end-user connections to this pod, such as desktops.mycorp.example.com.
For example, when the Horizon Cloud pod in Microsoft Azure is configured to use Unified Access Gateway for end-user connections, your organization has a DNS CNAME or A record that maps the FQDN that you provided in the deployment wizard to the auto-generated public FQDN of the pod’s deployed load balancer. See Obtain the Pod Gateway’s Load Balancer Information to Map in your DNS Server for a description of this auto-generated public FQDN.

If you want those Horizon clients that have implemented the client retry feature to automatically retry the connection when the system has to power on the underlying desktop VM or farm RDSH VM, set the Allow Client to Wait for Powered-Off VM option to Yes in the Horizon Cloud Administration Console’s Broker page. The Horizon Client for Windows and Horizon Client for Mac starting with version 4.8 and later have this feature implemented.

Procedure

1. Start the Horizon Client.
2. In the client, select the choices to add a new server.
3. In the new server configuration, enter the name that was added to your DNS for end-user connections, for example, desktops.mycorp.com.
4. Enter the credentials for your Active Directory user in the authentication dialog box.
5. If RADIUS two-factor authentication is configured for this pod, enter the RADIUS credentials.
6. From the displayed list of entitled desktops and remote applications, connect to the one you want to use.

When the underlying desktop VM or farm RDSH VM is powered off, due to any power-management schedules configured in the VDI desktop assignment or farm, the system starts powering on the VM in response to the connection request. If you are running version 4.8 or later of Horizon Client for Windows or Horizon Client for Mac and you have Allow Client to Wait for Powered-Off VM option set to Yes for your tenant environment, the client displays a message describing the connection will be made when the desktop is ready and the estimated time it might take.

7. (Optional) To configure additional options that apply when you launch the selected desktop or application, right-click the icon and make your selection.

Log In to Desktops and RDS-Based Remote Applications Using a Browser

Your users can access the resources in your Horizon Cloud environment that you have entitled to them by pointing their browser to the fully qualified domain name (FQDN) that your organization has configured for end-user connections to those resources.
These steps describe using a browser to launch a desktop provided by the pod.

**Note** If integration with a VMware Workspace ONE® Access™ environment is configured, end users might have to access their desktops and remote applications using that environment. See Enforce Having End Users Go Through Workspace ONE Access to Access Their Horizon Cloud Entitled Desktops and Applications.

**Prerequisites**
- Familiarize yourself with the most up-to-date information regarding Horizon HTML Access. For example, to check for up-to-date Horizon HTML Access support information, see the VMware Product Interoperability Matrixes at https://www.vmware.com/resources/compatibility/sim/interop_matrix.php and to see the respective documentation, see the Horizon HTML Access documentation page at https://docs.vmware.com/en/VMware-Horizon-HTML-Access/index.html.
- From your organization's DNS information, obtain the fully qualified domain name (FQDN) that your organization has associated in its domain name system (DNS) for end-user connections to this Horizon Cloud pod in Microsoft Azure, such as desktops.mycorp.example.com.
  For example, when the pod is configured to use Unified Access Gateway for end-user connections, your organization's DNS has a CNAME record that maps the FQDN configured on the gateway to the Azure load balancer's auto-generated public FQDN. See Obtain the Pod Gateway's Load Balancer Information to Map in your DNS Server.
- If you want your end users' Horizon HTML Access clients to retry the connection automatically when the system has to power on the underlying desktop VM or RDSH VM, set the **Allow Client to Wait for Powered-Off VM** option to **Yes**. This option is located on the Horizon Cloud Administration Console's Broker page. The Horizon HTML Access client starting with version 4.10 has this feature implemented.
- Verify that you have the credentials for a user that has a VDI desktop, session desktop, or remote application assignment.

**Procedure**

1. Point a browser to a URL of the form https://<desktops-FQDN>, where *desktops-FQDN* is the fully qualified domain name that was added to your DNS for end-user connections.
   For example, if your company's DNS associated an FQDN of myDesktops.example.com, point the browser to https://myDesktops.example.com.

2. Sign in using the credentials for a user that has a desktop assignment.

**Results**

Icons representing the user's assignments are displayed in the browser. The user can launch a desktop or application by clicking its icon.
Accessing Local Files with Remote Applications Using File Redirection

The file redirection feature allows users to open local files in entitled remote applications that support a given file type.

The feature is enabled in the Horizon Client when the **Open local files in hosted applications** option is selected.

This functionality allows users to do the following:

- Open a local file in a remote application by double-clicking the file in the client machine or by right-clicking, selecting **Open with**, and choosing the remote application in the menu.
- In the remote application, browse the complete folder where the file resides.
- Save changes made using the remote application to the local client disk.
- Register an entitled application as a file handler for the file types that those applications can open, or chose to open with the remote application a single time.

When an application is set as the default handler:

- The file’s preview icon matches the entitled application’s icon in the application launcher page.
- The file type description is overridden by the remote application, if any.
- Double-clicking a file of that type launches the Horizon Client.

Enforce Having End Users Go Through Workspace ONE Access to Access Their Horizon Cloud Entitled Desktops and Applications

When you have integrated your Horizon Cloud environment with your Workspace ONE Access environment, you can specify that end users must go through Workspace ONE Access to access their desktops. Requiring end users to access their desktops through Workspace ONE Access prevents direct desktop access using their Horizon Client or by HTML access. This enforcement is useful when you want to use the two-factor authentication method that is set in your Workspace ONE Access environment.

Your end users typically launch their entitled desktops using the following methods.

- From a browser, by loading the FQDN for end-user access that your organization’s DNS records have associated with the pod they need to access.
- From the Horizon Client application, by including that FQDN as a new server location in the client application.
- From Workspace ONE Access, if your environments are integrated.

In the Horizon Cloud Administration Console, you can optionally configure your Horizon Cloud environment to require your end users use Workspace ONE Access only. You can configure enforcement on users who are accessing their desktops and applications from locations outside your corporate network or on users accessing from inside your corporate network, or both. You can also configure the client to automatically redirect to Workspace ONE Access the enforcement is enabled.
The feature to force end-user access to Workspace ONE Access works with the Workspace ONE Access redirection feature in the following ways.

<table>
<thead>
<tr>
<th>Force end-user access through Workspace ONE Access setting</th>
<th>Workspace ONE Access redirection setting</th>
<th>What happens when the end user's client connects to Horizon Cloud to access their desktops and applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled (yes)</td>
<td>Enabled (yes)</td>
<td>Client is automatically redirected to Workspace ONE Access.</td>
</tr>
<tr>
<td>Enabled (yes)</td>
<td>Disabled (no)</td>
<td>Client displays a message that tells the user that they must access Horizon Cloud using Workspace ONE Access. Automatic redirection does not occur.</td>
</tr>
<tr>
<td>Disabled (no)</td>
<td>Enabled (yes)</td>
<td>Client displays the Horizon Cloud login screen for the end user to log in. Automatic redirection does not occur because forced access to Workspace ONE Access is not enabled.</td>
</tr>
<tr>
<td>Disabled (no)</td>
<td>Disabled (no)</td>
<td>Client displays the Horizon Cloud login screen for the end user to log in. In this scenario, both forced access and the automatic redirection features are disabled.</td>
</tr>
</tbody>
</table>

Prerequisites

Verify that your Horizon Cloud and Workspace ONE Access environments are successfully integrated. See Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access.

Procedure

1. In the console, navigate to **Settings > Identity Management** and click **Configure**.
2. In the dialog box, make selections according to your organization’s needs.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Force Remote Users to Workspace ONE Access</strong></td>
<td>When set to <strong>Yes</strong>, users that are trying to access their desktops from locations outside of your corporate network must log in to Workspace ONE Access and access desktops from there.</td>
</tr>
<tr>
<td><strong>Force Internal Users to Workspace ONE Access</strong></td>
<td>When set to <strong>Yes</strong>, users that are trying to access their desktops from locations within your corporate network must log in to Workspace ONE Access and access desktops from there.</td>
</tr>
</tbody>
</table>

3. Click **Save** to confirm the configuration to the system.
4 (Optional) Set Workspace ONE Access redirection on the identity management configuration.

**Note** You can have Workspace ONE Access redirection enabled for only one of the identity management URLs that are configured on the Identity Management page. If your Identity Management page lists multiple configurations with different identity management URLs, and one is associated with the toggle is set to **YES**, when you try to set the toggle to **YES** for a different identity management URL, an error message is displayed.

a On the Identity Management page, select the check box for the Workspace ONE Access configuration for which you want to set redirection and click **Edit** to open its configuration.

b Set the **Workspace ONE Redirection** toggle to **YES**.

c Click **Save**.

What to do next

Verify that the desktop access behaves according to your settings by trying to access a desktop using the Horizon Client or using a browser directly instead of through Workspace ONE Access.
The Horizon Cloud administrative console’s menus provide a quick way to navigate to monitor activity and perform various functions in your Horizon Cloud environment. These menus are located along the left side of the console.

### Table 8-1. Console Navigation Menus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting Started</td>
<td>If you set the Getting Started page as your default landing page, clicking this icon displays the Getting Started page. See About the Horizon Cloud Getting Started Wizard. Otherwise, clicking this icon displays the Health Visibility and Insights into Your Cloud-Connected Pods Provided by the Cloud Monitoring Service in Horizon Cloud.</td>
</tr>
</tbody>
</table>
| Monitor    | Provides access to:  
- Dashboard that depicts information about your overall environment: issue status, capacity and utilization levels, end-user activity, and more.  
- Activity reports and audit logs.  
- Various detailed reports related to end users' desktop and application sessions.  
- Notifications.                                                                                                                                 |
| Assignments| Provides access to the console's assignments-related area from which you can work with assignments that entitle end-user access to those assignable items that are in your environment's inventory.                                                                                   |

**Tip** The console is dynamic and reflects the workflows and settings that are appropriate for the up-to-the-moment situation in your Horizon Cloud tenant environment. The labels displayed for the console's assignment-related pages will vary depending on factors such as the tenant's configured brokering setting, the types of cloud-connected pods in your fleet, the tenant's regional cloud plane, and features that are based on specific licensing.
Table 8-1. Console Navigation Menus (continued)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Inventory** | When your environment has pods deployed in Microsoft Azure, this console area provides access to work with assets such as:  
- Base image virtual machines and other virtual machines (if any) that the system has imported from your in-cloud pod.  
- Published (sealed) images  
- RDSH farms  
- Remote applications from the RDSH farms  
- App Volumes applications, when your tenant environment is enabled to use App Volumes.  
When your environment has cloud-connected Horizon pods, this console area provides access to work with images that are managed in the cloud plane. |
| **Settings** | Provides access to screens from which you can work with system-wide settings and configurations for various system areas such as:  
- Active Directory domains  
- Roles and permissions  
- Capacity-related aspects of your environment  
- Identity management using Workspace ONE Access.  
- The VM types and sizes used for pods in Microsoft Azure  
- Configuration settings that apply to your environment and your pod fleet overall  
- Getting Started page |

This chapter includes the following topics:

- About the Monitor Menu in the Horizon Cloud Administration Console
- About the Assignments Menu in the Horizon Cloud Administration Console
- About the Inventory Menu in the Horizon Cloud Administration Console
- About the Settings Menu in the Horizon Cloud Administration Console

**About the Monitor Menu in the Horizon Cloud Administration Console**

Use **Monitor** to navigate to various dashboards, displays, and reports. You can explore details about usage of your environment, the administrator and user activity in the environment, see system notifications, and view various reports.

Click **Monitor** to navigate to these pages.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Displays information about your overall environment: pod health status, capacity and utilization levels, end-user activity, and more.</td>
</tr>
<tr>
<td>Activity</td>
<td>Provides activity details for administrators and end users, and audit logs.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reports</td>
<td>Provides access to various reports related to end users' desktop and application sessions.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you have disabled monitoring user-session information for utilization, trending, and historical analysis, the associated data reports are disabled and not visible on the Reports page. When that monitoring feature is disabled, the system collects such user session information for a limited period of time and hashes the user name to enable real-time administration while disabling historical and aggregated viewing of that user information. As a result, the reports that usually display historical and aggregated viewing of that data, such as the Session History report, are not available. For information on how to enable the monitoring of user-session information, see the monitoring section of Customizable General Settings for Your Horizon Cloud Tenant Environment.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Lists notifications, which provide information about the system, such as important events.</td>
</tr>
</tbody>
</table>

### Activity Page

The Activity page shows data regarding current and past events in the system.

The Activity page is available from the Monitor icon. You can perform these tasks.

- Filter the events displayed using the filter tools available on each tab.
- Refresh the list.
- Cancel some Administrator events. See below for more information.
Download the displayed information as a report file with the Export feature.

**Important** On the Users tab, if you select All Pods in the pod filter, the download button is disabled. You can download data for all of your pods by performing a download for each pod.

**Note** If you have many activity records, plan to download the information when you can wait up to 10 minutes before performing other tasks in the console. After you make your selections for the downloaded report, the system starts preparing the report. A message appears stating that the report is being compiled and it can take some time. Depending on the number of records, the preparation time can take several minutes. For example, a report with 50,000 records takes approximately 10 minutes. When the preparation is done, another dialog box appears with the message Report Generated Successfully and a Download button. After clicking the Download button, you must wait for the download to complete before closing this dialog box. Closing it before the download is complete cancels the download.

For the report file for the audit logs, the system generates an XLSX file. For the report file for the administrator or user events, the system generates a CSV file, and then a ZIP file containing that CSV file. The data in the generated CSV file is not sorted by date. You can correct that in one of the following ways:

- Open the CSV file in Excel and set the date format for the cells that contain dates to *mm/dd/yy hh:mm AM/PM*.
- In Excel, create a new blank workbook and use Excel's Data Import wizard to import the downloaded CSV file.

The Activity page contains tabs for administrator events, user events, and audit logs for events initiated on your pods.

**Administrator Events**

The Admins tab displays information about administrator events. Expand an event to view details and subtasks for that event. Click an event to view details and progress for that event. Click the event description to view further information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Details regarding the event.</td>
</tr>
<tr>
<td>Status</td>
<td>Successful indicates that an event was performed in its entirety. Failed indicates that an event was either partially performed or not performed at all.</td>
</tr>
<tr>
<td>% Completion</td>
<td>Current percentage of event completed.</td>
</tr>
<tr>
<td>Time</td>
<td>Time that the event was logged.</td>
</tr>
</tbody>
</table>

These filtering options are available on the Admins tab:

- Display events for only a certain time period, a specific pod, or a certain status, using the filters at the top of the tab.
Filter events shown in the table using the filter tool in each column.

From the Admins tab, you can cancel assignment-related tasks before they complete by selecting the task in the list and clicking Cancel Tasks.

Before attempting to select a task for cancellation, refresh the view to update the status for the tasks displayed.

If a task is currently in a state where the system allows you to cancel it, you can select the check box corresponding to that cancellable task. If all tasks in the list are cancellable, you also have the option of selecting the 'select all' check box at the top of the list to cancel all tasks. If not, you must select tasks individually.

The following table shows the tasks that you can cancel.

<table>
<thead>
<tr>
<th>Task</th>
<th>Cancel When Task is in Queued State</th>
<th>Cancel When Task is in Running State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Farm Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the system has automatically created an expansion task for an RDSH farm, the farm must be offline before you can cancel that task.</td>
<td>Note the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- When the system has automatically created an expansion task for an RDSH farm, the farm must be offline before you can cancel that task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Resources that have already been created, such as VMs and OS/data disks, are destroyed when the task is canceled. When VMs are destroyed or not created, this changes the size of the assignment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- This option is not available for multi-cloud assignments.</td>
</tr>
<tr>
<td>Assignment Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the system has automatically created an expansion task for a VDI desktop assignment, the assignment must be offline before you can cancel that task.</td>
<td>Note the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- When the system has automatically created an expansion task for an RDSH farm, the farm must be offline before you can cancel that task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Resources that have already been created, such as VMs and OS/data disks, are destroyed when the task is canceled. When VMs are destroyed or not created, this changes the size of the assignment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- This option is not available for multi-cloud assignments.</td>
</tr>
<tr>
<td>Convert VM to Image</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you cancel this task, and want to retry it, first confirm that the VM is in a state where it can be converted. If you are not sure, power off and then power on the VM.</td>
<td><strong>Note</strong> If you cancel this task, and want to retry it, first confirm that the VM is in a state where it can be converted. If you are not sure, power off and then power on the VM.</td>
</tr>
</tbody>
</table>
User Events
The Users tab displays descriptions and times logged for end-user events. These filtering options are available on the Users tab:

- Display events for only a certain time period or a specific pod, using the filters at the top of the tab.
- Filter events shown in the table using the filter tool in each column.

Audit Logs
The Audit Logs tab displays the time, status, description, and user information logged for events that have occurred from administrator-initiated actions on your pods. For more information, see Working with Audit Logs.

You can filter events displayed using the Filters tool at the top of the tab.

Reports Page
Use the Reports page to access various reports related to end users’ desktop and application sessions.

Important  The Desktop Health, Utilization, Azure Concurrency, Sessions, and VDI Applications Usage reports do not reflect user-related data until an hour has passed from the time you deployed your Horizon Cloud pod into Microsoft Azure or from the time you enabled monitoring user session information.

In addition to that one hour elapsed time, four of the reports are updated at specific UTC (Coordinated Universal Time) times: Utilization, Azure Concurrency, Sessions, and VDI Applications Usage. As a result, those reports might not be populated with information collected during the time since the last UTC update time for that report. For details, see the table below.

Select Monitor > Reports to open the Reports page, where you can view detailed information for a variety of report types. When you create a report, it displays in the console with options to filter the results, manually refresh the page, and export data to a Microsoft Excel worksheet.

There are two tabs on the Reports page. On the Create Report tab, you click the report type to create the report in the console. The My Reports tab lists Sessions, VDI Applications Usage, and User Usage reports that have been prepared for download.

Exporting Report Data
There are two different export functions, depending on the type of report:

- For most reports, you export data by clicking the export button at the top right of the report table. The Microsoft Excel worksheet containing the report data downloads immediately.
For Sessions, VDI Applications Usage, and User Usage reports, you export data by clicking the Export button at the top left of the report table and set parameters for report data to export. Because these reports are larger than other types, they take longer to complete. So that you do not have to wait for the process to finish, you enter one or more email addresses to be notified when the report is ready for download on the My Reports tab of the Reports page.

To export data for a Sessions, VDI Applications Usage, or User Usage report:

1. Click the **Export** button at the top left of the report table.
2. At the top of the Export Report dialog box, enter the following.
   - **Period** - Select a period from the drop-down menu. The longest period you can select from the menu is **Last 90 days**. If you select **Custom** and set a period of longer than 90 days, the export fails.
   - **Description** - (Optional) Enter a description of up to 250 words. This description appears in the list on the My Reports tab to help you identify the specific report.
3. Under Notifications in the Export Report dialog box, enter the following.
   - **Email address** - Enter an email address to receive a notification when the report is ready for download.
   - **Notify others** – (Optional) You can enter up to five additional email addresses, separated by commas, to send notifications to other individuals in your team.
4. Click **Export**.
   
   A dialog box displays indicating that the export process has begun.
5. Click **OK**.
   
   When the report is ready for download, the system sends a notification email to the email addresses you entered. This email contains a link to the My Reports tab of the Reports page, where the report appears in the list.

**Note** If you have been logged out from the console, you are prompted to log back in to access the My Reports tab.

6. On the My Reports tab, select the report in the list and click **Download**.

**Important** In larger deployments, the CSV file generated by the system might be too large to be opened by Microsoft Excel. In this case, you can repeat the export using a shorter time period to avoid this issue.
Report Types

**Note** If you have disabled monitoring user session information for utilization, trending, and historical analysis, the reports associated with that type of data are disabled and not visible on the Reports page. When the Cloud Monitoring Service is disabled, the system collects such user session information for a limited period of time and hashes the user name to enable real time administration while disabling historical and aggregated viewing of that user information. As a result, the reports that would display historical and aggregated viewing of that data, such as the Sessions report, are not available.

For information about toggling the Cloud Monitoring Service options, see [Enabling or Deactivating the Cloud Monitoring Service (CMS) for Your Horizon Cloud Tenant Environment](#).

The vRealize Operations Desktop Agent option is installed by default. If you do not install this option, activity-related data from user sessions in the desktop instance or farm RDSH instances based on this image is not reported. As a result, data from end-user activity and other types of desktop activity will not be displayed in reports in the administrative console. Also, for the RDP protocol, the vRealize Operations Desktop Agent provides only a subset of metrics that it provides for other protocols.

**Caution** If you have cloud-connected Horizon pods that are sending desktop data to vRealize Operations Manager, enabling CMS causes data to be sent to the Cloud Monitoring Service instead. To continue using vRealize Operations Manager to collect that desktop session data, disable CMS.
## Report Type

### User Mapping
View details and sort by various categories, such as User name, Domain, Desktop Name, Desktop Model, Farm, and Mapping Type (User or Group).

**Note** This report is populated only for users that have at least one direct assignment to a desktop. In the console, you can select individual users or user groups when making a desktop assignment. If a user has at least one assignment done as an individual user and zero or more assignments done as being part of the assigned group, this report reports all of that user’s desktop assignments.

However, if all the user’s desktop assignments are done using groups, that user’s assignments are not reported in this report.

If the user is mapped to a desktop as an individual user, the Group Name column is blank. If the user is mapped to a desktop from being a member of a group that is entitled to the desktop assignment, the Group Name column displays the entitled group’s name.

### Desktop Mapping
View details and sort by various categories, such as Desktop Name, Model, Assignment Name, Type, Farm, Active User, Mapped Users, and Mapped User Groups.

**Note** In this report, the Mapped Users column is populated only for dedicated VDI desktop assignments, because for such assignments, each user gets mapped to a specific VDI desktop and returns to that same desktop at each login. That mapped user is the user assigned to that desktop. However, for floating VDI desktop assignments and session desktop assignments that are served by farms, users do not get mapped to specific desktop VMs. As a result, there is no data in the Mapped Users column for those desktop assignment types.

### Desktop Health
View list of desktops, which you can filter by assignment or error status. Click a desktop to view its real-time desktop health report.

- For RDS desktops, the report includes CPU use %, memory use %, disk IOPS, and active/disconnected sessions.
- For VDI desktops, the report includes CPU use %, memory use %, disk IOPS, duration, bandwidth, and latency.
- For all desktops, a Desktop Health alert displays when one or more of the following parameters is at or above a set threshold value: CPU use %, memory use %, and disk latency.
  - Threshold values are 90% for CPU, 80% for memory use, and 100 ms for disk latency.
  - These parameters are checked every minute, and the alert is triggered when the measurement is at or above the threshold value for 10 consecutive minutes.

**Note** This report’s data is updated every minute by the data from the backend reporting system.
<table>
<thead>
<tr>
<th>Report Type</th>
<th>Details</th>
</tr>
</thead>
</table>
| Utilization      | View consumption trends for deployed capacity over a pre-defined time window in both graphical and tabular formats. If you have multiple types of pods in your deployment, there is a separate tab for each type.  
- For Horizon pods, information provided includes utilization of CPU, Memory, and Disk as well as session concurrency data at the deployment level and at the pod level.  
- For pods in Microsoft Azure, information provided includes utilization of deployed capacity as well as session concurrency. Ancillary details covering client use, protocol use, session duration distribution, access type, and service type are also provided for the sessions. For pods in Microsoft Azure, data can be filtered for the pool or farm. |
| **Note**         | - The Unique User Summary feature of this report is not provided when the Session Data setting is disabled.  
- This report is not provided when the Cloud Monitoring Service setting is disabled. Both of these settings are located in Settings > General Settings > Monitoring. See Customizable General Settings for Your Horizon Cloud Tenant Environment for more information. |
|                  | The backend reporting system sends the data for this report at a specific UTC time:  
- For the selected periods Last 24 hours or Last 1 week, the data is updated hourly. The update starts at 5 minutes past the hour UTC and takes about 15 minutes to finish.  
- For the other time periods, the data is updated daily. The update starts at 2am UTC and takes about 15 minutes to finish. |
| Azure Concurrency| View per-assignment data for capacity, number of concurrent users, peak concurrency, and applications in use. You can filter this information by time period.  
The reporting system sends the data for this report daily at a specific UTC time. The update starts at 2am UTC and takes about 15 minutes to finish. Due to that update timing, data for sessions that take place after the 2am UTC time point are not reflected in this report until the next day.                                                                                                                                                                                                                                                                                                                                 |
| **Note**         | - This report is available for pods in Microsoft Azure only.  
- This report is not provided when the Cloud Monitoring Service setting is disabled in Settings > General Settings > Monitoring. |
| URL Configurations| View information for currently configured URL redirects. For more information, see Create a URL Redirection Customization and Assign it to Users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Agent Versions   | View current versions of agents for each VM. For a pod in Microsoft Azure, this tab also displays the pod's manifest version to help you determine if the agent version must be updated or not.  
Select a pod in the Pod drop-down at the top left of the page to show information for that pod. You can also sort data on all columns, including Assignment Name. |
<table>
<thead>
<tr>
<th>Report Type</th>
<th>Details</th>
</tr>
</thead>
</table>
| Sessions                    | View session information for user sessions including User Name, Pod, Pod Type, Session Type (Desktop or Application), Last Login Time, Client IP, Client Type, Desktop Name, Pool/Farm Name, Protocol Type, Total Session Duration (including idle and disconnected time), and Session Idle Duration, across all your pools over a pre-defined time period. The reporting system sends the data for this report daily at a specific UTC time. The update starts at 2:10am UTC and takes about 15 minutes to finish. Due to that update timing, data for sessions that take place after the 2am UTC time point are not reflected in this report until the next day.  
  
  **Note**  
  - The **User Name** column does not appear in this report when the **Session Data** setting is disabled.  
  - This report is not provided when the **Cloud Monitoring Service** setting is disabled.  
  
  Both of these settings are located in **Settings > General Settings > Monitoring**. See **Customizable General Settings for Your Horizon Cloud Tenant Environment** for more information.  
  
  To export data for this report, follow the steps above under **Exporting Report Data**. |
| VDI Applications Usage      | View a list of applications that end users have used in VDI desktops and each application's total usage duration. Can be filtered by time period. This data can help you see which are the most used applications in a particular VDI desktop assignment. The reporting system sends the data for this report at a specific UTC time:  
  - For the selected period **Last 24 hours**, the data is updated hourly. The update starts at 20 minutes past the hour UTC and takes about 15 minutes to finish.  
  - For the other time periods, the data is updated daily. The update starts at 2:30am UTC and takes about 15 minutes to finish.  
  
  **Note** This report is not provided when the **Cloud Monitoring Service** setting is disabled in **Settings > General Settings > Monitoring**.  
  
  To export data for this report, follow the steps above under **Exporting Report Data**. |
| User Usage Report           | View a record of desktop applications usage by the user over the pod for a pre-defined time period. This report helps you identify the number of sessions that the user has launched and their total active usage time.  
  
  **Note** This report is not provided when either the **Cloud Monitoring Service** setting or the **Session Data** setting is disabled in **Settings > General Settings > Monitoring**.  
  
  To export data for this report, follow the steps above under **Exporting Report Data**. |

### Notifications Page

Horizon Cloud uses notifications to inform you of certain types of system activity, such as events and service registrations.
You can view recent notifications in the administrative console by clicking the bell icon located in the upper right corner of any page (🔔). Open the Notifications page to view all notifications. These notifications include both active and dismissed notifications, by clicking Monitor > Notifications.

You can also show the notifications for different periods of time up to 30 days, refresh the page, and filter your search.

**Table 8-2. Notification Types**

<table>
<thead>
<tr>
<th>Notification Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Registration</td>
<td>Service registration notifications are issued during the configuration of your environment. The system issues this type of notification when one of its packaged services is registered successfully.</td>
</tr>
<tr>
<td>Pod related</td>
<td>Pod-related notifications are issued when the system detects a change in the status of the deployed pod in Microsoft Azure. These notifications include ones for when a pod has lost connectivity with the Horizon Cloud cloud plane and when subnets are full. When subnets are full, then system operations involving cloning VMs raise notifications.</td>
</tr>
<tr>
<td>Pod API related</td>
<td>These notifications arise from conditions detected by the cloud plane’s API requests that are made to the pod resources in Microsoft Azure, such as API slow downs or timeouts.</td>
</tr>
<tr>
<td>Primary bind account locked</td>
<td>These notifications are issued when the system detects the primary domain-bind account is in a failed or inactive state. For more information, see Notifications When the Primary Domain-Bind Account is Locked Out.</td>
</tr>
<tr>
<td>Domain Bind Account used for emergency access</td>
<td>This notification is issued when the primary domain bind account or auxiliary domain bind account is used to log in to the console. As described in Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment, the primary and auxiliary domain bind accounts are always assigned the Super Administrator role, which grants all the permissions to perform management actions in the console.</td>
</tr>
</tbody>
</table>

**Working with Audit Logs**

The Audit Logs tab displays the time, status, description, and user information logged for events that have occurred from administrator-initiated actions on your pods. The amount and types of event data reported on the Audit Logs tab might vary by pod type. The Horizon Cloud control plane retains event data for one year.
Viewing Audit Logs

- To display the audit logs, do one of the following:
  - Select **Monitor > Activity**. On the Activity page, click the **Audit Logs** tab.
  - Select **Settings > Capacity**. On the Capacity page, click the name of the pod for which you want to view logs, and then click the **Audit Logs** tab.

By default, the Audit Logs tab displays the logs for every pod-related event that transpired in the past 24 hours, in descending order of time with the most recent events listed first.

- To sort the logs by ascending order of time, click the **Time** column header. To toggle back to descending order, click the header again.

- To refresh the display of audit logs with the most recently reported events, click the Refresh button.

Filtering Audit Logs

To customize the display of audit logs, you can adjust the settings for the Time Period filter. You can also apply additional filters to refine further the selection of logs that are displayed. Each filter has drop-down menus that let you define the operations and values used to narrow the selection of logs.

- To customize the Time Period filter, select an operation and time value from the drop-down menus, and click **Apply**.
To specify an additional filter, click the plus sign (+) button. Using the drop-down menus, select the filter type, operation, and value for the filter. Then click Apply.

The options available from the operation and value menus vary depending on the filter type. For example, if you select Severity for the filter type, Greater Than or Equal To for the operation, and Success for the value, the filter displays all the logs with the status "Success" or "Info."

You can also apply more than one filter of the same type. For example, you can apply a Severity filter that shows logs with status Equal To the value Success. Then you can apply an additional Severity filter that shows logs with status Equal To the value Failure.

### Downloading Audit Logs

**Note** The download feature is only available to users who have Horizon Cloud Super Administrator privileges.

To download the current, filtered list of audit logs, click the Download ( ) button.

The downloaded logs reside in a CSV file and have the following properties:

- The download file includes all the logs that fulfill the current filtering criteria, regardless of whether they are visible on the Audit Logs tab.
  
  For example, the current filter might return a total of 1000 logs spanning multiple pages of the Audit Logs tab. However, each page can only display 10 logs. The download file contains all 1000 logs from all the Audit Logs pages, not just the currently viewed page.

- The download file always lists logs in descending order of time, regardless of the sort order specified on the Audit Logs tab. The sort order only applies to the display on the Audit Logs tab.

- By default, the download file uses the name format AuditReport-<YYYY-MM-DDTHH_MIN_SEC.millisZ> (for example, “AuditEventReport-2019-08-14T11_16_32.096Z”).

### About the Assignments Menu in the Horizon Cloud Administration Console

The console’s navigation bar’s Assignments are provides access to the assignment-related workflows you can perform in your Horizon Cloud environment.

**Tip** The console is dynamic and reflects the workflows and settings that are appropriate for the up-to-the-moment situation in your Horizon Cloud tenant environment. The labels displayed for the console’s assignment-related pages will vary depending on factors such as the tenant’s configured brokering setting, the types of cloud-connected pods in your fleet, the tenant’s regional cloud plane, and features that are based on specific licensing.
When You Have Mixed Pod Types

When you have both Horizon pods and pods in Microsoft Azure, clicking Assignments displays different choices depending on your tenant’s configured brokering settings and whether your tenant is enabled for use of App Volumes.

When All of Your Pods are Horizon Pods

When all of your pods are Horizon pods, clicking Assignments displays a page from which you can initiate actions to create new desktop assignments and work with your existing assignments. For each listed assignment, you can click its name see more information about that assignment, such as which users it is assigned to and other details. For more information about desktop assignments for cloud-connected Horizon pods, see Chapter 6 Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment and its subtopics.

When All of Your Pods are In Microsoft Azure

When you have zero Horizon pods, clicking Assignments provides access to choices from which you initiate actions to create new assignments and work with your existing assignments. On the assignments-related pages, for each listed assignment, you can click its name see more information about that assignment, such as which users it is assigned to and other details. When you click on a VDI desktop assignment, in addition to seeing more information about the assignment, you can also navigate to the VDI desktop assignment's Desktops tab to see the list of virtual desktops that are in that VDI desktop assignment and optionally perform actions on those desktops.

For high-level information about managing assignments for your pod in Microsoft Azure and links to additional documentation topics, see Managing Assignments Provisioned By Horizon Cloud Pods in Microsoft Azure.

About the Inventory Menu in the Horizon Cloud Administration Console

The Horizon Cloud console's navigation bar's Inventory provides access to pages for working with assets that are in your environment's inventory, such as RDSH farms, assignable images and applications, and virtual machines (VMs) that have been imported into your environment.

Click Inventory to navigate to these pages.

Tip As described in Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud, the console dynamically reflects the current state of your tenant environment. As a result, clicking Inventory might display entries and labels that are variations of the ones described below.
### Option | Description
--- | ---
**Applications** | Opens the Applications page, where you can add applications into your inventory, edit parameters for applications in the inventory, rename applications, and remove applications from the inventory. See [Applications in Your Horizon Cloud Inventory](#).

**Farms** | Opens the Farms page. See [Farms in Horizon Cloud](#).

At a page level, you can:
- View the RDSH farms available in your environment.
- Create an RDSH farm.
- Edit an existing farm.
- Move a farm online or offline.
- Delete a farm.

When you click the name of a specific farm, you open its details page. From a farm's details page, you can perform actions on that specific farm:
- Edit various settings, such as the farm's name and its size.
- Power off and delete the farm's VMs.
- Work with sessions currently connected to the farm's VMs.
- Examine activity that has taken place in the farm.

**Images-related pages** | These pages provide access to image-related workflows.

- When your environment has cloud-connected VMware Horizon pods, an entry [Images (VMware)](#) provides access to image-related workflows involving those pods. For details about those features, see the [Actions You Can Perform on Published Images from Horizon Cloud Pods in Microsoft Azure](#) documentation topics.

- For pods deployed in Microsoft Azure, an entry [Images](#) or [Images (Microsoft Azure)](#) provides access to image-related workflows involving those pods. These workflows are described in:
  - [Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure](#)
  - [Actions You Can Perform on Published Images from Horizon Cloud Pods in Microsoft Azure](#)
  - [Managing Published Images for Horizon Cloud Pods in Microsoft Azure](#)

On this page, you can also:
- Download the DaaS bootstrap file. If needed based on the manifest version of your pod, you typically use the [Download Bootstrap](#) button to download an encrypted bootstrap file to deploy to your images. When you select this option, you are prompted to enter a password of 8-20 ASCII characters containing at least one each of the following: lowercase letter, uppercase letter, number, and symbol (‘!@#$%^&*’). Do not use non-ASCII characters in the password.

- Refresh the DaaS bootstrap password. Use the [Refresh Password](#) button to refresh a previously set DaaS bootstrap password.

  **Note** If you refresh the password after having downloaded a bootstrap file but before applying the bootstrap file using the keytool utility, then the resultant agents will not be able to pair. Therefore, it is recommended that you download the bootstrap file again after refreshing the password.

**Imported VMs** | Opens the Imported VMs page. The virtual machines (VMs) displayed on this page include:
- The VMs that you created and imported using the [Import](#) action button.
- VMs that the system imported from the pods' `podID-base-vms` resource groups.

See [Imported VMs Page](#) for details.
**Imported VMs Page**

The administrative console's Imported VMs page lists the virtual machines (VMs) that have been brought into your Horizon Cloud environment.

You can perform the following actions on a listed VM by selecting the check box next to the VM and clicking the respective action. Some of the actions are under the More option.

**Note**

- If the process to import an image from the Microsoft Azure Marketplace fails, the system generates a notification about the failure and displays a Failed link in the Agent Status column. Clicking that link opens the Notification page where you can read the reason for the failure.

- The Imported VMs page does not automatically refresh itself. After you perform an action, you might have to click the refresh action to see the current status. As an example, when a VM is powered off and you choose the Power On action, the page displays **In progress** as the power-on process starts, and continues to show that status until you refresh the page.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM power and guest operating system actions</td>
<td>For a VM in Microsoft Azure, the available actions are Power On, Power Off, and Restart.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the selected VM.</td>
</tr>
<tr>
<td>Convert to Image</td>
<td>Convert the selected VM to an image that Horizon Cloud can use for farms or VDI desktop assignments. See Convert a Configured Image VM to an Assignable Image in Horizon Cloud. Note Make sure the VM has all of the applications and drivers you want installed on it before converting it.</td>
</tr>
<tr>
<td>Reset Agent Pairing</td>
<td>Updates the agent state that governs the pairing of the VM with Horizon Cloud. You typically use this action in the following scenarios:</td>
</tr>
<tr>
<td></td>
<td>For a VM recently imported using the Create a Base Virtual Machine Automatically from the Microsoft Azure Marketplace and Pair it with Horizon Cloud: in this scenario, this action restarts the agent software that the workflow installed in the VM, which completes the pairing of the imported VM with the cloud plane. For a VM that you manually created and installed the agent software in it, using the Manually Build and Import a Virtual Machine from Microsoft Azure into Horizon Cloud: in this scenario, this action restarts the agent software that the workflow installed in the VM, which completes the pairing of the imported VM with the cloud plane. For a listed VM that shows an error message in its Agent Status column: in this scenario, this action restarts the agent software to repair the pairing failure and pair the VM with the cloud plane.</td>
</tr>
</tbody>
</table>

**About the Settings Menu in the Horizon Cloud Administration Console**

The Horizon Cloud console’s navigation bar’s Settings provides access to pages for working with various aspects of your Horizon Cloud environment, such as environment-wide settings, identity
management, role-based access (RBAC) settings for the console, your deployed pods, and various related settings and configurations.

Click **Settings** to access these pages in the console.

**Remember** As described in *Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud*, the console dynamically reflects the current state of your tenant environment. As a result, clicking Settings might display entries and labels that are variations of the ones described below. Usually, but not always, the console hides a page from view if that page is not applicable to the up-to-the-moment situation in your tenant environment.

<table>
<thead>
<tr>
<th>User Interface Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td>Displays settings that apply environment-wide for this particular Horizon Cloud tenant environment, such as those My VMware users who can log in to the environment, their roles, and other comparable settings, including the toggle to enable or disable monitoring user session information. You can edit settings from this page. See <a href="#">Customizable General Settings for Your Horizon Cloud Tenant Environment</a> for details.</td>
</tr>
<tr>
<td><strong>Active Directory</strong></td>
<td>View and edit Active Directory (AD) details and configure the True SSO capabilities for your environment. True SSO provides the capabilities for your end users to connect to their desktops and RDS-based remote applications without having to enter AD credentials. See <a href="#">Complete Configuring True SSO for your Horizon Cloud Environment</a>.</td>
</tr>
<tr>
<td><strong>Roles &amp; Permissions</strong></td>
<td>Edit roles and permissions. See <a href="#">Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment</a>.</td>
</tr>
<tr>
<td><strong>Capacity</strong></td>
<td>View details about your deployed pods, such as each pod's utilization and capacity usage, and drill down to view and optionally update some of the editable properties associated with a pod, such as its specified NTP server, its associated Microsoft Azure subscription's application key, and so on. For details, see <a href="#">Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types</a>.</td>
</tr>
</tbody>
</table>
| **Identity Management** | Configure integration of your Horizon Cloud environment with your VMware Workspace ONE® Access™ environment.  

**Note** The console hides this page from view when:  
- You have deployed your first pod in a brand new, clean-slate tenant environment and have not yet selected the brokering method for your pods to use to broker end-user connections to their pod-provisioned entitled resources.  
- Your tenant environment is configured to use Universal Broker as the brokering method. |
| **Licenses** | View details of current licenses for your environment, including numbers of seats and billing cycles. You can also click the SID for a license to open the MyVMware subscription list page (you must log in using your MyVMware credentials). |
| **VM Types & Sizes** | Manage the types and sizes of VMs to be used in farms and assignments for pods in Microsoft Azure. For details, see [Managing VM Types and Sizes for Farms and Assignments](#). |
| **Getting Started** | Display the Getting Started wizard. See [About the Horizon Cloud Getting Started Wizard](#) for details. |
| **Broker** | Configure settings that apply to the system's brokering of pod-provisioned resources to your end users, such as settings that control timeouts for end-user sessions. |
Customizable General Settings for Your Horizon Cloud Tenant Environment

Use the Horizon Cloud Administration Console's General Settings page to modify settings that apply to your overall Horizon Cloud tenant environment.

As described in Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud, the console dynamically reflects the current state of your tenant environment. As a result, the sections you see and settings you can change in the General Settings page are only those that are relevant and appropriate for the current state of your tenant environment. For example, when your cloud-connected pods are all Horizon pods and no pods in Microsoft Azure, only the settings relevant to Horizon pods are provided in this page. When you have at least one pod deployed in Microsoft Azure, the General Settings page makes available settings relevant to that pod type.

To change a setting, use the pencil icon next to the section that contains the setting that you want to change. An edit window displays with that section's settings. Change the settings in that window and save your changes to the system.

Note When changing any of the following settings, it can take up to 5 minutes for the update to take effect.

- The Enable Dedicated Desktop Assignment Name setting in the Desktop Assignment Options section.
- The settings in the Domain Security Settings section, listed in Domain Security Settings on General Settings Page.
- Default Domain
- My VMware Accounts
- Session Timeout
- Deletion Protection
- RDSH Farm
- Desktop Assignment Options
- Image Management Settings
- Domain Security Settings
- Monitoring
- Contact Information
Default Domain

If you have only one Active Directory domain registered with your environment, the name of that domain appears here. If you have multiple Active Directory domains registered, this text box displays the name of that Active Directory domain that is specified as the default Active Directory domain, the one that appears first in the domain selection list in the Active Directory login page used when administrators log in to the administrative console.

This setting only governs which Active Directory domain appears first in the domain selection list on that Active Directory login page. As described in Log In to the Horizon Cloud Administration Console to Perform Management Tasks on Your Horizon Cloud Environment, when your environment has multiple Active Directory domains registered, the Active Directory login page has a domain selection list. You can use this Default Domain text box to specify one of the Active Directory domains as the default. That default Active Directory domain then appears first in the Active Directory login page's domain selection list. Click Edit to change the current setting.

My VMware Accounts

To give users the ability to log into Horizon Cloud, you add their My VMware accounts. After adding their My VMware information here, then assign their Active Directory user accounts the role that is appropriate for their job or business tasks. See Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment.

Session Timeout

These settings govern timeouts of connections to your Horizon Cloud environment:

- The Admin Portal Timeout setting governs the amount time an administrator can be continuously logged in to the console. When that time has elapsed, the administrator's authenticated session ends and the administrator must log back in.

Deletion Protection

The Deletion Protection setting controls the number of desktop VMs that can be deleted per hour in each of your dedicated desktop assignments. Select one of the following options for Mass Delete Dedicated Desktop (per hour).

- Unlimited - Unlimited desktop VMs can be deleted from dedicated desktop assignments.
- None - No desktop VMs can be deleted from any dedicated desktop assignment unless you allow them for a particular assignment using the Max Desktop Deletions (see note below).
- **Custom** - Number of desktop VMs that can be deleted from a dedicated desktop assignment per hour. If you select **Custom**, you must also enter a numerical value to the right of this drop-down menu. You can allow additional desktop VMs to be deleted from a particular assignment using the **Max Desktop Deletions** (see note below).

**Note**  If you selected **None** or **Custom**, you can allow additional deletions for a particular assignment before this limit is invoked by editing the **Max Desktop Deletions** setting when you create or edit the assignment. If you have entered a value greater than 0 for the **Max Desktop Deletions**, then the system authorizes deletions of that number of VMs before counting them against the rate you set for **Deletion Protection**.

For example, you might set **Max Desktop Deletions** to **Custom** with a value of 10 and set **Deletion Protection** to **Custom** with a value of 1. In this case, after the first 10 VMs are deleted (no matter how long it takes for the count to reach 10), the system only allows 1 additional VM to be deleted per hour from that time forward.

If you select **Unlimited** for **Deletion Protection**, there is no need to use the **Max Desktop Deletions** setting.

For more information about the **Max Desktop Deletions** setting, see Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure.

To prevent all VM deletions in a dedicated desktop assignment, use the **Prevent Deletions** setting on the **Assignments** page. See Prevent Deletions or Allow Deletions for a Dedicated Desktop Assignment.

**RDSH Farm**

You can provide a message that Horizon Cloud displays to end users when their logged-in Windows session with their session desktop or remote application has reached the farm's configured maximum session time. The system will forcibly log out the user from their logged-in Windows session after the grace period time expires.

In the **Grace Period** text box, you can provide a time for which the system waits before forcibly logging out the user, after the reminder message has been sent.

**Desktop Assignment Options**

Use this setting to configure the displayed virtual desktops' names seen by your end users when they access their assigned virtual desktops using their end-user clients. This setting applies only to virtual desktops provisioned by a dedicated VDI desktop assignment provisioned from pods in Microsoft Azure. For information about desktop assignments in Horizon Cloud, see About Desktop Assignments for Your Horizon Cloud Environment's Pods in Microsoft Azure.

Initially, when an end user logs in to their end-user client and sees a desktop newly provisioned from a dedicated VDI desktop assignment, the client displays the name of the dedicated VDI desktop assignment. At this point in time, a specific desktop virtual machine (VM) is not yet assigned to that end user as their dedicated desktop VM. When that end user takes the step to
launch the virtual desktop for the first time, at that point, the system dedicates that specific desktop VM to that user as a result of that initial launch. Then for subsequent desktop launches, the name for that desktop that appears in that end user's client depends on the setting you choose here.

**Important**

- Enabling the **Enable Dedicated Desktop Assignment Name** setting applies to pods at pod manifest version 1900 and later. When the pod is at a manifest version lower than 1900, the legacy behavior stays in effect for virtual desktops provisioned from that pod, regardless of the toggle setting.

- When you change the setting, it can take up to 5 minutes for the update to take effect.

- This option does not apply to end-user connections using Workspace ONE Access. When an end user uses Workspace ONE Access to access a desktop entitled to them from a dedicated VDI desktop assignment, Workspace ONE Access displays the assignment name and the user's Horizon Client and HTML Access portal displays the VM name for subsequent desktop launches.

- When the toggle **Enable Dedicated Desktop Assignment Name** is disabled, the end-users clients display the name of the virtual desktop's underlying VM. Displaying the VM name is the legacy behavior.

- When the toggle **Enable Dedicated Desktop Assignment Name** is enabled, the end-user clients continue to display the name of the dedicated VDI desktop assignment that provisions the virtual desktop, even for subsequent desktop launches.

**Image Management Settings**

These settings are displayed when your tenant includes at least one Horizon pod. These settings apply to the Image Management Service features used with those pods. Use these settings to optimize the image replication process. For information about the Image Management Service, see [Managing Horizon Images from the Cloud](#).
Domain Security Settings

Use these settings to prevent the communication of Active Directory domain names to unauthenticated users using the various Horizon clients to connect to the pods in Microsoft Azure. These settings govern whether the Active Directory domain information is sent to the client and, if sent, how it is displayed in the end-user clients' login pages. For details, see Domain Security Settings on General Settings Page.

Important

- These settings are applied to all of your environment's pods that are deployed in Microsoft Azure, the ones that are under the same Horizon Cloud customer account (tenant).

- The combination of options selected here changes the user experience in the clients. Certain combinations can set requirements for how end users enter the domain information on the client login page, especially when using older clients, command-line clients, and when your environment has multiple Active Directory domains. How these settings affect the client user experience depends on the client. You might need to balance your desired end-user experience according to your organization's security policies. For more information, see Domain Security Settings on General Settings Page.

- The General Settings page does not display this Domain Security Settings section when your Horizon Cloud environment has any pods in Microsoft Azure that are not yet updated to pod manifest version 1273 or later. To get access to these controls, update all your pods in Microsoft Azure to this release.

- Until all your pods are updated to pod manifest version 1273 or later, your environment is configured by default to provide the same behavior as it was in the previous Horizon Cloud release. Until all your pods are at this release level, the system sends the Active Directory domain names to the end-user clients and the clients have the legacy behavior that displays the Active Directory domain drop-down menu.

Then when all your pods' manifests are at version 1273 or later, these settings are displayed in the General Settings page. At that point, the displayed settings reflect the legacy behavior (both controls set to No), and you can change them to control the communication of domain information to the clients.

To see your pods' current manifest versions, use the Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types. For this release's pod manifest version, see the Release Notes page linked from the Horizon Cloud Documentation page.

Monitoring

The Horizon Cloud Cloud Monitoring Service (CMS) collects and stores session, application, and desktop data from connected pods for monitoring and reporting purposes. The CMS is one of the central services provided in Horizon Cloud. For an introduction to the CMS, see Chapter 3 Introducing the Cloud Monitoring Service's Unified Visibility, Health Monitoring, and Help Desk.
Features Provided in Horizon Cloud. The information collected by the CMS is used in charts on the Dashboard page and reports on the Reports page. See Health Visibility and Insights into Your Cloud-Connected Pods Provided by the Cloud Monitoring Service in Horizon Cloud and Reports Page.

- Use the Cloud Monitoring Service toggle to enable or disable the Horizon Cloud cloud monitoring service. It is enabled by default.

  When this setting is disabled, the Session Data setting below does not appear.

- When the cloud monitoring service is enabled, you can use the Session Data toggle to opt in or opt out of tracking user information related to your end users' sessions. Information collected includes times they logged in, session durations, and average session length per user.

  When you opt in to the collection of user data, Horizon Cloud collects this information and maintains it for the duration of your use of Horizon Cloud. You can delete the collected data by turning off the Session Data toggle.

  When you opt out of the collection of user data but leave the CMS enabled, Horizon Cloud collects session data for a limited period and hashes the user name to allow real-time administration while disabling historical and aggregated viewing of information. As a result, some reports, such as the User Usage report, are not available. In this case the system also continues to collect other data related to applications and desktops in connected pods.

Contact Information
Administrator contact information.

Domain Security Settings on General Settings Page
You use these settings to prevent communication of Active Directory domain names to unauthenticated users using the various Horizon clients. These settings govern whether the information about the Active Directory domains that are registered with your Horizon Cloud environment is sent to the Horizon end-user clients and, if sent, how it is displayed in end-user clients' login screens.

Configuring your environment includes registering your environment with your Active Directory domains. When your end users use a Horizon client to access their entitled desktops and remote applications, those domains are associated with their entitled access. Prior to the March 2019 quarterly service release, the system and clients had default behavior with no options to adjust that default behavior. Starting in March 2019, the defaults are changed, and you can optionally use the new Domain Security Settings controls to change from the defaults.

Important When changing these settings, it can take up to 5 minutes for the update to take effect.

This topic has the following sections.

- Domain Security Settings
Domain Security Settings

Combinations of these settings determine whether domain information is sent to the client and whether a domain selection menu is available to the end user in the client.

**Important** These settings apply to all of your pods in Microsoft Azure that are within the same Horizon Cloud environment. All pods that are deployed in Microsoft Azure using the same Horizon Cloud customer account (tenant) get the same combination. All of the end users connecting to your pods will receive the behavior according to these settings, regardless of which pod is provisioning their virtual desktops and remote applications.

**Caution** These settings change the user experience in the clients. The behavior for end users using versions of Horizon Client prior to version 5.0 is different than for Horizon Client 5.0 and later. Certain combinations can set requirements on how your end users specify their domain information in the client login screen, especially when using older clients, command-line clients, and when your environment is configured with multiple Active Directory domains. How these settings affect the client user experience depends on the client. You might need to balance your desired end-user experience according to your organization's security policies. See sections Single Active Directory Domain Scenarios and User Login Requirements and Multiple Active Directory Domain Scenarios and User Login Requirements.
Table 8-3. Domain Security Settings on the General Settings Page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show Default Domain Only</strong></td>
<td>This option controls what domain information the system sends to connecting clients prior to user authentication.</td>
</tr>
<tr>
<td></td>
<td>- Yes - The system sends only the literal string value <em>DefaultDomain</em>.</td>
</tr>
<tr>
<td></td>
<td>- No - The system sends the list of registered Active Directory domain names to the client.</td>
</tr>
</tbody>
</table>

| **Hide Domain Field**      | This option controls the visibility in the client login screen of whatever domain-related information is sent to the client, based on the Show Default Domain Only setting. |
|                            | - Yes - Nothing about domains is displayed in the client login screen, regardless of what Show Default Domain Only is set to. Neither the literal string value *DefaultDomain* nor the domain names are displayed in the client login screen. |
|                            | - No - The client login screen displays one of the following items, depending on the Show Default Domain Only setting.                  |
|                            |   - The literal text *DefaultDomain*, when Show Default Domain Only is Yes. This combination is optimized for user experience in Horizon Clients older than version 5.0, while also providing improved security. |
|                            |   - The list of domain names in a drop-down menu, when Show Default Domain Only is No.                                                 |

This Release’s Default Behavior Compared with Past Releases

The following table details the previous default behavior, the new default behavior, and the settings you can use to adjust the behavior to meet your organization's needs.

<table>
<thead>
<tr>
<th>Previous Release Default Behavior</th>
<th>This Release Default Behavior</th>
<th>Corresponding Domain Security Settings Combination for this Release's Default Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>The system sent the names of the registered Active Directory domains to the clients.</td>
<td>The system sends only a literal string value (<em>DefaultDomain</em>) to the clients and not the names of the registered Active Directory domains.</td>
<td><strong>Show Default Domain Only</strong>  Default setting: <strong>Yes</strong></td>
</tr>
<tr>
<td><strong>Note</strong> Sending the literal string provides support for older Horizon clients which are implemented to expect a string list of domain names.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The clients displayed a drop-down menu in the login screen that presents the list of registered Active Directory domain names for the end user to choose their domain prior to logging in.</td>
<td>The clients display that literal string <em>DefaultDomain</em>.</td>
<td><strong>Hide Domain Field</strong>  Default setting: <strong>No</strong></td>
</tr>
</tbody>
</table>
Relationship to Your Pods' Manifest Levels

When you are an existing customer with pods created in an earlier service release, until all of your pods in Microsoft Azure are updated to the manifest level for this Horizon Cloud release, your environment is configured by default to provide the same behavior as it had in the previous Horizon Cloud release. That legacy behavior is:

- The system sends the Active Directory domain names to the client (Show Default Domain Only is set to No).
- The clients have a drop-down menu that displays the list of domain names to the end user prior to logging in (Hide Domain Field is set to No).

Also, until all of your pods are at this service release level, the General Settings page does not display the Domain Security Settings controls. If you have a mixed environment with existing non-updated pods and newly deployed pods at this release level, the new controls are not available. As a result, you cannot change from the legacy behavior until all of your pods are at this service release level.

When all of your environment's pods are updated, the settings are available in the Horizon Cloud administrative console. The post-update defaults are set to the pre-update behavior (Show Default Domain Only is No and Hide Domain Field is No). The post-update default settings are different than the new-customer defaults. These settings are applied so that the pre-update legacy behavior continues for your end users after the update, until you choose to change the settings to meet your organization's security needs.

Single Active Directory Domain Scenarios and User Login Requirements

The following table describes the behavior for various setting combinations when your environment has a single Active Directory domain, without two-factor authentication, and your end users use the Horizon Clients 5.0 and later versions.
Table 8-4. Behavior For Horizon Clients 5.0 and Later Versions and You Have One Active Directory Domain

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Horizon Client 5.0 Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>The client’s login screen has the standard user name and password fields. No domain field is displayed. No domain name is sent. The following screenshot is an example for how the resulting login screen looks like for the Windows client.</td>
<td>When there is a single domain, to log in, end users can enter either of the following values in the User name text box. The domain name is not required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• username</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• domain\username</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Using the command-line client launch and specifying the domain in the command works.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>The client’s login screen has the standard user name and password fields. The domain field displays <em>DefaultDomain</em>. No domain name is sent. The following screenshot is an example for how the resulting login screen looks like for the Windows client.</td>
<td>When there is a single domain, to log in, end users can enter either of the following values in the User name text box. The domain name is not required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• username</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• domain\username</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Using the command-line client launch and specifying the domain in the command works.</td>
</tr>
</tbody>
</table>
Table 8-4. Behavior For Horizon Clients 5.0 and Later Versions and You Have One Active Directory Domain (continued)

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Horizon Client 5.0 Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
</table>
| No | Yes | The client's login screen has the standard user name and password fields. No domain field is displayed. The system sends the domain name to the client.  
**Note**: This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain name.  
The login screen looks the same as the one in the first row of this table, with no domain field displayed. | An end user must include the domain name in the **User name** text box.  
- domain\username |
| No | No | The client's login screen has the standard user name and password fields and a standard drop-down domain selector displays the one available domain name. The domain name is sent. | The end user can specify their user name in the **User name** text box and use the single domain that is in the list visible in the client.  
Using the command-line client launch and specifying the domain in the command works. |

This table describes the behavior when your environment has a single Active Directory domain and your end users use previous versions of the Horizon clients (pre-5.0).

**Important** Using the command-line client launch of older (pre-5.0) clients and specifying the domain in the command fails for all of the combinations below. To work around this behavior, either use *DefaultDomain* for the command's domain option or update the client to the 5.0 version. However, when you have more than one Active Directory domain, passing *DefaultDomain* does not work.
## Table 8-5. Behavior For Older Horizon Clients (Before 5.0) and You Have One Active Directory Domain

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Pre-5.0 Horizon Client Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
</table>
| Yes                                                      | Yes               | The client's login screen has the standard user name and password fields. No domain field is displayed. No domain name is sent. | An end user must include the domain name in the **User name** text box.  
  - domain\username |
| Yes                                                      | No                | The client's login screen has the standard user name and password fields. The domain field displays *DefaultDomain*. No domain name is sent. | An end user must enter **username** in the **User name** text box. When the domain name is included, an error message displays that states the specified domain name does not exist in the domain list. |
| No                                                       | Yes               | The client's login screen has the standard user name and password fields. No domain field is displayed. The system sends the domain name to the client.  
  **Note** This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain name.  
  The login screen looks the same as the one in the first row of this table, with no domain field displayed. | An end user must include the domain name in the **User name** text box.  
  - domain\username |
| No                                                       | No                | The client's login screen has the standard user name and password fields and a standard drop-down domain selector displays the one available domain name. The domain name is sent. | The end user can specify their user name in the **User name** text box and use the single domain that is in the list visible in the client. |

## Multiple Active Directory Domain Scenarios and User Login Requirements

This table describes the behavior for various setting combinations when your environment has multiple Active Directory domains, without two-factor authentication, and your end users use the Horizon Clients 5.0 and later versions.

Basically, the end user has to include the domain name when they type in their user name, like domain\username, except for the legacy combination where the domain names are sent and are visible in the client.
Table 8-6. Behavior For Horizon Clients 5.0 and Later Versions and You Have Multiple Active Directory Domains

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Horizon Client 5.0 Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>The client's login screen has the standard user name and password fields. No domain field is displayed. No domain names are sent. The following screenshot is an example for how the resulting login screen looks like for the Windows client.</td>
<td>An end user must include the domain name in the User name text box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Login Screen Screenshot" /></td>
<td><img src="image" alt="Login Screenshot" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Server:</strong></td>
<td><strong>Server:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Login Screen Screenshot" /></td>
<td><img src="image" alt="Login Screenshot" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>User name:</strong></td>
<td><strong>User name:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Login Screen Screenshot" /></td>
<td><img src="image" alt="Login Screenshot" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Password:</strong></td>
<td><strong>Password:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Login Screen Screenshot" /></td>
<td><img src="image" alt="Login Screenshot" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Domain:</strong> <em>DefaultDomain</em></td>
<td><strong>Domain:</strong> <em>DefaultDomain</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Login Screen Screenshot" /></td>
<td><img src="image" alt="Login Screenshot" /></td>
</tr>
</tbody>
</table>

An end user must include the domain name in the **User name** text box.
- `domain\username`

Using the command-line client launch and specifying the domain in the command works.

| Yes                                                      | No                | The client's login screen has the standard user name and password fields. The domain field displays *DefaultDomain*. No domain names are sent. The following screenshot is an example for how the resulting login screen looks like for the Windows client. | An end user must include the domain name in the **User name** text box. |
|                                                         |                   | ![Login Screen Screenshot](image)       | ![Login Screenshot](image) |
|                                                         |                   | **Server:**                             | **Server:**       |
|                                                         |                   | ![Login Screen Screenshot](image)       | ![Login Screenshot](image) |
|                                                         |                   | **User name:**                          | **User name:**    |
|                                                         |                   | ![Login Screen Screenshot](image)       | ![Login Screenshot](image) |
|                                                         |                   | **Password:**                           | **Password:**     |
|                                                         |                   | ![Login Screen Screenshot](image)       | ![Login Screenshot](image) |
|                                                         |                   | **Domain:** *DefaultDomain*             | **Domain:** *DefaultDomain* |
|                                                         |                   | ![Login Screen Screenshot](image)       | ![Login Screenshot](image) |

An end user must include the domain name in the **User name** text box.
- `domain\username`

Using the command-line client launch and specifying the domain in the command works.
Table 8-6. Behavior For Horizon Clients 5.0 and Later Versions and You Have Multiple Active Directory Domains (continued)

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Horizon Client 5.0 Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>The client's login screen has the standard user name and password fields. No domain field is displayed. The system sends the domain names to the client.</td>
<td>An end user must include the domain name in the User name text box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain names.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The login screen looks the same as the one in the first row of this table, with no domain field displayed.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>The client's login screen has the standard user name and password fields and a standard drop-down domain selector displays the list of domain names. The domain names are sent.</td>
<td>The end user can specify their user name in the User name text box and select their domain from the list visible in the client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using the command-line client launch and specifying the domain in the command works.</td>
<td></td>
</tr>
</tbody>
</table>

This table describes the behavior when your environment has multiple Active Directory domains and your end users use previous versions of the Horizon clients (pre-5.0).

**Important**

- Setting **Hide Domain Field** to **Yes** allows end users to enter their domain in the **User name** text box in these pre-5.0 Horizon clients. When you have multiple domains and you want to support use of pre-5.0 Horizon clients by your end users, you must set **Hide Domain Field** to **Yes** so that your end users can include the domain name when they type in their user name.

- Using the command-line client launch of older (pre-5.0) clients and specifying the domain in the command fails for all of the combinations below. The only work around when you have multiple Active Directory domains and want to use command-line client launch is to update the client to the 5.0 version.
Table 8-7. Behavior For Older Horizon Clients (Before 5.0) and You Have Multiple Active Directory Domains

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Pre-5.0 Horizon Client Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
</table>
| Yes                                                     | Yes               | The client's login screen has the standard user name and password fields. No domain field is displayed. No domain name is sent. | An end user must include the domain name in the User name text box.  
- domain\username |
| Yes                                                     | No                | The client's login screen has the standard user name and password fields. The domain field displays *DefaultDomain*. No domain name is sent. | This combination is unsupported for environments with multiple Active Directory domains. |
| No                                                      | Yes               | The client's login screen has the standard user name and password fields. No domain field is displayed. The system sends the domain name to the client.  
**Note** This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain names. | An end user must include the domain name in the User name text box.  
- domain\username |
| No                                                      | No                | The client's login screen has the standard user name and password fields and a standard drop-down domain selector displays the one available domain name. The domain name is sent. | The end user can specify their user name in the User name text box and select their domain from the list visible in the client. |

About Pods in Microsoft Azure with Unified Access Gateway Instances Configured with Two-Factor Authentication

As described in Specify Two-Factor Authentication Capability for the Pod, when you deploy a pod into Microsoft Azure, you have the option of deploying it with RADIUS two-factor authentication configured on its Unified Access Gateway instances.

When a pod in Microsoft Azure has its Unified Access Gateway configured with RADIUS two-factor authentication, end users attempting to authenticate with their Horizon clients first see a screen asking for their two-factor authentication credentials, followed by a login screen asking for their Active Directory domain credentials. In this case, the system sends the domain list to the clients only after the end user's credentials successfully pass that initial authentication screen.

Generally speaking, if all of your pods have RADIUS two-factor authentication configured on their Unified Access Gateway instances, you might consider having the system send the domain list to the clients and have the clients display the domain drop-down menu. That configuration provides the same legacy end-user experience for all of your end users, regardless of which Horizon client
version they are using or how many Active Directory domains you have. After the end user successfully completes the two-factor authentication passcode step, they can then select their domain from the drop-down menu in the second login screen. They can avoid having to include their domain name when they enter their credentials into the initial authentication screen.

However, because the Domain Security Settings are applied at the Horizon Cloud customer account (tenant) level, if some of your pods do not have two-factor authentication configured, you might want to avoid sending the domain list, because those pods will send the domain names to the clients connecting to them prior to the end users logging in.

**Important** When a pod’s two-factor authentication configuration has Maintain Username configured as Yes, ensure that the Hide Domain Field is set to No. Otherwise, your end users will not be able to provide the required domain information for the system to associate with their login credentials.

The end-user login requirements by Horizon client follow the same patterns that are described in Single Active Directory Domain Scenarios and User Login Requirements and Multiple Active Directory Domain Scenarios and User Login Requirements. When connecting to a pod that has RADIUS two-factor authentication configured and you have multiple Active Directory domains, the end user must provide their domain name as domain\username if Hide Domain Field is set to Yes.

**File Share Page**

The File Share page provides details about any file shares that have been registered with your Horizon Cloud environment.

**Note** Because the Horizon Cloud Administration Console is dynamic and responsive to the current state of your Horizon Cloud environment, typically this page will not be visible when your environment only has pods deployed in Microsoft Azure. Currently, registering file shares for use with pods deployed in Microsoft Azure is not supported. As a result, no information is provide on this page for such pods.

**Licenses Page**

The Licenses page provides information about your products licensed under the Horizon Universal License.

Information displayed for each license is described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SID</td>
<td>Service Instance ID. This value is a unique identifier generated for each subscription. You can also click the SID for a license to open the MyVMware subscription list page (you must log in using your MyVMware credentials).</td>
</tr>
<tr>
<td>Total Seats</td>
<td>Number of seats included in the license.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Billing      | Type of billing and total length of license. Billing types are:  
  - Paid - There was one bill at the start of the license.  
  - Monthly - There is one bill for each month of the license.  
  - Trial - There is no bill because it is a trial license. |
| Type         | Type of license. License types are:  
  - Named - Seat count shown is for named users. For named users, the system counts the number of unique users that have accessed the Horizon environment. If a named user runs multiple single-user desktops, published desktops, or published applications, the user is still counted once.  
  - Concurrent - Seat count shown is for concurrent users. For concurrent users, the system counts single-user desktop connections per session. If a concurrent user runs multiple single-user desktops, each connected desktop session is counted separately. |
| Classification | License classifications are:  
  - Horizon Apps Service Universal  
  - Horizon Service Universal  
  - Workspace ONE Apps Service Universal  
  - Workspace ONE Service Universal |
| Start Date   | Date that the license became active.                                                                                                          |

### Identity Management Page in the Horizon Cloud Administration Console

If your Horizon Cloud environment's configuration supports using Workspace ONE Access with your pods in Microsoft Azure, you can use the Identity Management page to add, edit, and configure the required identity management provider information. If you do not already have a Workspace ONE Access cloud tenant associated with your Horizon Cloud tenant, you can initiate setting up a Workspace ONE Access cloud tenant from this page.

As described in Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud, the console dynamically reflects the current configuration and state of your tenant environment. The console makes the Identity Management page available when your tenant environment is configured to use single-pod brokering for your pods in Microsoft Azure. When your environment is configured to use the Universal Broker, this page is not available for your use. To see the brokering type that is configured for your environment, navigate to the console's Broker page (Settings > Broker).
Workspace ONE Access Environment

This section is visible when your pods in Microsoft Azure are using the single-pod type of brokering. If those pods are using single-pod type of brokering and your Horizon Cloud tenant is already associated with a Workspace ONE Access cloud tenant, the name of that tenant is displayed here. If you do not already have a Workspace ONE Access cloud tenant and you want to initiate creating one, you can use the SET UP button to initiate creating one for use with this Horizon Cloud tenant. After clicking SET UP, provide the values in the displayed window and submit them to the system.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Region</td>
<td>Select the Workspace ONE Access region for the new tenant.</td>
</tr>
<tr>
<td>Tenant Name</td>
<td>Type a name for the tenant.</td>
</tr>
<tr>
<td>Username</td>
<td>Type a name to use for the admin account of the Workspace ONE Access tenant.</td>
</tr>
<tr>
<td>Email</td>
<td>Type the email address to use for the admin account in Username. The welcome email is sent to that email address when the system has created the Workspace ONE Access tenant.</td>
</tr>
</tbody>
</table>

**Note**  After you receive the email notification that your Workspace ONE Access cloud tenant is created, additional steps are required for integrating the new Workspace ONE Access tenant with your pod. For those subsequent steps, see Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access.

**Configured Providers List**

The Identity Management page displays the currently configured providers, including the following information for each.

- Status - Current status of the listed configuration. Hover on the icon to see the current status.
- Workspace ONE Access URL - The metadata URL of the identity management provider.
- Workspace ONE Redirection - Indicates whether automatic redirection to Workspace ONE Access is configured for the listed configuration. You can only enable redirection for one identity provider per tenant. This feature is primarily used with the feature to force end-user access to their desktops and applications through Workspace ONE Access. See Configure the Option to Force End-User Access to Use Workspace ONE Access.
- Timeout SSO Token - Timeout value in minutes.
- Data Center - For a pod deployed in Microsoft Azure, the displayed value corresponds to the pod’s software version for the specific pod that is configured with this particular provider. This number is the same as the pod’s version number that is listed in the pod’s details page. See the description of the pod’s details page in Chapter 4 Managing Your Cloud-Connected Pods, for All Horizon Cloud Supported Pod Types.
- Client Access FQDN - The FQDN that you tell your end users to make their connections to, for connecting to Horizon Cloud.
- Location - The pod’s location.
Pod - The pod for which this configuration applies.

Create an Identity Management Provider Configuration

Configuring a new identity provider for one of your pods in Microsoft Azure is a multi-step process. See the information in Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access and follow the steps in Configure a Horizon Cloud Pod in Microsoft Azure for Workspace ONE Access.

Edit Settings for a Configuration

To edit the information for a configuration on this page:

1 Select the listed configuration.
2 Click **Edit**.
3 Edit the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout SSO</td>
<td>Timeout value in minutes.</td>
</tr>
<tr>
<td>Token</td>
<td></td>
</tr>
<tr>
<td>Client Access</td>
<td>For a pod in Microsoft Azure, you enter here the FQDN that you tell your end users to make their connections to, for connecting to Horizon Cloud.</td>
</tr>
<tr>
<td>FQDN</td>
<td></td>
</tr>
<tr>
<td>Workspace ONE</td>
<td>When editing the configuration, you can change the current setting of this toggle.</td>
</tr>
<tr>
<td>Redirection</td>
<td>When you also have the configuration to force end-user access to go through Workspace ONE Access, you can set this toggle to <strong>YES</strong> to have the end users' clients automatically redirect to their Workspace ONE Access environment. Read about the options to force end-user access to go through Workspace ONE Access in Configure the Option to Force End-User Access to Use Workspace ONE Access. With the automatic redirection configured to <strong>YES</strong>, in the end-user clients, when the client attempts to connect to Horizon Cloud and is forcing access through Workspace ONE Access, the client is automatically redirected to the Workspace ONE Access environment that is specified in this identity management provider configuration. When the toggle is set to <strong>NO</strong>, automatic redirection is not enabled, and the clients display an informational message to the user instead.</td>
</tr>
</tbody>
</table>

**Note** You can have this redirection enabled for only one of the identity management URLs per pod. If you try to enable this feature for multiple URLs and the same pod, an error message is displayed.

4 Click **Save**.

Configure the Option to Force End-User Access to Use Workspace ONE Access

For each listed provider, you can use the following steps to configure whether end users can access their assigned desktops and remote applications directly from Horizon Cloud or must access only using Workspace ONE Access.

**Note** When you change these settings, it can take up to 5 minutes for the update to take effect.

1 Click **Configure**.
2 Edit settings as described below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force Remote Users to Workspace ONE Access</td>
<td>Select YES to block remote user access except through the identity management provider. Option only displays if that provider status is green.</td>
</tr>
<tr>
<td>Force Internal Users to Workspace ONE Access</td>
<td>Select YES to block internal user access except through the identity management provider. Option only displays if that provider status is green.</td>
</tr>
</tbody>
</table>

3 Click Save.

When you force end-user access through Workspace ONE Access, you typically also edit the corresponding identity provider configuration to specify that the end-user clients automatically redirect to Workspace ONE Access. See Edit Settings for a Configuration.

The feature to force end-user access to Workspace ONE Access works with the Workspace ONE Access redirection feature in the following ways.

<table>
<thead>
<tr>
<th>Force end-user access through Workspace ONE Access setting</th>
<th>Workspace ONE Access redirection setting</th>
<th>What happens when the end user's client connects to Horizon Cloud to access their desktops and applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled (yes)</td>
<td>Enabled (yes)</td>
<td>Client is automatically redirected to Workspace ONE Access.</td>
</tr>
<tr>
<td>Enabled (yes)</td>
<td>Disabled (no)</td>
<td>Client displays a message that tells the user that they must access Horizon Cloud using Workspace ONE Access. Automatic redirection does not occur.</td>
</tr>
<tr>
<td>Disabled (no)</td>
<td>Enabled (yes)</td>
<td>Client displays the Horizon Cloud login screen for the end user to log in. Automatic redirection does not occur because forced access to Workspace ONE Access is not enabled.</td>
</tr>
<tr>
<td>Disabled (no)</td>
<td>Disabled (no)</td>
<td>Client displays the Horizon Cloud login screen for the end user to log in. In this scenario, both forced access and the automatic redirection features are disabled.</td>
</tr>
</tbody>
</table>

Remove a Configuration

To remove one of the configurations:

1 Select the configuration in the list.
2 Click Remove.
3 Click Delete to confirm.
Broker-Related Settings for Your Horizon Cloud Tenant Environment

Use the Horizon Cloud Administration Console's Broker page to modify broker-related settings that apply to your overall Horizon Cloud tenant environment.

As described in Tour of the Cloud-Based Horizon Cloud Administration Console for Administrative Tasks in Horizon Cloud, the console dynamically reflects the current state of your tenant environment. As a result, the console displays sections on this page and the various settings based on which ones are relevant and appropriate for the current, up-to-the minute state of your tenant environment.

**Note** When changing any of the following settings described in the sections below, it can take up to 5 minutes for the update to take effect.

- The settings in the **Session Timeout** sections.
- The **Clean Up HTML Access Credentials When Tab is Closed** setting.

### Universal Broker

The console displays this section when your tenant is configured to have your cloud-connected pods use the Universal Broker to broker end users' clients to their entitled pod-provisioned resources. To change any of the settings for the Universal Broker configuration, click the pencil icon next to the **Universal Broker** label and then follow the on-screen prompts. For additional details about the on-screen settings, see the information described in Configure Universal Broker.

### Single-Pod Broker

The console displays this section when your tenant is configured to have your pods in Microsoft Azure use the VMware Horizon Cloud Service on Microsoft Azure's classic pod-based brokering method to broker end users' clients to their entitled pod-provisioned resources.

### Session Timeout

These settings govern the end users' connections made from their endpoint devices using Horizon Client, Horizon HTML Access, and Workspace ONE. You can adjust these timeout settings to allocate enough time to avoid a user unexpectedly finding that they need to reauthenticate to Horizon Cloud. These settings are associated with the connection between an end user's endpoint device and their assigned VDI desktops, RDS session desktops, and remote applications provided by Horizon Cloud. These settings are separate from the users' logged-in session to the underlying Windows operating system of those desktops and applications. When Horizon Cloud detects the conditions determined by these settings have occurred, it expires the user's authenticated Horizon Client, Horizon HTML Access, or Workspace ONE connection.

**Note** For the meaning of the term connection broker as it is used in the following table, see Selected Pod-Related Terminology Used in these Administration Guide Documentation Topics.
<table>
<thead>
<tr>
<th><strong>Timeout</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Heartbeat Interval</td>
<td>Controls the interval between Horizon Client heartbeats and the state of the endpoint’s connection to the Horizon Cloud pod’s connection broker. These heartbeats report to the pod’s connection broker the amount of idle time that has passed in the connection to the endpoint. Idle time occurs when no interaction occurs with the end-point device, as opposed to idle time in the Windows operating system session that underlies the user’s desktop or remote application usage. In large desktop deployments, setting the activity heartbeats at longer intervals might reduce network traffic and increase performance.</td>
</tr>
</tbody>
</table>
| Client Idle User            | Maximum time that an end user can be idle in a connection between their client device and the Horizon Cloud pod’s connection broker, such as when no keyboard or mouse activity on the client device is detected. When this maximum is reached, the user’s authentication to the broker expires and all active Horizon Client, Horizon HTML Access, and Workspace ONE remote (RDS-based) application connections are closed.  
  - The single sign-on (SSO) credentials at the connection broker are discarded. The user must reauthenticate in their client to reopen a connection from their end-point device to connect to the pod’s connection broker.  
  - RDS-based application sessions are disconnected.  
  **Note** Set the **Client Idle User** timeout to be at least double the **Client Heartbeat Interval** setting to avoid unexpected disconnects from desktops. |
| Client Broker Session       | Maximum time that a Horizon Client, Horizon HTML Access, or Workspace ONE connection can be connected to the pod’s connection broker before the connection’s authentication expires. The timeout count starts each time the user authenticates to Horizon Cloud. When this timeout occurs, the user can continue to work in their assigned session. If the user performs an action that causes communication to the pod’s connection broker, such as changing settings, the system requires the user to reauthenticate and log back in to their client (Horizon Client, Horizon HTML Access, or Workspace ONE).  
  **Note** The **Client Broker Session** timeout must be at least equal to the sum of the **Client Heartbeat Interval** setting and the **Client Idle User** timeout. |

**HTML Access**

The **Clean Up HTML Access Credentials When Tab is Closed** setting affects system security and ease of use when end users use HTML Access to access their desktops or applications. The setting determines if end users must enter their credentials again.

- A value of **Yes**, the option that emphasizes security, prompts end users to again enter their credentials when they reconnect.

- A value of **No**, the option that emphasizes ease of use, does not prompt end users to enter their credentials when they reconnect.

**Pool/Farm Options**

The **Allow Client To Wait For Powered-Off VM** option governs what happens if the end user uses Horizon Client to try to connect to a desktop or remote application when the underlying VDI or RDSH virtual machine is powered off in the cloud. As a result of an assignment’s or RDSH farm’s power management settings, there might not be enough powered-on virtual machine capacity to serve the client’s request. When the connection is initiated, Horizon Cloud starts powering on the underlying virtual machine needed to fulfill the request.
However, although the underlying virtual machine is powering on, the Horizon Cloud agent in the virtual machine has not yet started up and cannot respond to the Horizon Client connection request. Because it can take some time between the client connecting and the agent starting, you can use this option to have the client retry the connection and inform the end user of the estimated time. For this scenario, when the **Enable Client Retry** toggle is set to **Yes**, the client presents a message to the end user that describes the estimated waiting time.

1. Horizon Cloud starts powering on the underlying virtual machine in the cloud that will serve the end user's client request.
2. Horizon Cloud notifies Horizon Client to retry the connection when the agent in the virtual machine is up and running.
3. The client prompts the user with a message that describes the wait time estimated before the client retries the connection.

**About the Horizon Cloud Getting Started Wizard**

You use the Getting Started wizard to perform the configuration steps that are needed before you can fully manage and use the environment, such as registering an Active Directory domain. The Getting Started wizard displays by default when you log in to the Horizon Cloud Administration Console for the first time. After you have finished registering one Active Directory domain and given the Horizon Cloud Super Administrators role to an Active Directory group in that domain, then you have access to the console's left hand navigation bar for performing administration tasks in your environment. Also at that point in time, you can switch the toggle at the bottom of the Getting Started page to stop using the Getting Started as the default console home page and use the Dashboard page as your default home page instead.

**Important**  System workflows involving pods in Microsoft Azure require that the Super Administrators role be given to the domain-join account you specify in the Active Directory domain registration steps. The system workflows are those that involve joining virtual machines in those pods to your Active Directory domain, such as when importing a base image, creating farm RDSH VMs, creating VDI desktop instances, and so on.

Therefore, to avoid such workflows failing, when you have cloud-connected pods in Microsoft Azure, the domain-join account you specify in the Active Directory domain registration steps must be in a group to which you give the Super Administrators role. For more information about the requirements for that domain-join account, see [Service Accounts That Horizon Cloud Requires for Its Operations](#).
The Getting Started wizard provides a high-level overview of the work that you have done, and what is still to do. You can access the wizard from Settings > Getting Started.

**Note** To ensure that you completed all tasks required to run and manage the environment, review the steps in High-Level Workflow for When Your Very First Horizon Cloud Cloud-Connected Pod is from Using the Pod Deployer to Deploy a Pod into Microsoft Azure and its subtopics for your type of pod. You cannot perform certain tasks from the Getting Started wizard, such as uploading certificates.

**Table 8-8. Getting Started Wizard Selections**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capacity</strong></td>
<td>Provides:</td>
</tr>
<tr>
<td></td>
<td>- A high-level overview of your environment’s existing pods.</td>
</tr>
<tr>
<td></td>
<td>- Access to the Add Cloud Capacity wizard, used to deploy your first pod in a cloud capacity environment, such as the Microsoft Azure cloud.</td>
</tr>
<tr>
<td></td>
<td>- The Manage Subscriptions action, used to edit, add, and delete subscription information.</td>
</tr>
<tr>
<td><strong>General Setup</strong></td>
<td>Provides details and links for the initial configuration of various pod-wide settings, such as registering an Active Directory domain.</td>
</tr>
<tr>
<td></td>
<td>See General Setup Section of the Horizon Cloud Administration Console’s Getting Started Wizard.</td>
</tr>
<tr>
<td><strong>Desktop Assignment</strong></td>
<td>- When you have pods deploying in Microsoft Azure, this section provides links to task pages related to working with virtual machines (VMs) that</td>
</tr>
<tr>
<td></td>
<td>are imported into your Horizon Cloud environment, and for publishing golden images. These images are used in farms and VDI desktop assignments.</td>
</tr>
<tr>
<td></td>
<td>See Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure and its subtopics.</td>
</tr>
<tr>
<td></td>
<td>- When you have Horizon on-premises pods or Horizon pods in VMware Cloud on AWS, this section provides links to task pages related to configuring</td>
</tr>
<tr>
<td></td>
<td>desktop assignments. Desktop assignments allow you to make desktop pools from multiple cloud-connected pods available to end users.</td>
</tr>
<tr>
<td></td>
<td>See Chapter 6 Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment.</td>
</tr>
<tr>
<td><strong>Application Assignment</strong></td>
<td><strong>Note</strong> In this release, this section is not displayed when your cloud-connected pods are only Horizon pods on-premises or in VMware Cloud on AWS.</td>
</tr>
<tr>
<td></td>
<td>When you have pods deploying in Microsoft Azure, this section provides links to task pages related to applications and application assignments.</td>
</tr>
<tr>
<td></td>
<td>See Applications in Your Horizon Cloud Inventory and its subtopics.</td>
</tr>
</tbody>
</table>

When you have completed the required steps of registering at least one Active Directory domain and given the Super Administrator role to at least one of your Active Directory user groups, displaying the wizard is optional. To toggle having the wizard appear every time you log in to the console, move the slider at the bottom of the wizard’s main page to **Yes**.

**Note** Even though the wizard’s primary use occurs during your first time setting up a pod and most people toggle off the wizard after that, some people find the wizard might be a convenient launching point when performing some of the standard tasks.
General Setup Section of the Horizon Cloud Administration Console's Getting Started Wizard

In the first-time configuration for a pod connected to your Horizon Cloud environment, you use the choices in the General Setup section for the initial configuration of various pod-wide settings, such as registering an Active Directory domain. After the first-time configuration, you can use the choices in the General Setup section to open the console pages in which you can edit the configurations.

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My VMware Accounts</td>
<td>Give access for other people to log in to the console and your Horizon Cloud environment using their own My VMware accounts. See Give Administrative Roles to Individuals in Your Organization for Logging In To and Performing Actions in Your Horizon Cloud Tenant Environment Using the Horizon Cloud Administration Console.</td>
</tr>
</tbody>
</table>
| Active Directory  | Register the initial Active Directory domain and add the domain bind and domain join information. Domain registration of at least one Active Directory domain is required to give roles and permissions to console users or assign services to users. You must register an Active Directory domain and finish the domain join before you can perform other operations with the first cloud-connected pod, including registering additional Active Directory domains. For information about tasks related to Active Directory and your pods, see:  
  - Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment  
  - Register Additional Active Directory Domains as Cloud-Configured Active Directory Domains with Your Horizon Cloud Tenant Environment  
  - Add Additional Auxiliary Bind Accounts for a Cloud-Configured Active Directory Domain in Horizon Cloud |
<p>| Roles &amp; Permissions| Assign roles to users who will be managing the environment. A role grants its associated permissions to the users given that role. See Assign Roles to Active Directory Groups that Control Which Areas of the Horizon Cloud Administration Console are Activated for Individuals in Those Groups After They Authenticate to Your Horizon Cloud Tenant Environment. |</p>
<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broker</td>
<td>Enable the brokering technology that you want used when your end users' clients connect to the pod-provisioned resources that you have entitled those end users to use. Configure settings related to the brokered end-user sessions, such as session timeout settings.</td>
</tr>
</tbody>
</table>
| Cloud Monitoring Service | The Horizon Cloud cloud monitoring service collects and stores session, application, and desktop data from connected pods for monitoring and reporting purposes.  
  - Use the Cloud Monitoring Service toggle to enable or disable the Horizon Cloud cloud monitoring service. It is enabled by default.  
    When this setting is disabled, the Session Data setting below does not appear.  
    - When the cloud monitoring service is enabled, you can use the Session Data toggle to opt in or opt out of tracking user information related to your end users' sessions. Information collected includes times they logged in, session durations, and average session length per user.  
      When you opt in to the collection of user data, Horizon Cloud collects this information and maintains it for the duration of your use of Horizon Cloud. You can delete the collected data by turning off the Session Data toggle.  
      When you opt out of the collection of user data but leave the cloud monitoring service enabled, Horizon Cloud collects session data for a limited period and hashes the user name to allow real-time administration while disabling historical and aggregated viewing of information. As a result, some reports, such as the User Usage report, are not available. In this case, the system also continues to collect other data related to applications and desktops in connected pods.  
      The information collected by the Horizon Cloud cloud monitoring service is used in charts on the Dashboard page and reports on the Reports page. See Health Visibility and Insights into Your Cloud-Connected Pods Provided by the Cloud Monitoring Service in Horizon Cloud and Reports Page. |
Using the Filter Field in the Horizon Cloud Administration Console

Various pages in the Horizon Cloud administrative console provide ways to filter the medium to large amount of information that is displayed on the page, such as the various reports and the Activity page. On some pages, a filter field appears at the top of the page. On other pages, each column has a filter icon in the column heading that you click to access the filter text box. For those pages that provide filtering, as you enter characters into the filter text box, the system displays only the subset of the displayed records that contain characters that match that pattern.

The following screenshots illustrate examples of the filter box that is provided in some pages and the filter icon that is provided for columns in some pages. This first example is in the Images page.

This second example is in the Activity page.

<table>
<thead>
<tr>
<th>Description</th>
<th>Status</th>
<th>% Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expanding assignment lakwin7</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Converting desktop lakwin7</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Converting desktop lakwin7</td>
<td></td>
<td>100%</td>
</tr>
</tbody>
</table>

**Note** For those filter text boxes that are at the top of the page, the system begins matching the pattern and filtering the records displayed in the page after you have entered three (3) characters into the filter text box. For the filter icon at the top of column headings, the system begins filtering after you enter one (1) character.
On-Screen Filtering in the Reports Pages

In the tabs of the Reports page, the filtering text box works on the number of items that are displayed on the user interface itself and not on the total set of system records for that item. These pages support displaying up to 500 items. Therefore, if the system contains more than 500 records for an item, up to 500 items only are displayed in the user interface page. Using the filter text box only filters the 500 displayed records. The filter is not applied to the full set. Here is an example to illustrate:

- You have 2000 users assigned to a VDI floating desktop assignment.
- The user names range from vdiuser-1 to vdiuser-2000, such as vdiuser-500, vdiuser-501, vdiuser-502, and so on, up to vdiuser-2000.
- Over the course of a day, all 2000 users log in and use a desktop from that assignment.
- When you navigate to Monitor > Reports > Desktop Mapping, a displayed message states the report has more than 500 items.
- When you enter vdiuser-54 into the filter to see the records for users vdiuser-54, vdiuser-540, vdiuser-541 up to vdiuser-549, you expect to see 11 rows displayed.

However, instead of displaying the expected 11 rows filtered out of the full 2000 set, the Desktop Mapping page displays only the subset of the originally displayed 500 rows that match the filter pattern. To see the full data set, use the export feature (出口).
Troubleshooting for Administrators of Horizon Cloud Environments

You can troubleshoot issues that you might experience in ongoing operation of your Horizon Cloud environment.

This chapter includes the following topics:

- Required Administrator Actions When the Disk Size for a Farm or VDI Desktop Assignment is Increased
- Cannot Successfully Log In at the First Login Screen of the Horizon Cloud Administration Console
- Convert to Image Task Fails with Timeout Error Even After Addressing the Logged Microsoft Windows Sysprep Errors
- For a Windows Server 2012 Image, Convert to Image Task Fails with Timeout Error
- Notifications When the Primary Domain-Bind Account is Locked Out
- New Farm Remains In Progress
- Windows Error Message Appears When Trying to Connect to a Desktop from a Floating VDI Desktop Assignment
- Email Feedback Option Does Not Work
- Considerations For Using Nested Active Directory Domain Organizational Units
- When Your Pod is Not Yet Updated to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image

Required Administrator Actions When the Disk Size for a Farm or VDI Desktop Assignment is Increased

When you create or edit a farm or a VDI desktop assignment, you have the option of increasing the OS disk size value. When that option is used, the OS disk of each VM in that farm or assignment is created at that size. However, as a result of default behavior of VMs in Microsoft Azure, even though the VM's disk is expanded, the partition containing the C drive is not expanded to encompass the entire disk. That new space on the VM's disk is unused until you take actions in the VM to expand the C drive partition to encompass the new space.
Microsoft provides several ways to expand the partition to cover the full disk. The following Powershell commands are untested by VMware and are given only as an example of one way the expansion might be achieved using a script. You must determine the method that is most appropriate for your organization.

```
,size = (Get-PartitionSupportedSize -DiskNumber 0 -PartitionNumber 2)
Resize-Partition -DiskNumber 0 -PartitionNumber 2 -Size $size.SizeMax
```

This example assumes the disk number is 0 and partition number is 2. More information about these Powershell commands is available at https://docs.microsoft.com/en-us/powershell/module/storage/resize-partition?view=win10-ps.

**Cannot Successfully Log In at the First Login Screen of the Horizon Cloud Administration Console**

When the My VMware account system is experiencing a system outage for maintenance, you are not able to log in to Horizon Cloud's administrative console.

**Problem**

You try to log in to Horizon Cloud at https://cloud.horizon.vmware.com. Even though the Horizon Cloud login screen does not indicate any reason, you find when you enter valid My VMware account credentials into the first login screen, the attempt fails.

**Cause**

Login authentication into the console relies on My VMware account credentials. If the My VMware account system is experiencing a system outage and cannot take authentication requests, logging in to the console during that period fails.

**Solution**

◆ If you encounter issues logging in to the console's main login screen, check the Horizon Cloud System Status page at https://status.horizon.vmware.com to see the latest system status.

On that page, you can also subscribe to receive updates.

**Convert to Image Task Fails with Timeout Error Even After Addressing the Logged Microsoft Windows Sysprep Errors**

Even though you have taken steps to prevent Microsoft Sysprep issues from occurring when you convert your image VM to a published image, the conversion task times out in a subsequent attempt.
Problem

In the first attempt to publish the image, in the Activity page, you see that the image conversion process fails with a timeout error because of Microsoft Sysprep issues related to appx packages. After you follow the optimization steps described in Customize the Imported VM’s Windows Operating System and address any issues described in the Microsoft Sysprep error logs, you try to convert the image. In this second attempt, you see messages in the Activity page as "Waited 20 minutes for virtual machine to power off: Convert the image back to the virtual machine".

Cause

This situation happens because the second attempt to run the Microsoft Sysprep process is hung or not responsive. Use the following steps to work around the issue.

Solution

1. Ensure that you address the Microsoft Sysprep issues according to the error messages in the Microsoft Sysprep error logs and VMware KB 2079196 and Microsoft KB 2769827.

2. In the image VM, examine the VMware Horizon Agent service and ensure it has its startup type set to Automatic.

   If the image is located in a pod with a manifest earlier than 1600, the VM will also have the VMware DaaS Agent service. Verify that the VMware DaaS Agent service has its startup type set to Automatic.

3. Reboot the image VM.

4. Try the conversion process again on the rebooted VM.

For a Windows Server 2012 Image, Convert to Image Task Fails with Timeout Error

Sometimes after you have installed applications into a Windows Server 2012 image VM to customize it before running the publishing workflow, the publishing process fails with the error message about timing out after 20 minutes.

Problem

After installing applications into the Windows Server 2012 image VM, logging off the VM, and then starting the publishing workflow, sometimes the workflow fails with the VM powering off while the Microsoft System Preparation (Sysprep) process is running.

Solution

1. Ensure that you address the Sysprep issues according to the error messages in the Sysprep error logs and VMware KB 2079196 and Microsoft KB 2769827.
2 In the image VM, examine the VMware Horizon Agent service and ensure it has its startup type set to Automatic.

If the image is located in a pod with a manifest earlier than 1600, the VM will also have the VMware DaaS Agent service. Verify that the VMware DaaS Agent service has its startup type set to Automatic.

3 Reboot the VM.

4 Try the conversion process again on the rebooted VM.

**Notifications When the Primary Domain-Bind Account is Locked Out**

When Horizon Cloud detects an authentication failure due to a locked primary domain-bind account, a notification is displayed in the administrative console to alert you to remedy the state of the account. The system uses the primary domain-bind account as a service account to connect to the Active Directory (AD) server and query Active Directory.

Each time an administrator successfully logs in to the console, the system checks whether the primary domain-bind account is in a failed or inactive state. If the system determines the account is in a failed or inactive state, a notification is created. When the notification is created, it is added to the Notifications page and is reflected in the count on the bell icon located in the upper right corner of the console. You can read the notification details by clicking the bell icon or by navigating to the Notifications page.

**Note** The connection state for the connection between the system and the AD server is cached for 15 minutes. As a result, it might take up to 15 minutes from the time the primary domain-bind account goes into a locked-out state until the notification is reflected in the console. For example, if you log in to the console, and then manually locked out your primary domain-bind account in your AD server, it might take up to 15 minutes for the notification to display in the console. Similarly, if you see the lockout notification in the console and then fix the account in your AD server, the console might continue to show the account lockout notification for up to 15 minutes after the fix.

If the primary domain-bind account becomes locked out, the system falls back to use an active configured auxiliary domain-bind account to authenticate the connection to the Active Directory server. When you see a notification that the primary domain-bind account is locked out, you should take action to remedy the state of the primary domain-bind account to ensure successful system connection continues over time.

**New Farm Remains In Progress**

You initiate creation of a new farm from the Farms page and the system begins creating the farm and its RDSH virtual machines (VMs). However, even after thirty minutes have passed, the page
shows the farm's status is still in progress. When you drill into the farm details page, you see that one of its VMs is in offline status.

**Problem**

Even though the other VMs in the farm show online status, the farm creation process cannot complete because one VM continues to show offline status.

**Cause**

A temporary network connection loss causes the VM's state to show as offline in Horizon Cloud, preventing completion of the farm creation workflow.

**Solution**

1. Navigate to the farm's Session Hosts tab.
2. Select the check box next to the offline VM and click **Delete**.

   The system deletes the VM. Then after a few minutes, the system automatically recreates the VM, it completes coming online, and the farm changes to online status.

### Windows Error Message Appears When Trying to Connect to a Desktop from a Floating VDI Desktop Assignment

When an end user tries to connect to a desktop from a floating VDI desktop assignment, a Windows message appears that states *Windows couldn't connect to the System Event Notification Service service. Please consult your system administrator.*

**Problem**

After the user sees this message and clicks the displayed **OK** button, the session might disconnect. Sometimes after clicking **OK**, the user can log in to the desktop. Usually after clicking **OK**, the user can try to log into the desktop again and the second attempt is successful.

**Cause**

This issue is a known Microsoft Windows issue that is described at [this page at answers.microsoft.com](http://answers.microsoft.com).

### Email Feedback Option Does Not Work

When you click the email link in the **Share your Feedback** window, nothing happens or a browser error message appears.
Problem

In the Share your Feedback window, you have the option of clicking the email link to send an email with your feedback:

Share Your Feedback

Depending on your settings for your local system's browser or mail application, when you click the console's Feedback icon, you might see one of the following:

- Nothing happens.
- A browser error message appears.

Cause

The design for this menu choice is to run the new mail action of your local system's default mail application, using mailto:feedback.horizonair@vmware.com. This error occurs when the browser cannot perform the mailto action, such as under these conditions:

- Your browser is set up to block pop-up windows.
- Your browser's applications list is not configured with a default action for the mailto content type or the mailto content type is configured with the action Always ask.
- Your local system does not have a default local mail application configured.
Solution

1. If your browser blocks pop-up windows, add the console’s URL to the exception list.

2. Configure your browser’s `mailto` content type’s action with a mail application, so that the email link can successfully open a new email form.

3. If you do not want to change your browser settings, you can submit feedback by manually sending an email to feedback.horizonair@vmware.com.

Considerations For Using Nested Active Directory Domain Organizational Units

When you create a farm or a VDI desktop assignment using the Horizon Cloud Administration Console, you can use the Computer OU field to optionally specify an Active Directory organizational unit (OU) where the farm’s VMs or the VDI desktop VMs are to be located. You can use these steps to locate the nested OU information for your organization to use in the Computer OU field.

**Note**  
Microsoft limits an individual OU to 64 characters or less. An OU path that is longer than 64 characters, but with no individual OU having more than 64 characters, is valid. However, each individual OU must be 64 characters or less.

As a result, in the console’s Active Directory page’s Default OU field and the farm and VDI desktop assignments’ Computer OU fields, you can enter OUs that are up to 64-characters long, not counting the `OU=` portion of your entry.

Use these steps to locate the nested OU information in your organization’s Active Directory domain server.

**Procedure**

1. From your Active Directory machine, open Active Directory Users and Computers.

2. Select View > Advanced features (Enabled Advanced features).

3. Navigate to the Organizational Unit where the desktops will be placed.

4. Right-click and select Properties.

5. Click the Attribute editor and select distinguishedName.

6. Click View.

7. Enter the distinguished name information in the Computer OU field in the console.
   
   Only the `OU=` part of the string is required. The `DC=` part is optional.
When Your Pod is Not Yet Updated to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image

Starting with pod manifest version 1230 and later for pods in Microsoft Azure, domain accounts can direct connect to image virtual machines that have the agent software installed. Prior to pod manifest 1230, the agent software installed in a domain-joined VM prevents domain accounts from directly connecting to that VM. Starting with pod manifest 1230, you can use a domain account to log in and customize the image VM. However, if your pod is at a manifest earlier than 1230, you can use these steps to configure the ability for domain accounts to remote connect to the imported image.

So that you can customize the image for your organization’s needs, you must be able to remotely connect to and log in to that image’s virtual machine located in Microsoft Azure. If the image VM is joined to an Active Directory domain and your organization has a policy that prevents use of local administrator accounts on domain-joined VMs, you will not be able to log in to the image VM until you configure the DaaS Direct Connect Users local group with those domain accounts you want used for customizing the image.

You connect to the image VMs in Microsoft Azure using your Remote Desktop Protocol (RDP) software. As part of the overall process of creating the image VM, these items are put in place:

- The VM is always joined to the domain when it was created either using the Import Virtual Machine wizard prior the December 2019 service release. The VM is also joined to the domain when manually created and you explicitly joined it to the domain, or it was created using the Import Virtual Machine wizard after the December 2019 service release and you selected the wizard option to join the domain. Prior to the December 2019 service release, the Import Virtual Machine wizard always automatically joined the VM to the domain.

- The Horizon agent software is installed in the VM’s Microsoft Windows operating system.

By default, the agent software prevents using any account to RDP to the VM’s guest Microsoft Windows system other than the VM’s local administrator account with which the agent software was installed. For example, when you try to RDP to the image VM using a domain administrator account that is a member of the local Administrators group, even though the connection is made initially, as the Microsoft Windows session starts, a message is displayed. The message states that direct connection to your virtual desktop is not allowed.
However, some organizations typically have policies that prevent use of the local administrator account on domain-joined VMs. To enable providing domain accounts with the ability to RDP and log in to customize the image VM, installing the agent software also creates a local group named DaaS Direct Connect Users. This group does not have local administration rights. The agent allows domain accounts in this group to connect to the desktop using a direct RDP connection. The DaaS Direct Connect Users group is empty when created. To give the RDP capability to those domain accounts you want used to customize the image, you add those domain users to the DaaS Direct Connect Users local group.

The following screenshot is an example showing the DaaS Direct Connect Users group in the Local Users and Groups window on a image VM that was created using the Import Virtual Machine from Marketplace wizard.

When you cannot direct connect to the VM using the local administrator account, you use a Group Policy Object (GPO) policy in your Active Directory environment to add domain accounts to the DaaS Direct Connect Users group. The following steps describe using the GPO policy's Restricted Groups - Members Of method for adding members to the DaaS Direct Connect Users group on the domain-joined VM.

1. In your Active Directory environment, create a new GPO.
2. Right-click on the GPO and select **Edit**.
3. In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Restricted Groups**.
4. Right-click **Restricted Groups** and select **Add Group**.
5. In the Add Group box, type DaaS Direct Connect Users and click **OK**.
6. In the properties dialog, use the **Members of this group** area and its **Add** button to add those domain accounts that you want able to connect to the image VM.
7. When you are finished adding accounts into the **Members of this group** area, click **OK** to close the properties dialog.
8. Close the Group Policy Management Editor and the Group Policy Management Console.
9. Link the newly created GPO to the same domain that is used for the image VM.
After the new GPO is linked to the domain, you can use one of those specified domain accounts to RDP to the image VM and customize it. Follow the steps as described in Customize the Imported VM's Windows Operating System and its subtopics.
Revision History — Changelog — Administration of Your Horizon Cloud Tenant Environment and Your Fleet of Onboarded Pods

This documentation topic provides the history of substantive changes to Administration of Your Horizon Cloud Tenant Environment and Your Fleet of Onboarded Pods.

**Note** Only substantive and significant changes made to the guide's topics starting from August 31, 2018 are provided. Details about revisions prior to that date are not available. Also, minor content revisions such as fixing typos, format changes such as turning lists into tables, and other such insignificant changes are not provided.

### October 8, 2020

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 OCT 2020</td>
<td>Updates for the new features corresponding to the October 8, 2020 What's New in the Horizon Cloud Release Notes. Also the following updates:</td>
</tr>
<tr>
<td></td>
<td>Information added to the following topics to state that all manual desktop pools — managed or unmanaged — are not eligible to participate in multi-cloud assignments based on Horizon pods.</td>
</tr>
<tr>
<td></td>
<td>- Horizon Pods - Create a New Desktop Pool for Multi-Cloud Assignments</td>
</tr>
<tr>
<td></td>
<td>- Horizon Pods - Prepare an Existing Desktop Pool for Use in a Multi-Cloud Assignment</td>
</tr>
<tr>
<td></td>
<td>- Horizon Pods - Create a Multi-Cloud Assignment of VDI Desktops</td>
</tr>
</tbody>
</table>

### July 9, 2020 — October 7, 2020

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 SEP 2020</td>
<td>Information added to the following topics to state that manual desktop pools that are unmanaged are not eligible to participate in multi-cloud assignments based on Horizon pods.</td>
</tr>
<tr>
<td></td>
<td>- Horizon Pods - Create a New Desktop Pool for Multi-Cloud Assignments</td>
</tr>
<tr>
<td></td>
<td>- Horizon Pods - Prepare an Existing Desktop Pool for Use in a Multi-Cloud Assignment</td>
</tr>
<tr>
<td></td>
<td>- Horizon Pods - Create a Multi-Cloud Assignment of VDI Desktops</td>
</tr>
<tr>
<td>8 SEP 2020</td>
<td>Updates made to align this guide with the September 9, 2020 new items listed in the Horizon Cloud Release Notes and information added to the following topics to respond to customer feedback.</td>
</tr>
<tr>
<td></td>
<td>- New topic for the new Managing Subscriptions feature: Horizon Cloud — Deleting, Editing, and Adding Microsoft Azure Subscription Information</td>
</tr>
<tr>
<td></td>
<td>- Pods in Microsoft Azure - View Details About a VDI Multi-Cloud Assignment</td>
</tr>
<tr>
<td></td>
<td>- Horizon Cloud Connector Known Considerations</td>
</tr>
</tbody>
</table>
### March 17, 2020 — July 8, 2020

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 JUN 2020</td>
<td>Updates made to align this guide with the June 9, 2020 new items listed in the Horizon Cloud Release Notes. The regional names that appear in the Welcome email have been updated to use human-friendly names. The following doc topic is also updated to align with that change: DNS Requirements for a Horizon Cloud Pod in Microsoft Azure.</td>
</tr>
<tr>
<td>27 MAY 2020</td>
<td>Updates made to align this guide with the May 27, 2020 new items listed in the Horizon Cloud Release Notes.</td>
</tr>
<tr>
<td>12 MAY 2020</td>
<td>Updates made to align this guide with the May 12, 2020 service updates listed in the Horizon Cloud Release Notes. Also corrected entries in the table for agent-related ports and protocols requirements in doc topics Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later and Ports and Protocols Requirements for a Horizon Cloud Pod Deployed Prior to the September 2019 Release.</td>
</tr>
<tr>
<td>5 MAY 2020</td>
<td>Added topic About External and Forest Trust Support for Cloud-Connected Pods in Horizon Cloud.</td>
</tr>
<tr>
<td>28 APR 2020</td>
<td>Topics updated:</td>
</tr>
<tr>
<td></td>
<td>- Removed paragraphs from two doc topics that had incorrect statements about the serial port redirection and scanner redirection options: For Pods at Manifest 1600 and Higher, Install the Agent-Related Software Components in the Base Virtual Machine and Pair it with Horizon Cloud and For Pods at Manifests Lower Than 1600, Install the Agent-Related Software Components in the Base Virtual Machine.</td>
</tr>
<tr>
<td>Revision</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>14 APR 2020</td>
<td>Topics updated:</td>
</tr>
<tr>
<td></td>
<td>- Removed the notes that said the automated Import VM from Marketplace wizard could not be used when the pod is configured with a proxy. The previous limitations that prevented the wizard's use when the pod is configured with a proxy have been addressed.</td>
</tr>
<tr>
<td></td>
<td>- Added a note that even though the pod deployment wizard will display a choice for the Azure Germany cloud environment, support for that choice is discontinued because Microsoft now has German regions in their set of standard global regions and has sunsets use of their separate Azure Germany cloud environment. See <a href="https://kb.vmware.com/kb/77121">VMware Knowledge Base article 77121</a>.</td>
</tr>
<tr>
<td></td>
<td>- Updated the supported client information for Universal Broker.</td>
</tr>
<tr>
<td>17 MAR 2020</td>
<td>Updates for the new features corresponding to the March 17, 2020 What's New in the <a href="https://www.vmware.com/support/">Horizon Cloud Release Notes</a>.</td>
</tr>
</tbody>
</table>

**December 12, 2019 — March 16, 2020**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 FEB 2020</td>
<td>Updated to remove an out-of-date graphic from this introduction page, to remove descriptions of brokering based on Cloud Pod Architecture, and to add a description of the system's default whitelisted appx packages to the doc topic Using the Remove Windows Store Apps Option When Using the Import Desktop Wizard.</td>
</tr>
<tr>
<td>13 JAN 2020</td>
<td>Updated for:</td>
</tr>
<tr>
<td></td>
<td>- Information about the Horizon Universal Broker feature. This feature is now in Initial Availability for cloud-connected Horizon 7 pods. This feature is used with multi-cloud assignments. For the system requirements and detailed information, see the topic Chapter 6 Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment and all of its subtopics that pertain to multi-cloud assignments for cloud-connected Horizon 7 pods.</td>
</tr>
<tr>
<td></td>
<td>- Addition of prominent Attention and Remember notes to the Configure Automated Updates of the Horizon Cloud Connector Virtual Appliance to point out that you will only see the corresponding options in the user interface if and only if your Horizon Cloud tenant account is enabled with the relevant capability, and you must explicitly request enablement of that capability by contacting your VMware representative. By default, those options are deactivated for tenants unless you request access to that feature.</td>
</tr>
<tr>
<td>12 DEC 2019</td>
<td>Updates for the new features corresponding to the December 13, 2019 What's New in the <a href="https://www.vmware.com/support/">Horizon Cloud Release Notes</a>.</td>
</tr>
</tbody>
</table>

**September 17, 2019 — December 11, 2019**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 November 2019</td>
<td>Revised the topics about creating desktop images to accurately distinguish the steps required when the image is in a pod that has manifest version lower than 1600 from the steps required for pods of manifest 1600 and higher. See Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure and its subtopics.</td>
</tr>
<tr>
<td>17 SEP 2019</td>
<td>Updates for the new features corresponding to the September 17, 2019 What's New in the <a href="https://www.vmware.com/support/">Horizon Cloud Release Notes</a>.</td>
</tr>
</tbody>
</table>
### July 4, 2019 — September 16, 2019

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 JUL 2019</td>
<td>Updated doc topic <strong>Updating Your Horizon Cloud Pod</strong> with specifics about the number of available cores required in your Microsoft subscription for stage one to be successful.</td>
</tr>
<tr>
<td>4 JUL 2019</td>
<td>Updates for the new features corresponding to the July 2019 What's New in the <strong>Horizon Cloud Release Notes</strong>.</td>
</tr>
</tbody>
</table>

### March 21, 2019 — July 3, 2019

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 JUN 2019</td>
<td>The following topics and areas are updated.</td>
</tr>
<tr>
<td></td>
<td>- Information related to integrating a VMware Identity Manager™ environment with a Horizon Cloud pod in Microsoft Azure. The updated topics include:</td>
</tr>
<tr>
<td></td>
<td>- Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access, Configure a Horizon Cloud Pod in Microsoft Azure for Workspace ONE Access, Identity Management Page in the Horizon Cloud Administration Console, Configure SSL Certificates Directly on the Pod Manager VMs, Such as When Integrating the Workspace ONE Access Connector Appliance with the Horizon Cloud Pod in Microsoft Azure, So that Connector Can Trust Connections to the Pod Manager VMs, High-Level Workflow for When Your Very First Horizon Cloud Cloud-Connected Pod is from Using the Pod Deployer to Deploy a Pod into Microsoft Azure.</td>
</tr>
<tr>
<td>21 MAR 2019</td>
<td>Updates for the new features corresponding to the March 2019 What's New in the <strong>Horizon Cloud Release Notes</strong>.</td>
</tr>
</tbody>
</table>

### December 13, 2018 — March 20, 2019

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 JAN 2019</td>
<td>Added a new topic that gives an example of locating the NetBIOS name that the registering Active Directory domain workflow requires. See <strong>Locating the Information Required for the Horizon Cloud Register Active Directory Workflow's NETBIOS Name and DNS Domain Name Fields</strong>.</td>
</tr>
<tr>
<td>23 JAN 2019</td>
<td>Updated the VDI table row in topic <strong>Multiple-Monitor Support for Desktops and Remote Applications Provided By a Horizon Cloud Pod in Microsoft Azure</strong> to match the VDI assignment's model information that the Administration Console provides.</td>
</tr>
<tr>
<td>22 JAN 2019</td>
<td>Revisited the description of the Assignment page's <strong>Recover</strong> action, in <strong>About the Assignments Menu in the Horizon Cloud Administration Console</strong>. Removed the task topic about recovering desktops in a VDI desktop assignment, because that task is not applicable to pods in Microsoft Azure.</td>
</tr>
<tr>
<td>13 DEC 2018</td>
<td>Updates for the new features corresponding to the December 2018 What's New in the <strong>Horizon Cloud Release Notes</strong>.</td>
</tr>
</tbody>
</table>
May 2018 — December 12, 2018

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 SEP 2018</td>
<td>Updated <a href="#">Manually Pair the Configured Virtual Machine with Horizon Cloud For Pods with Manifests Lower Than 1600</a> to correct the VMware, Inc. portion of the registry path.</td>
</tr>
<tr>
<td>5 SEP 2018</td>
<td>Updated <a href="#">Convert a Certificate File to the PEM Format Required for Pod Deployment</a> to fix a broken link to the Unified Access Gateway documentation page.</td>
</tr>
</tbody>
</table>
| 31 AUG 2018 | Topics updated:  
- [DNS Requirements for a Horizon Cloud Pod in Microsoft Azure](#) updated to correct port information about True SSO Enrollment Server and RADIUS, remove s3-us-west-2.amazonaws.com from the DNS table, and fix some grammar issue.  
- [Add a Gateway Configuration to a Deployed Horizon Cloud Pod](#) updated to correct description of Name ID Suffix field and add more information about the PAP authentication mechanism.  
- [Integrate a Horizon Cloud Pod in Microsoft Azure with Workspace ONE Access](#) and [Configure a Horizon Cloud Pod in Microsoft Azure for Workspace ONE Access](#) updated to add a note about ensuring the VMware Identity Manager™ connector's authoritative time source matches the node's configured NTP server.  
- [Complete Configuring True SSO for your Horizon Cloud Environment](#) updated to clarify you enter the fully-qualified domain name of the enrollment server. |