You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to
docfeedback@vmware.com
Contents

About This Horizon Cloud Administration Guide 7

1 Introduction to Horizon Cloud 10
   End-to-End Workflow When Your Very First Cloud-Connected Pod is from Deploying into VMware Cloud 12
   End-to-End Workflow When Your Very First Cloud-Connected Pod is from Connecting Horizon Cloud with an Existing Manually Deployed Horizon 7 Pod 12
   Suggested Workflow for When Your Very First Cloud-Connected Pod is from Deploying into Microsoft Azure 13

2 Getting Started Using Your Horizon Cloud Environment 18
   Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment 20
   Service Accounts That Horizon Cloud Requires For Its Operations 29
   Locating the Information Required for the Register Active Directory Workflow's NETBIOS Name and DNS Domain Name Fields 32
   Horizon Cloud Support for Active Directory Domain Controllers That Have LDAP Server Signing Requirements 34
   Log in to the Horizon Cloud Administration Console 35
   Give Administrative Access to People in Your Organization 37
   Register Additional Active Directory Domains 38
   Add Additional Auxiliary Domain Bind Accounts 44
   Assign Administrative Roles to Active Directory Groups 45
   Join or Leave the Customer Experience Improvement Program 48
   Remove the Active Directory Domain Registration 48
   Upgrade Horizon 7 Cloud Connector Virtual Appliance 50
   Troubleshoot the Horizon 7 Cloud Connector Virtual Appliance Upgrade 51

3 Unified Visibility, Health Monitoring, and Help Desk Operations Using the Horizon Cloud Administration Console 53
   Tour of the Horizon Cloud Administration Console 54
   Dashboard Page 55
   Capacity Page 59
      Deploying Pods Using the Capacity Page 65
   Help Desk Features in Your Horizon Cloud Environment 108
      Using the Console's Search Feature 109
      The User Card in the Horizon Cloud Administration Console 110

4 Workflows for Cloud-Connected VMware Horizon 7 Pods 115
   Changing the State of a Pod 115
   Change a Pod to Managed State 116
Change a Pod to Monitored State 117
Creating Desktop Assignments 117
   Worksheet for Creating a Desktop Assignment 117
   Create a New Desktop Assignment 120
Managing Desktop Assignments 122
   Edit a Desktop Assignment 125
   Delete a Desktop Assignment 125
Disconnecting Pods 126
   Disconnect a Pod 126
   Clear the Cloud-Managed Properties from a Pod 127

5 Introduction to Horizon Cloud Pods in Microsoft Azure 129
   Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure 135
      Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace 137
      Customize the Master Image VM's Windows Operating System 148
      Install NVIDIA Graphics Drivers in a GPU-Enabled Master Image 153
      Convert a Configured Master Virtual Machine to an Assignable Image 155
      Manually Build the Master Virtual Machine in Microsoft Azure 157
   Using Microsoft Azure Disk Encryption with Your Farms and VDI Desktops 184
   Using Data Disks with Virtual Desktops from a Horizon Cloud Pod in Microsoft Azure 187
      Setting Up a Data Disk for a Master Image VM 189
   VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure 194
      Install the NSX Agent in the Master Image 197
      Firewall Rules Required in NSX Manager for Pod-Provisioned VMs 200
      Add the Required Forwarding Policy in NSX Manager for the Pod-Provisioned VMs 201
   Farms in Horizon Cloud 202
      Create a Farm 202
      Managing Farms in Horizon Cloud 215
      Example of Farm Rolling Maintenance 220
   Applications in Your Horizon Cloud Inventory 221
      Importing New Applications from an RDSH Farm Using Auto-Scan from Farm 222
      Manually Adding Custom Applications from an RDSH Farm 223
      Create a Remote Application Assignment 224
   Creating Desktop Assignments in Horizon Cloud 226
      Types of Desktop Assignments 226
      Create an RDSH Session Desktop Assignment 228
      Create a Floating VDI Desktop Assignment 229
      Create a Dedicated VDI Desktop Assignment 242
   Create a URL Redirection Customization and Assign it to Users 253
      Understanding What URL Content Redirection Is 256
      Configuring Agent-to-Client Redirection 257
Managing Assignable Images 260
  Actions You Can Perform on Assignable Images 260
  Change RDS-Enabled Images Used for Farms 263
  Change Images Used for VDI Desktop Assignments 265
Managing Assignments 267
  View an Assignment 271
  Edit an Assignment 272
  Delete an Assignment 273
  Resizing a VDI Desktop Assignment 274
  About Network Security Groups and Your VDI Desktops 275
Managing VM Types and Sizes for Farms and Assignments 276
Updating the Agent-Related Software Used by Horizon Cloud 277
  Update Agent Software for RDSH Images 279
  Update Agent Software for Dedicated VDI Desktop Assignments 284
  Update Agent Software for Images Used by Floating VDI Desktop Assignments 291
Managing Your Pods Deployed in Microsoft Azure 294
  Obtain the Pod's Load Balancer Information to Map in your DNS Server 295
  Upload SSL Certificates Used to Support Direct Connections 297
  Update the Subscription Information Associated with Deployed Pods 300
  Examine a Subscription's Current Usage of Your Microsoft Azure Limits 301
  Updating Your Horizon Cloud Pod 302
  Backup and Restore Service for Pods in Microsoft Azure 307
  Change the Horizon Cloud Pod's NTP Setting 307
  Change the FQDN and Certificate Used for the Pod's Unified Gateway Configuration 308
  Add a Unified Access Gateway Configuration to a Pod, With or Without Two-Factor Authentication 309
  Removing a Subscription Entry 315
  Convert a Certificate File to the PEM Format Required for Pod Deployment 316
  DNS, Ports, Protocols Requirements for a Horizon Cloud Pod in Microsoft Azure 319
  Default Network Security Group Rules for the VMs in a Horizon Cloud Pod Deployed in Microsoft Azure 330
  Resource Groups Created For a Pod Deployed In Microsoft Azure 335
Integrate a Horizon Cloud Pod in Microsoft Azure with a VMware Identity Manager™ Environment 337
  Configure a Pod in Microsoft Azure for VMware Identity Manager™ 341
  Confirm End-User Access to Desktop Assignments in VMware Identity Manager™ 342
Configure True SSO for Use with Your Horizon Cloud Environment 343
  Install and Configure a Windows Server 2012 R2 Certificate Authority 344
  Set Up a Certificate Template on the CA 346
  Download the Horizon Cloud Pairing Bundle 349
  Set up the Enrollment Server 350
  Complete Configuring True SSO for your Horizon Cloud Environment 351
End User Connections to Desktops and Applications Provided by Your Horizon Cloud Environment 352
Enable Time Zone Redirection for RDS Desktop and RDS-Based Application Sessions 352
Multiple-Monitor Support for Desktops and Remote Applications Provided By a Horizon Cloud Pod in Microsoft Azure 352
Access Desktops and Applications 354

6 About Menu Selections in the Administration Console 360
   About the Monitor Icon 361
   Activity Page 362
   Reports Page 364
   Notifications Page 367
   About the Assignments Icon 367
   About the Inventory Icon 369
   Imported VMs Page 370
   About the Settings Icon 371
      Edit General Settings 372
      Horizon Client Timeout Settings 375
      Domain Security Settings on General Settings Page 376
      File Share Page 385
      Utility VMs Page 385
      Identity Management Page 386
      About the Horizon Cloud Getting Started Wizard 388

7 Using the Filter Field in the Administration Console 391

8 Troubleshooting for Administrators of Horizon Cloud Environments 393
   Cannot Successfully Log In at the First Login Screen of the Administration Console 393
   Convert to Image Task Fails with Timeout Error Even After Addressing the Logged Microsoft Windows Sysprep Errors 394
   For a Windows Server 2012 Image, Convert to Image Task Fails with Timeout Error 395
   Notifications When the Primary Domain-Bind Account is Locked Out 395
   New Farm Remains In Progress 396
   Windows Error Message Appears When Trying to Connect to a Desktop from a Floating VDI Desktop Assignment 396
   Give Feedback Menu Choice Does Not Work 397
   Considerations For Using Nested Active Directory Domain Organizational Units 397
   Horizon 7 Cloud Connector Known Considerations 398
      Set a Password Expiry Policy for the Horizon 7 Cloud Connector Root User 399
      Static IP and Proxy Configuration for the Horizon 7 Cloud Connector Virtual Appliance 400
   When Your Pod is Not Yet Upgraded to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image 401
About This Horizon Cloud Administration Guide

This *Administration Guide* explains how to use VMware Horizon® Cloud Service™ to administer the pods you have connected to this cloud service.

The service offers more than one deployment mode. This document applies when you are using the Horizon Cloud Administration Console to work with the following items:

- VMware Horizon® 7 pods that you installed on-premises and then connected to Horizon Cloud
- VMware Horizon 7 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
- VMware Horizon 7 pods in your VMware Cloud software-defined data centers (SDDCs) that were deployed using this release's Tech Preview automated deployer feature.

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

For information about how VMware handles information collected through this product, click here: [https://www.vmware.com/help/privacy.html](https://www.vmware.com/help/privacy.html)

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 7 pod in VMware Cloud, a VMware Horizon 7 pod on-premises, or a pod in Microsoft Azure. For information on how to connect a supported environment to the cloud service, see the *Horizon Cloud Deployment Guide*.

**Important** This document describes features available in the 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 Administration 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 Administration Console that you are expecting to see, contact your VMware account representative to verify whether your license entitles your use of that feature.
Document Revision History

This document, *Horizon Cloud Administration Guide*, is updated with each release of the product or when necessary.

This table provides the update history.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 JUL 2019</td>
<td>Initial version, when the described features were deployed live into production. For features relating to pods in Microsoft Azure, those features correspond to the software at manifest version 1493 and later. For features related to cloud-connected Horizon 7 pods, those features correspond to Horizon 7 at version 7.9 and Horizon 7 Cloud Connector 1.3 and later.</td>
</tr>
</tbody>
</table>

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 7
- VMware Cloud
- VMware Horizon® 7 Cloud Connector™
- VMware Unified Access Gateway™
- VMware Identity Manager™
- VMware Workspace™ ONE™
- VMware Horizon® Client™
- VMware Horizon® HTML Access™
- Microsoft Azure and its Marketplace
- Microsoft Active Directory
- VMware User 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.
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 Administration Console and clicking > Support.

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.
Introduction to Horizon Cloud

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 called a cloud-connected pod. You can then work with all of your cloud-connected pods and the available desktop-as-a-service features using the Horizon Cloud Administration Console.

**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 connected to the cloud control plane. Supported capacity environments are ones such as Microsoft Azure cloud or VMware Cloud™ on AWS or on-premises infrastructure.

Depending on the type of capacity you are using, you can use the Horizon Cloud Administration Console for an automated pod deployment and connection to Horizon Cloud. For some types of pods, even though they cannot be automatically deployed and configured, you can still connect Horizon Cloud to those pods that already exist. Then you can use the Administration Console with the cloud-connected pods after they are connected.

**Horizon Cloud Control Plane**

VMware hosts the Horizon Cloud control plane in the cloud. This cloud service enables the central orchestration and management of virtual desktops, remote desktop sessions, and remote applications for your users. The cloud service also manages your pods. The pods are physically located in your provided capacity environments. When you log in to the cloud service, you can see all of your 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.
The cloud control plane also hosts a common management user interface called the Horizon Cloud Administration Console, or Administration Console for short. The Administration Console runs in industry-standard browsers. It provides IT administrators with a single location for management tasks involving user assignments and the virtual desktops, remote desktop sessions, and applications. The Administration Console is accessible from anywhere at any time, providing maximum flexibility.

**Important** The Administration 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 Administration 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. The Administration Console dynamically reflects the elements related to such features only when your license includes use of such features.

When you are expecting to see a feature in the Administration Console and do not see it, contact your VMware account representative to verify whether your license entitles your use of that feature.

## 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 Administration Console for an automated deployment, your customer account must have the appropriate licensing. For licensing information, contact your VMware account representative.

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Horizon 7 pod located in your on-premises infrastructure</td>
<td>Deploy the Horizon 7 Cloud Connector in your on-premises infrastructure and configure it to connect that pod to Horizon Cloud.</td>
</tr>
<tr>
<td>VMware Horizon 7 pod that you manually installed and configured in your VMware Cloud on AWS SDDC</td>
<td>Deploy the Horizon 7 Cloud Connector in your VMware Cloud SDDC 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 Horizon Cloud Administration Console’s automated deployment wizard.</td>
</tr>
<tr>
<td>VMware Horizon 7 pod deployed by Horizon Cloud into your VMware Cloud SDDC</td>
<td>Deploy the pod using the Horizon Cloud Administration Console’s automated deployment wizard.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- **End-to-End Workflow When Your Very First Cloud-Connected Pod is from Deploying into VMware Cloud**
- **End-to-End Workflow When Your Very First Cloud-Connected Pod is from Connecting Horizon Cloud with an Existing Manually Deployed Horizon 7 Pod**
- **Suggested Workflow for When Your Very First Cloud-Connected Pod is from Deploying into Microsoft Azure**
End-to-End Workflow When Your Very First Cloud-Connected Pod is from Deploying into VMware Cloud

This is a high-level list of the steps for using the wizard in Horizon Cloud to make your very first cloud-connected pod by deploying a Horizon 7 pod into your VMware Cloud SDDC. 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 Directory domain, you can use the unified visibility, health monitoring, and help desk services features provided in this Horizon Cloud release.

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

1. Fulfill the prerequisites, as described in the separate prerequisites checklist document. You can open that document from this PDF link or navigate to it from the Horizon Cloud documentation landing page.

2. Perform the preparatory tasks outside of Horizon Cloud. See the Horizon Cloud Deployment Guide.

3. Deploy the pod. See Horizon Cloud Deployment Guide.

4. Register the pod's Active Directory domain with Horizon Cloud, which includes providing the name of domain-bind and domain-join accounts. See Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment.

5. 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 depend on the domain join account having the Horizon Cloud Super Administrators role. See Assign Horizon Cloud Administrative Roles to Active Directory Groups

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.

End-to-End Workflow When Your Very First Cloud-Connected Pod is from Connecting Horizon Cloud with an Existing Manually Deployed Horizon 7 Pod

This list is a high-level of the steps when you are making your very first cloud-connected pod by connecting to 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 VMware Cloud capacity. After these workflow steps are completed for your very first cloud-connected pod, you can use the Horizon Cloud Administration Console features for visibility, health monitoring, and help desk services with that pod. At that point, you can also deploy additional pods.
Before beginning this workflow, you must have already installed and configured your Horizon 7 pod. For information about manually installing a Horizon 7 pod that you can use with this Horizon Cloud release:

- For manually installing pods using on-premises capacity, see the relevant installation information for the most recent version of Horizon 7 from the Horizon 7 Documentation page.

- For manually installing pods using VMware Cloud capacity, see the best practices guide for deploying Horizon 7 on VMware Cloud, available from the Horizon 7 on VMware Cloud on AWS product page.

This Horizon Cloud release provides unified visibility, health monitoring, and help desk services in the Horizon Cloud Administration Console. Perform the following steps when you are deploying your very first cloud-connected pod and you are connecting to a manually deployed pod with which you want to use the Horizon Cloud features.

**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 7 pods before you can successfully complete the required Active Directory domain registration and Super Administrators role assignment step.

1. Fulfill the prerequisites. See the Horizon Cloud Deployment Guide.
2. Deploy the Horizon Cloud Connector into that pod environment. See the Horizon Cloud Deployment Guide.
3. Optionally configure a CA-signed certificate for the Horizon 7 Cloud Connector virtual appliance. See the Horizon Cloud Deployment Guide.
4. Register the pod's Active Directory domain with Horizon Cloud, which includes providing names of domain-bind and domain-join accounts. See Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment.
5. Give the Horizon Cloud Super Administrators role to an Active Directory group that includes that domain-join account as a member. See Assign Horizon Cloud Administrative Roles to Active Directory Groups.

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.

**Suggested Workflow for When Your Very First Cloud-Connected Pod is from Deploying into Microsoft Azure**

This is a high-level list of the steps for using the wizard in Horizon Cloud to make your very first cloud-connected pod by deploying a 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 Directory 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.

For an overall introduction to pods in Microsoft Azure, see Chapter 5 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 wizard to deploy it into Microsoft Azure.

1. Fulfill the prerequisites, as described in the separate prerequisites checklist document. You can open that document from this PDF link or navigate to it from the Horizon Cloud documentation landing page.

2. Perform the preparatory tasks outside of Horizon Cloud. See Getting Started with VMware Horizon Cloud Service on Microsoft Azure.

3. Deploy the pod. See Getting Started with VMware Horizon Cloud Service on Microsoft Azure.

4. 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.

5. 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 depend on the domain join account having the Horizon Cloud Super Administrators role. See Assign Horizon Cloud Administrative Roles to Active Directory Groups.

6. Upload SSL certificates to the pod directly, using the pod's summary page in the Administration Console, if you plan to have one or both of the following use cases:
   - Use VMware Identity Manager™ with the pod. When you use VMware Identity Manager™ with the pod, you must configure the VMware Identity Manager™ connector to point to the pod's manager VM.
   - Clients connecting directly to the pod's manager VM.
See Upload SSL Certificates to a Horizon Cloud Pod for Direct Connections.

**Note** Uploading the SSL certificate to the pod directly is not necessary when your end-user connections go to the Unified Access Gateway instances in the pod through the load balancer connected to those instances.

In general, uploading an SSL certificate to the pod directly is a recommended practice, because that ensures Horizon Clients that might make direct connections to the pod environment can have trusted connections, and is the supported configuration for using VMware Identity Manager™ with the pod. However, connections direct to the pod using HTML Access (Blast) appear as untrusted connections in the end user's browser. The end-user browsers display the typical untrusted certificate error when they make their connections direct to the pod. To have connections using HTML Access (Blast) avoid the displayed untrusted certificate error, you must have those connections use the load balancer and Unified Access Gateway instances from the pod's Unified Access Gateway configuration. If you do not want to expose your fully qualified domain name to the Internet, you can deploy an internal Unified Access Gateway configuration. This internal Unified Access Gateway configuration uses a Microsoft internal load balancer to which end users who are internal to your corporate network can point their connections.

7 Import a master image. See Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure.

8 Depending on whether your master image is for provisioning VDI desktops or for RDSH-based session desktops and RDSH-based remote applications, perform one or more of the following steps as appropriate.

- In a master image for VDI desktops, 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.
  - Install NVIDIA Graphics Drivers in a GPU-Enabled Master Image.

- In a master RDS-enabled server image 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.
  - Install NVIDIA Graphics Drivers in a GPU-Enabled Master Image.

9 Convert that master image into an assignable image, also known as sealing or publishing the image. See Convert a Configured Master Virtual Machine to an Assignable Image.
10 To provision session-based RDSH desktops and remote applications from a published master 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, Importing New Applications from an RDSH Farm Using Auto-Scan from Farm, and Create a Remote Application Assignment.

11 To provision VDI desktops from a published master VDI desktop image, create a dedicated or floating VDI desktop assignment. See Create a Floating VDI Desktop Assignment and Create a Dedicated VDI Desktop Assignment.

12 When a pod is deployed with a Unified Access 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's deployed Microsoft load balancer information.

   a 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 public FQDN. Your DNS server record maps that 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.

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

   b 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. Your DNS server record maps that 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   internal-load-balancer-private-IP

For details on how to locate the load balancer's public FQDN in the Administration Console, see Obtain the Pod's Load Balancer Information to Map in your DNS Server.

13 When a pod is deployed to have RADIUS two-factor authentication for a Unified Access Gateway configuration, you must configure your RADIUS system with the Unified Access Gateway configuration's corresponding load balancer IP address as a client allowed to make requests of that RADIUS system. The pod's Unified Access Gateway instances authenticate requests from the RADIUS system through that address.

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. For such cloud-connected pods, you can use the Horizon Cloud Administration Console for visibility, health monitoring, and help desk services with those pods.

For an overall introduction to Horizon Cloud, see the Deployment guide for this service level.

To perform administrative tasks in the environment, you use the cloud-based Administration Console. This user interface provides an integrated view and centralized access to manage virtual desktops and applications for delivery to your end users. The Administration Console works in an industry-standard Web browser. For the list of supported Web browser types and versions, see the Release Notes.

Depending on the type of capacity you have access to, you can use the Horizon Cloud Administration 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 connect the Administration Console to those pods that already exist, after performing some required connection steps.

**Important** The Administration 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 Administration 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. The Administration Console dynamically reflects the elements related to such features only when your license includes use of such features.

When you are expecting to see a feature in the Administration Console and do not see it, contact your VMware account representative to verify whether your license entitles your use of that feature.

Before you can perform administrative tasks on a Horizon Cloud pod, you must:

- Connect your first pod to Horizon Cloud. For details, see the Getting Started guide for this service level.
- Register at least one Active Directory domain and grant the Super Administrator role 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 Administration 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 an image from the Microsoft Azure Marketplace, creating farm server 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 7 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 7 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 7 on-premises and Horizon 7 in VMware Cloud on AWS pods using the Horizon 7 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 Cloud Connector cloud-pairing workflow for subsequent pods. Even though the Cloud 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 Cloud Connector's cloud-pairing workflow to remove the connection between each of the cloud-connected pods until you are down to a single cloud-connected pod.

2. Use the 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. Re-run the Cloud Connector 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. Registering additional Active Directory domains provides for user-related management tasks that involve users in those domains, such as working with the help desk features. 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 Administration Console, that domain is added to the set of cloud-configured Active Directory domains for your Horizon Cloud environment.

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
- Give Administrative Access to People in Your Organization
- Register Additional Active Directory Domains as Cloud-Configured Active Directory Domains
- Add Additional Auxiliary Bind Accounts for a Cloud-Configured Active Directory Domain
- Assign Horizon Cloud Administrative Roles to Active Directory Groups
- Join or Leave the Customer Experience Improvement Program
- Remove the Active Directory Domain Registration
- Upgrade Horizon 7 Cloud Connector Virtual Appliance

**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 7 Cloud Connector, in the case of Horizon 7 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 master VMs, farm server 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 the following 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 Administration Console. Main services are locked until you finish these tasks.

- Also, due to a known issue, when connecting Horizon 7 on-premises and Horizon 7 in VMware Cloud on AWS pods using the Horizon 7 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 Cloud Connector cloud-pairing workflow for subsequent pods. Even though the Cloud 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:
  
  a Use the Unplug action in the Cloud Connector's cloud-pairing workflow to remove the connection between each of the cloud-connected pods until you are down to a single cloud-connected pod.
  
  b Use the Administration Console to remove the failed registration, by following the steps in Remove the Active Directory Domain Registration.
  
  c Complete the first Active Directory domain registration process, related to that pod.
  
  d Re-run the Cloud Connector cloud-pairing 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 7 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.

**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 Administration 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 Administration 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 Administration Console and update the configuration to use an accessible domain-bind account.

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 Administration 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.

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 master 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 Administration 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 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 7 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. Open a browser to Horizon Cloud at [https://cloud.horizon.vmware.com](https://cloud.horizon.vmware.com).
2. Log in using the My VMware credentials associated with the Horizon Cloud environment.
   
   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.

   The Administration 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**.

3. In the Getting Started wizard, expand **General Setup** section if it is not already expanded.
4. Under Active Directory, click **Configure**.
5 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 7 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 7 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 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 7 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 7 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 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.                                                                                                                             |
You can optionally provide values for advanced properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>

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.

6 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.
7 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>
</table>
| **Primary DNS Server IP** | 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. |
| **Secondary DNS Server IP** | (Optional) IP of a secondary DNS Server                                                                                                    |
| **Default OU**       | Active Directory organization unit (OU) that you want used by the pod’s desktop-related virtual machines such as imported VMs, farm server 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.  
**Note** 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. |
| **Join Username**    | User account in the Active Directory that has permissions to join computers to that Active Directory domain.  
**Note** Only provide the user name itself. Do not include the domain name here. |
| **Join Password**    | The password associated with the name in the Join Username text box.                                                                         |
8. (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 server 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 server 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 Administration 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 server 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>Auxiliary Join Username</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>Auxiliary Join Password</td>
<td>The password associated with the name in the Auxiliary Join Username text box.</td>
</tr>
</tbody>
</table>

9. 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.
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 Administration Console.

This assignment ensures that at least one of your Active Directory domain’s user accounts is granted the permissions to log in at the second Administration Console login screen 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.

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: first 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.

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 Administration Console are now available.
- Signing in to the Administration Console to perform management tasks has two login screens: first a My VMware login to Horizon Cloud and then an Active Directory login using an account from the group with the super administrator role.
- Users in the group to which you granted the Super Administrator role will be able to access the Administration 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 Access to People in Your Organization.
- User accounts from the registered Active Directory domain can be selected for assignments involving resources from pods in Microsoft Azure.
- The Administration 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 Administration 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.

- 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 Access to People in Your Organization and Assign Horizon Cloud Administrative Roles to Active Directory Groups.

- 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 Administration Console to explore or perform other management tasks. See Tour of the Horizon Cloud Administration Console.

- If you have additional Active Directory domains with users to whom you want to grant management access to the Administration 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.

- Assign the demo administrator role to those users in this domain to whom you want to grant read-only access to the Administration Console. See Assign Horizon Cloud Administrative Roles to Active Directory Groups.

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 server instances, creating VDI desktop instances, and so on.

You use the Administration Console to provide the credentials for these accounts to Horizon Cloud.
You must ensure 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 of 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 Administration 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 will not be able to log in to the Administration Console and update the configuration.

  **Important** If both the primary and auxiliary domain bind accounts expire or become inaccessible, then you will not be able to log in to the Administration Console and update the configuration with working domain bind account information. If you choose not to set Never Expires on the primary or auxiliary domain bind accounts, you should make them have different expiration times. You will have to 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.

- At a minimum, the domain bind account must have read permissions which can look up AD accounts for all of the AD organizational units (OUs) that you anticipate using in the Desktop-as-a-Service operations that Horizon Cloud provides, such as assigning desktop VMs to your end users. The domain bind account needs the ability to enumerate objects from your Active Directory.

  **Important** The typical default settings in Active Directory give a standard domain user account the ability to do that enumeration. However, if you have limited the security permission in your Active Directory, you must ensure that the domain bind account has read permissions for all of the OUs and objects that you anticipate and expect you will use with Horizon Cloud.

### Domain Join Account Requirements

- The domain join account cannot change or be locked out.

- Ensure 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 Administration 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 server VMs and VDI desktop VMs will fail.

- The domain join account requires the sAMAccountName attribute.
- 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.

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 field 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 fields 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:

- List Contents [For Descendant Objects of Computer OU]
- Read All Properties [For Descendant Objects of Computer OU]
- Write All Properties [For Descendant Objects of Computer OU]
- Read Permissions [For Descendant Objects of Computer OU]
- Reset Password [For Descendant Computer Objects of Computer OU]
- Create Computer Objects [For Descendant Objects of Computer OU]
- Delete Computer Objects [For Descendant Objects of Computer OU]

**Caution** Notice that the Reset Password permission is slightly different from the others. Reset Password permission is specifically For Descendant Computer Objects.

For the other six permissions, setting Full Control might not work in all cases to satisfy the system's permission checking on the domain join account. Using Full Control and expecting it to satisfy the system's permissions checks might not always work.
Locating the Information Required for the 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 Administration Console's 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 Administration Console displays the Register Active Directory window. The following screenshot shows the top portion of the window.

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.
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 Administration 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.

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**.
Log in to the Horizon Cloud Administration Console

The Administration Console is a Web interface provided by the cloud service. You use an industry standard browser to log in to the interface. Some details of the login steps vary depending on the configuration of your specific environment.

**Note**  Login authentication into the Horizon Cloud Administration Console relies on My VMware account credentials. If the My VMware account system is experiencing a system outage and cannot take authentication requests, you will not be able to log in to the Administration Console during that time period. If you encounter issues logging in to the Administration Console’s first 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.

You first log in using the My VMware credentials of a My VMware account that has access permissions to your environment. The windows that display after the My VMware login window vary depending on the state of the pods associated with the My VMware account.

**Note**  If you have not logged in with the My VMware credentials and accepted the Horizon Cloud terms of service, a notification box about the terms of service displays after you click Login.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Window Displayed After the My VMware Login Window</th>
<th>What to Do Next</th>
</tr>
</thead>
<tbody>
<tr>
<td>First pod not yet deployed or paired with the cloud plane.</td>
<td>Getting Started wizard and the Capacity section</td>
<td>Deploy a pod or pair an existing pod with the cloud plane. For detailed steps, see Horizon Cloud Deployment Guide.</td>
</tr>
<tr>
<td>At least one pod deployed and paired, but no Active Directory domain configured in the cloud plane.</td>
<td>Getting Started wizard and the General Setup section</td>
<td>Perform the Active Directory registration procedure and assign the super administration role to a group of users, as described in Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment.</td>
</tr>
<tr>
<td>At least one Active Directory domain configured.</td>
<td>Active Directory login window displaying the name of the configured domain.</td>
<td>Log in using credentials for an account in the domain.</td>
</tr>
<tr>
<td>Multiple Active Directory domains configured.</td>
<td>Active Directory login window with a domain selection list.</td>
<td>Select a listed domain and log in using credentials for an account in the selected domain.</td>
</tr>
</tbody>
</table>

**Prerequisites**

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

When an Active Directory domain is already configured in the cloud plane for that My VMware account, verify that you have the credentials for an Active Directory account in that domain that has access permissions.

**Procedure**

2 Log in with your My VMware credentials.

The following screenshot illustrates the login screen, with credentials filled in.

![Welcome to VMware Horizon Cloud login screen](image)

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.

3 Depending on the options presented to you in the next window, complete the log-in sequence appropriate for your configured environment.

If the environment associated with the My VMware account has a cloud-configured Active Directory domain, the Active Directory login window appears and you must log in with Active Directory credentials.

The Administration Console appears.

**Note** If you mistype the Active Directory user name or password, the system re-displays 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 Administration 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 7 pods in your environment, you cannot change the 30 minutes default. See Edit General Settings.

Give Administrative Access to People in Your Organization

When signing in to the Administration Console, the first login screen requires an existing My VMware account that is associated with your Horizon Cloud environment. To give other users in your company or organization ability to log in to that first login screen, you associate the users’ My VMware accounts with your environment. You also associate each My VMware account with the Horizon Cloud role that is appropriate for their job role.

You associate My VMware accounts with your environment using either the My VMware Accounts area in the Getting Started wizard or the General Settings screen.

In addition to the Horizon Cloud role associated with an My VMware account, a person’s Active Directory user account should also have a Horizon Cloud role assigned through the Active Directory group to which they belong. The Horizon Cloud role assigned to the person's Active Directory account is what governs which Administration Console elements are accessible to a person after logging in with their Active Directory account at the Administration Console’s second login screen. For details, see Assign Horizon Cloud Administrative Roles to Active Directory Groups.

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 Administration Console. My VMware accounts are created using the registration process at https://my.vmware.com/web/vmware/registration.

Procedure

1 In the Administration 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.

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

If all of the added My VMware account IDs exist at vmware.com, they can be used to sign in to 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](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 Horizon Cloud Administrative Roles to Active Directory Groups.

---

### Register Additional Active Directory Domains as Cloud-Configured Active Directory Domains

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 domain, then you can use the Administration Console to work with users from that domain, such as in the help desk features or for desktop-related features from pods in Microsoft Azure.

**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.
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 Administration 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 Administration 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 Administration Console and update the configuration to use an accessible domain-bind account.

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 Administration 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.

Verify you have the Active Directory domain's NetBIOS name and DNS domain name. You will provide these values in the Administration 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 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 Administration 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 7 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 7 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 Register Active Directory Workflow's NETBIOS Name and DNS Domain Name Fields. |
| **DNS Domain Name** | - When you have cloud-connected Horizon 7 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 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><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 server 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. <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><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>
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 server 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 server 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 Administration 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 server 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>Auxiliary Join Username</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 <code>ouraccountname</code>, like the user logon name without the domain name. Entering slashes or at-signs will display an error.</td>
</tr>
<tr>
<td>Auxiliary Join Password</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.
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 Administration Console.

This assignment ensures that at least one of your Active Directory domain's user accounts is granted the permissions to log in at the second Administration Console login screen 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**.

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 Administration 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 Access to People in Your Organization.
- User accounts from the registered Active Directory domain can be selected for assignments involving resources from pods in Microsoft Azure.
- The Administration 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 Access to People in Your Organization and Assign Horizon Cloud Administrative Roles to Active Directory Groups.
Assign the demo administrator role to those users in this domain to whom you want to grant read-only access to the Administration Console. See Assign Horizon Cloud Administrative Roles to Active Directory Groups.

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

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 Administration 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 Administration 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.

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 Administration 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**.

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.

### Assign Horizon Cloud Administrative Roles to Active Directory Groups

Use the Administration Console's role-based access control to determine which administrative privileges are granted to which of your Active Directory user accounts. When logging in to the Administration Console, the second login screen uses the Active Directory account credentials. The system provides predefined roles that you can assign to your Active Directory groups.

These roles and their associated rights determine which management actions a user can perform using the Administration Console. The visibility of the Administration Console's features and elements is controlled by the role assigned to the person's Active Directory account. 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. You must assign a role to your organization's appropriate Active Directory groups before the users in that group can log in to the Administration Console's second login screen and access management actions.

**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 in 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 Administration 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><strong>Super Administrator</strong></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 perform management actions in the Administration 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><strong>Help Desk Administrator</strong></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 Administration 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>
<tr>
<td><strong>Help Desk Read Only Administrator</strong></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 Administration Console so that your Active Directory groups with this role can work with the user card features to see the status of end user sessions.</td>
</tr>
<tr>
<td><strong>Demo Administrator</strong></td>
<td>A read-only role that you can optionally assign to one or more groups. Demo administrators 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 Administration Console 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 Administration 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.

Procedure

1  In the Administration 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

If you want to give the same users access for the Administration Console's first login screen, add their My VMware accounts using the General Settings page. See Give Administrative Access to People in Your Organization for information.

The Administration Console's first login screen uses My VMware accounts, which are associated with the Horizon Cloud roles using the General Settings page. The second login screen uses Active Directory credentials, which are associated with the Horizon Cloud roles using this Roles & Permissions page.
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.

The CEIP appears the first time you log in to the 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. Log in to the Administration Console.

2. Click > CEIP.

3. Move the slider next to Join Customer Experience Improvement Program to No to leave CEIP or Yes to join.

   The default is Yes.

4. Click Save.

Remove the Active Directory Domain Registration

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.

In some situations, you might need or want to remove the Active Directory domain association from your customer account. Examples of such situations 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 Horizon Cloud customer account record in the cloud. However, because the information is incomplete, you find you cannot proceed to finish the domain registration using the Administration 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 7 Cloud Connector's onboarding workflow for multiple Horizon 7 pods using this Horizon Cloud customer record, before logging in to the Administration Console to complete the Active Directory domain registration process. The Horizon 7 Cloud Connector's onboarding workflow creates a partial configuration in Horizon Cloud of the Active Directory domains known to the Horizon 7 pods' Connection Servers. That partial configuration is completed when you perform the initial Active Directory domain registration workflow in the Administration Console. Due to a known issue in this release, connecting multiple Horizon 7 pods to Horizon Cloud prior to completing the registration workflow in the Administration Console can cause the registration workflow in the Administration Console 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 onboarding user interface and remove the partial Active Directory domain registration before attempting to register the domain.

The Administration 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.

- 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
  - Utility VMs listed on the Utility VMs 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 Administration 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**.

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

Log back in as described in Log in to the Horizon Cloud Administration Console.

Upgrade Horizon 7 Cloud Connector Virtual Appliance

To obtain the latest Horizon Cloud features for your cloud-connected Horizon 7 pods, you upgrade those pods' Horizon 7 Cloud Connector virtual appliance to the latest version applicable to Horizon Cloud.

Note  Proxy SSL configuration is not supported during an upgrade of the Horizon 7 Cloud Connector virtual appliance.

Prerequisites

- Download the most recent version of the Horizon 7 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 7 Cloud Connector virtual appliance and the existing Horizon 7 Cloud Connector virtual appliance that needs the upgrade are in the same network so that the new virtual appliance can establish an SSH communication with the existing virtual appliance.
- Use vSphere Web Client to take a snapshot of the existing Horizon 7 Cloud Connector virtual appliance.
- Obtain the static IP address, DNS address, gateway address, and subnet mask for the Horizon 7 Cloud Connector virtual appliance.
- When an Active Directory domain is already joined, verify that you have the credentials for an Active Directory account in that domain that has access permissions.
- Add the FQDN of the vCenter Server to the `/etc/hosts` file on the Horizon 7 Cloud Connector virtual appliance.

Procedure

1. In vSphere Web Client, power on the existing Horizon 7 Cloud Connector appliance.
   
   The Horizon 7 Cloud Connector appliance user interface IP address appears.

2. In a Web browser, enter the Horizon 7 Cloud Connector virtual appliance IP address to log in to the Horizon 7 Cloud Connector user interface.
   
   Use your My VMware account credentials to log in. This step verifies that the existing Horizon Cloud connection was successfully configured with the cloud-connected pod's Connection Server.

3. Deploy the latest version of the Horizon 7 Cloud Connector virtual appliance and use your My VMware account credentials to log in.

   Note  If the environment associated with the My VMware account has a joined Active Directory domain, the Active Directory login window appears and you must log in with Active Directory credentials.
4 Connect the latest version of the Horizon 7 Cloud Connector appliance that you just deployed with the appropriate Connection Server instance.

The previous version of the Horizon 7 Cloud Connector is connected to the cloud-connected pod's Connection Server instance. In the Connect to Horizon 7 Connection Server box, enter the FQDN of the Connection Server, and click Connect.

5 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 7 Cloud Connector actions, use a unique user name and password for the Connection Server.

7 Click Upgrade in the dialog box.

8 In the Old Cloud Connector address text box, enter the IP address of the earlier Horizon 7 Cloud Connector virtual appliance and then click Connect.

9 Click the check box to verify the thumbprint for the SSH connection.

10 Click Upgrade.

The cloud connection between the Horizon 7 pod and Horizon Cloud is successfully updated.

11 On the final wizard page, click Configure Virtual Center and specify vCenter Server settings.

This configuration enables support for Horizon Cloud to run maintenance actions on the virtual appliance, as needed for successful service operations.

   a 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.

   b Under Horizon Cloud Connector vCenter Server Credentials, enter the user name and password for vCenter Server.

   c Under Additional Static IP Details for Cloud Connector upgrade, enter the static IP, gateway, subnet mask, and DNS information that you gathered earlier for the Horizon 7 Cloud Connector virtual appliance.

   d Click Save.

**Troubleshoot the Horizon 7 Cloud Connector Virtual Appliance Upgrade**

The earlier version of the Horizon 7 Cloud Connector virtual appliance is disabled only at the end of the upgrade process. If there is any upgrade issue, you can roll back the upgrade to the earlier version of the Horizon 7 Cloud Connector virtual appliance.

*Note* When you perform any troubleshooting task, do not unplug the latest deployed version of the Horizon 7 Cloud Connector appliance.
Procedure

1. If the upgrade fails and the earlier version of the Horizon 7 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 7 Cloud Connector virtual appliance, you can perform the upgrade task again.

2. If the upgrade fails and the earlier version of the Horizon 7 Cloud Connector virtual appliance is not accessible, perform these steps:
   a. Power off the new Horizon 7 Cloud Connector virtual appliance.
   b. Revert the existing Horizon 7 Cloud Connector virtual appliance to the virtual appliance snapshot taken prior to the upgrade. Verify that the Horizon 7 Cloud Connector virtual appliance is accessible from the Web browser and displays the paired status.
   c. Perform the upgrade task to deploy the latest version of the Horizon 7 Cloud Connector appliance again. If the issue persists, contact VMware Support.
Unified Visibility, Health Monitoring, and Help Desk Operations Using the Horizon Cloud Administration Console

You use the Horizon Cloud Administration Console as the single pane of glass for working with your cloud-connected pods. The Administration Console provides a Dashboard page where you can see the health of those pods, a Capacity page where you can view the capacity levels of each pod, and a user-based search feature from which you can perform help desk operations to support your users.

Before you can use the Administration Console for these visibility, health monitoring, and help desk features, you must have in your Horizon Cloud environment a minimum of the following:

1. One cloud-connected pod
2. A completed Active Directory domain registration for at least one Active Directory domain to which that pod has line of sight
3. The Super Administrators role assigned to at least one group in that Active Directory domain

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

- End-to-End Workflow When Your Very First Cloud-Connected Pod is from Connecting Horizon Cloud with an Existing Manually Deployed Horizon 7 Pod
- Suggested Workflow for When Your Very First Cloud-Connected Pod is from Deploying into Microsoft Azure

Use the following topics and their subtopics to learn about the Administration Console, especially those features that provide for unified visibility, health monitoring, and help desk features.

This chapter includes the following topics:

- Tour of the Horizon Cloud Administration Console
- Dashboard Page
- Capacity Page
- Help Desk Features in Your Horizon Cloud Environment
## Tour of the Horizon Cloud Administration Console

The Horizon Cloud Administration Console is the user interface for your single point of control for managing and monitoring your Horizon Cloud environment and your cloud-connected pods.

### 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 Monitoring 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 Icon and topics Dashboard Page, Activity Page, Reports Page, and Notifications Page.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> In this release, this category's Activity and Reports pages apply only to pods in Microsoft Azure.</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 Icon.</td>
</tr>
<tr>
<td>Inventory</td>
<td>The Inventory category provides access to desktop-as-a-service artifacts from your pods in Microsoft Azure, 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 Icon.</td>
</tr>
<tr>
<td>Settings</td>
<td>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 Icon.</td>
</tr>
</tbody>
</table>

**Important** The Administration 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 Administration 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. The Administration Console dynamically reflects the elements related to such features only when your license includes use of such features.

When you are expecting to see a feature in the Administration Console and do not see it, contact your VMware account representative to verify whether your license entitles your use of that feature.

For example, in this release, some areas of the Administration Console are applicable only for pods deployed in Microsoft Azure. When your cloud-connected pods consist only Horizon 7 pods deployed on-premises or with VMware Cloud capacity, 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 7 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 Administration Console provides icons to access:

- **Notifications**. For more information, see [Notifications Page](#).
- The console’s search feature to search users or VMs. For more information, see [Using the Console’s Search Feature](#).
- Support-related information such as what's new in the current service level, Web-based documentation, build information, sending feedback, and requesting support.

**Dashboard Page**

This page is available from the **Monitor** icon and displays real-time metrics and health information about your overall environment, across all your Horizon Cloud cloud-connected pods.

The following screenshot illustrates the Dashboard page with four cloud-connected pods. Here there are two pods using Microsoft Azure capacity, one Horizon 7 on-premises pod, and one Horizon 7 pod using VMware Cloud capacity.
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 Global Footprint map along with two side tabs: Issues and Sessions. The map visually depicts your pods' geographic city locations and shows additional information when you hover on a location.

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.
The map displays differently and provides different information depending on whether the Issues or Sessions side tab is selected, as described below. The Issues tab is selected by default.

**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 location in the Location View.

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.

**Issues Tab Selected** When the Issues side tab is selected (as it is by default), the map has the title Global Footprint - Health and functions as described in this section.

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 under the list of pods opens the issue details window with a list of issues for that location. For more information about this window, see below.

The Issues side tab shows the total number of current issues at the top and lists the top five issues below. Hovering on an issue opens the pod information pop-up on the map for the location where the issue is occurring. Clicking on the **VIEW** link at the bottom of the tab opens the Global Footprint - Health issue list window.

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, as described below.

- 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 7 pods on-premises, the pod name is a link that you can click to launch Horizon Administrator for that pod's Horizon Connection Server.
- 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 lists issues related to user experiences.

Session Tab Selected (VDI & RDSH)

When the Sessions side tab is selected (as it is by default), the map has the title Global Footprint - Sessions and functions as described in this section.

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 the number of sessions for each, along with a pie chart of sessions by session type. Clicking on the VIEW link under the list of pods opens the Global Footprint - Sessions window for that location. For more information about this window, see below.

The top of the Sessions tab displays the number of end-user sessions to 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. Clicking on the VIEW link at the bottom of the tab opens the Global Footprint - Sessions window.

The Global Footprint - Sessions window contains a chart of sessions by session type and 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 \((\text{ActiveSessions} / \text{MaxPossibleSessions})\).

For your cloud-connected Horizon 7 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 7.7 pods.

**Capacity Page**

On the Capacity page, you can view and drill down to details such as status, location, capacity usage, and other information about your Horizon Cloud cloud-connected pods. Also from the Capacity page, you can add new locations and deploy pods into your available cloud capacity. The Capacity page is available from the **Settings** icon in the Horizon Cloud Administration Console.

The Capacity page gives you an overview of your cloud-connected pods, their status, and how they are doing in terms of utilization of their resources. The Capacity page is also an entry point to drill down into the details of a specific pod.
The Capacity page has two views, Location and Type. The Location view displays your pods in groupings according to the pods’ associated location information. The Type view displays your pods in groups according to the capacity types in which the pods are deployed (Microsoft Azure cloud capacity, VMware Cloud on AWS capacity, on-premises capacity). Both views display the following columns of information about each of your pods. When a particular pod type has no data applicable to a column, that column displays a hyphen (–). As an example, because on-premises Horizon 7 pods do not have subscription information associated with them, the Subscription column for a Horizon 7 pod displays a hyphen.

Table 3-1. Per-Pod Information Columns on the Capacity Page

<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 <a href="#">Health Statuses</a>.</td>
</tr>
<tr>
<td>Pod</td>
<td>Displays the name of the pod and an icon representing its type.</td>
</tr>
<tr>
<td>Version</td>
<td>For a pod in Microsoft Azure, this 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 7 pod, this displays the software version of the Horizon 7 Cloud Connector that connects the pod to Horizon Cloud.</td>
</tr>
<tr>
<td>State</td>
<td>For a Horizon 7 on-premises pod or a pod in VMware Cloud on AWS, this displays the state of the pod. In this release, a pod can be in either Monitored or Managed state.</td>
</tr>
<tr>
<td>Subscription</td>
<td>For a pod in Microsoft Azure, this displays the name of the subscription associated with that pod.</td>
</tr>
<tr>
<td>Column</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Desktop &amp; App Utilization</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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> In this release, the system reports desktop and application utilization only for pods in Microsoft Azure.</td>
</tr>
<tr>
<td></td>
<td>At the pod level, the Desktop &amp; App Utilization column displays the percentage calculated according to the following:</td>
</tr>
<tr>
<td></td>
<td>1 Summing all the active desktop and remote application sessions connect to the pod.</td>
</tr>
<tr>
<td></td>
<td>2 Summing all the potential desktop and remote application sessions the pod is configured to provide, based on its configured farm server and VDI desktop assignment session maximums.</td>
</tr>
<tr>
<td></td>
<td>3 Dividing the first sum by the second sum and multiplying by 100 to get a percentage value.</td>
</tr>
</tbody>
</table>
Health Statuses

The cloud monitoring service retrieves information about each of your cloud-connected 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.

**Unknown**
The cloud monitoring system cannot retrieve the health status from the pod. For a Horizon 7 pod, this status typically means the API call to that Horizon 7 pod cannot retrieve information, such as when the Horizon 7 Cloud Connector instance or the Connection Server instances are having issues and cannot provide the needed data.

Location View

In the Location view, the pods are grouped according to their associated locations. In this release, these locations are based on world city names. The system groups your pods by these locations, and uses the cities’ geographic coordinates to place icons representing your pods on the Global Footprint.

To view details about a particular pod, select View by Location and then click the pod’s name.

The following actions are available in the Location view.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New &gt; Location</strong></td>
<td>Specify a new location based on a world city name. In the City Name text box, start typing the name of a city. The system automatically displays world city names from its backend geography lookup table and you can choose a city from that list.</td>
</tr>
<tr>
<td><strong>New &gt; Pod</strong></td>
<td>Add a new pod. Use this action to deploy a pod after your initial one. For deploying pods using your Microsoft Azure cloud capacity, see Deploying Horizon Cloud Pods into Microsoft Azure from the Capacity Page. For deploying pods using your VMware Cloud capacity, see Run the Horizon Cloud Pod Deployment Wizard to Deploy the Pod into VMware Cloud.</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Select a location and click <strong>Edit</strong> to change to a different city name. In the City Name text box, start typing the name of a city. The system automatically displays world city names from its backend geography lookup table and you can choose a city from that list.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Select a location and click <strong>Delete</strong> to delete that location.</td>
</tr>
</tbody>
</table>

**Pod Details Page**

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 according to the pod type.
### Table 3-2. Pod Details Page According to Pod Type

<table>
<thead>
<tr>
<th>Pod Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon 7 on-premises</td>
<td>The page has a single tab named Summary and two buttons: <strong>Change State</strong> and <strong>Disconnect</strong>. If the pod is in Monitored state and meets certain requirements, you can change it to Managed state by clicking the <strong>Change State</strong> button. Ensure that the Horizon 7 pod is at version 7.9 or later. Ensure that the pod has been cloud-connected to Horizon Cloud using Horizon 7 Cloud Connector version 1.3 or later. You can use the <strong>Disconnect</strong> button to disconnect the pod from Horizon Cloud. See <a href="#">Disconnecting Pods</a>.</td>
</tr>
<tr>
<td>Horizon 7 in VMware Cloud on AWS</td>
<td>The page has a single tab named Summary and two buttons: <strong>Change State</strong> and <strong>Disconnect</strong>. If the pod is in Monitored state and meets certain requirements, you can change it to Managed state by clicking the <strong>Change State</strong> button. Ensure that the Horizon 7 pod is at version 7.9 or later. Ensure that the pod has been cloud-connected to Horizon Cloud using Horizon 7 Cloud Connector version 1.3 or later. You can use the <strong>Disconnect</strong> button to disconnect the pod from Horizon Cloud. See <a href="#">Disconnecting Pods</a>.</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>The page has the following tabs: Summary, System Activity, User Activity, and Audit Logs. You can use the action buttons on the pod's Summary tab to: Edit some of the pod's properties. Not all of its properties are editable. Delete the pod. Upload an SSL certificate to the pod. For steps, see <a href="#">Upload SSL Certificates to a Horizon Cloud Pod for Direct Connections</a>. Download logs, using the More &gt; Download Logs choice. If an update of the VMware pod software is available, schedule an update using the Update &gt; Schedule choice. The number displayed in the Version No 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.</td>
</tr>
</tbody>
</table>

---

### Type View

In the **Type** view, the pods are grouped according to their pod types. For pods in Microsoft Azure, the pods are further grouped by their associated subscription names. If a subscription does not have any associated pods, because those pods have been deleted, a Remove Subscription action is displayed in that subscription's row. See [Removing a Subscription Entry](#) for details.

In this view, for pods in Microsoft Azure, you can access the subscription information and limits for the subscriptions associated with each pod. The percentage of your Microsoft Azure subscription's quota that the pods in that subscription are using is displayed next to the subscription's name. Click the link to see more details about the pod's usage in terms of cores and Microsoft Azure VM family type.
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 Capacity page in the Administration Console. Then you can use the Capacity page to start adding additional cloud-connected pods.

In the Administration 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**, an information box opens and describes the requirement to download and install the Horizon 7 Cloud Connector. To connect an on-premises Horizon 7 pod requires you to
deploy that connector into your on-premises infrastructure and configure it to communicate with your Connection Server and with Horizon Cloud. For detailed steps for connecting an on-premises pod after you have downloaded the Horizon 7 Cloud Connector, see the Connect Horizon Cloud with an Existing Manually Deployed Horizon 7 Pod topic in the Horizon Cloud Deployment Guide.

- If you select **VMware Cloud on AWS** and your customer account has the appropriate licensing, that automated pod deployment wizard opens. You run the pod deployment wizard to deploy the pod's components into your VMware Cloud on AWS SDDC. For detailed steps, see Run the Horizon Cloud Pod Deployment Wizard to Deploy the Pod into VMware Cloud.

- If you select **VMware Cloud on AWS** and your customer account does not have the appropriate licensing, an information box opens and describes the requirement to download and install the Horizon 7 Cloud Connector. In this case, you can manually install a Horizon 7 pod in your VMware Cloud on AWS SDDC and use the Horizon 7 Cloud Connector to connect that pod to Horizon Cloud. For the steps to manually install that pod, see the VMware Horizon 7 on VMware Cloud on AWS Deployment Guide. Then follow the steps in the Connect Horizon Cloud with an Existing Manually Deployed Horizon 7 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. Start the pod deployment wizard in the Administration Console, 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)

   **1. Subscription**

   **2. Pod Setup**

   **3. Gateway Settings**

   **4. Summary**

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 Contributor role.

<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 <strong>Add New</strong> to enter new subscription information.</td>
</tr>
<tr>
<td>Subscription Name</td>
<td>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.</td>
</tr>
<tr>
<td>Environment</td>
<td>Select the cloud environment associated with your subscription, for example:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Azure</strong>, for the standard global Microsoft Azure cloud</td>
</tr>
<tr>
<td></td>
<td>- <strong>Azure - China</strong>, for the Microsoft Azure in China cloud</td>
</tr>
<tr>
<td></td>
<td>- <strong>Azure - Germany</strong>, for the Microsoft Azure Germany 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>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Directory ID</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>Application ID</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>Application Key</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>

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.
- Is the **Contributor** role configured on the application's service principal for the specified application ID.

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.

The following screenshot illustrates how this step's Identity Management area looks when a VMware Identity Manager™ tenant was already created during an earlier pod deployment for this customer account. You can have the pod deployer create a VMware Identity Manager™ tenant only once for the same customer account. When the VMware Identity Manager™ tenant has already been created during a previous pod deployment, you cannot change the **Identity Manager Tenant** toggle’s setting and the name of the existing tenant is displayed, as shown in the screenshot.

**Identity Management**

Identity Manager Tenant: ☐ NO 1 (Identity Manager Tenant with name la33idm already exists.)

[Cancel]  [Back]  [Next]
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Pod Name**                  | Enter a friendly name for this pod. This name is used in the Administration Console to identify this pod from your other pods.  
**Note** 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. |
| **Location**                  | 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 Administration 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.  
**Note** You must select a city from the system’s autocomplete list. |
| **Microsoft Azure Region**    | 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 [https://azure.microsoft.com/en-us/regions/services/](https://azure.microsoft.com/en-us/regions/services/) for details. |
| **Description**               | Optional: Enter a description for this pod.                                                                                                                                                              |
| **Virtual Network**           | Select a virtual network from the list.  
Only virtual networks (VNets) 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**       | Change this toggle to **Yes** 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 of the pod’s required subnets. |
| **Management Subnet**         | When **Use Existing Subnet** is set to **Yes**, **Management 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 management 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.  
When **Use Existing Subnet** is set to **No**, in **Management Subnet (CIDR)**, 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.  
**Caution** 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. |
<p>| <strong>Management Subnet (CIDR)</strong>  |                                                                                                                                                                                                          |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Subnet</td>
<td>When Use Existing Subnet is set to Yes, Desktop 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 desktop tenant subnet.</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 Use Existing Subnet is set to No, in Desktop Subnet (CIDR), enter a subnet address range (in CIDR notation) for the deployer to create a subnet to which all of this pod's VDI desktops and RDSH farm servers for end-user remote desktops and applications will get connected, 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 you enter is large enough to allow for accommodating the number of desktops you anticipate you will want this pod to provide. 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>
<tr>
<td>NTP Servers</td>
<td>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.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>If you require a proxy for outbound Internet connectivity, set this toggle to Yes 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 setting the toggle to Yes.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If your proxy server configuration requires a user name and password for authentication, provide those credentials also.</td>
</tr>
</tbody>
</table>
|                          | Use Proxy:  
|                          | Proxy:*  
|                          | Port:*  
|                          | Username:  
|                          | Password:  
|                          | Verify Password:  |

5 Proceed to the next step by clicking Next.

The following screenshot is an example of the next step when it is initially displayed.
To configure the pod with Unified Access Gateway and optionally RADIUS two-factor authentication, specify the information in this step for the configuration you want.

Complete the steps in the following topics:

- **Specify the Pod’s Gateway Configuration**
- **Specify Two-Factor Authentication Capability for the Pod**

If you do not want any Unified Access Gateway configuration on this pod, move the Enable External UAG to No.

The following screenshot is an example with this step completed.
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.

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 Unified Access Gateway configurations, you must configure your RADIUS system with the IP address of the Unified Access Gateway configuration's load balancer as a client allowed to make requests of that RADIUS system. The Unified Access Gateway instances authenticate requests from the RADIUS system through that address.

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'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.
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 subscription, you must perform the steps described in *Horizon Cloud 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 *Horizon Cloud Deployment Guide*, especially that the service principal has the Contributor role. You can navigate to the getting started document online from here.

- 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 *Horizon Cloud Deployment Guide*.

**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/ 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, Ports, Protocols Requirements for a Horizon Cloud Pod in Microsoft Azure.

- 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 Optionally Create the Pod's Required Subnets on your VNet in Microsoft Azure.

**Caution** The subnets you manually create on your VNet in advance for the pod deployment must remain empty. Do not put any resources on these subnets or otherwise use any of the IP addresses. If an IP address is already in use on the subnets, the pod might fail to deploy.

**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 When Deploying With a Unified Access Gateway Configuration

Caution  In the current release, you can only add the RADIUS two-factor authentication at the same time that you configure Unified Access Gateway on the pod. If you fail to choose the Enable 2-Factor Authentication? toggle for one of the Unified Access Gateway configurations, you will not be able to use the Administration Console later to add RADIUS two-factor authentication to the pod for that configuration (external or internal). For an already deployed pod, in the Edit Pod workflow, the Administration Console's Enable 2-Factor Authentication? toggle is disabled for the pod's existing Unified Access Gateway configuration.

<table>
<thead>
<tr>
<th>If you deploy with the Unified Access Gateway configuration as...</th>
<th>Later in the Edit Pod workflow, you...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both external and internal, but without RADIUS</td>
<td>Cannot add RADIUS to the pod</td>
</tr>
</tbody>
</table>
| External only, but without RADIUS                           | Cannot add RADIUS to that external Unified Access Gateway configuration.  
You will only be able to add the other, internal type of configuration. |
| Internal only, but without RADIUS                           | Cannot add RADIUS to that internal Unified Access Gateway configuration.  
You will only be able to add the other, external type of configuration. |

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. If you are going to deploy the pod with both the external and internal Unified Access Gateway configuration types and you want to use the same FQDN for both, you must determine how to route the incoming end-user client traffic to the appropriate load balancer. In this scenario, you need to set up the routing so that client traffic from the Internet is routed to the Microsoft Public Load Balancer and client traffic from your intranet is routed to the Microsoft Internal Load Balancer.

  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 Optionally Create the 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.

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 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 Pod's Gateway Configuration

In this step of the wizard, specify the information required to deploy the pod with Unified Access Gateway configured. When deploying the new pod, you can choose to have an external or internal Unified Access Gateway configuration, or both types on the same pod. By default, when this wizard step displays, Yes is selected for the external Unified Access Gateway configuration.

**Important** Keep in mind that in the current release, you can only add the RADIUS two-factor authentication at the same time that you configure Unified Access Gateway on the pod. If you fail to choose the Enable 2-Factor Authentication? toggle for your chosen Unified Access Gateway configuration, you will not be able to use the Administration Console later to add RADIUS two-factor authentication for that configuration. For an already deployed pod, in the Edit Pod workflow, the Administration Console's Enable 2-Factor Authentication? toggle is disabled for the pod's existing Unified Access Gateway configuration.

### If you deploy with the Unified Access Gateway configuration as...  
### Later in the Edit Pod workflow, you...

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both external and internal, but without RADIUS</td>
<td>Cannot add RADIUS to the pod</td>
</tr>
<tr>
<td>External only, but without RADIUS</td>
<td>Cannot add RADIUS to that external Unified Access Gateway configuration.</td>
</tr>
<tr>
<td></td>
<td>You will only be able to add the other, internal type of configuration.</td>
</tr>
<tr>
<td>Internal only, but without RADIUS</td>
<td>Cannot add RADIUS to that internal Unified Access Gateway configuration.</td>
</tr>
<tr>
<td></td>
<td>You will only be able to add the other, external type of configuration.</td>
</tr>
</tbody>
</table>

### External Unified Access Gateway configuration

The external Unified Access Gateway configuration gives the ability to provide access to desktops and applications for end users located outside of your corporate network. When the pod is deployed with an external Unified Access Gateway configuration, the pod includes a Microsoft Azure public load balancer and Unified Access Gateway instances deployed on the desktop tenant subnet to enable 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.

### Internal Unified Access Gateway configuration

An internal Unified Access 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 an internal Unified Access 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 is deployed with an internal Unified Access Gateway configuration, the pod includes a
Microsoft Azure internal load balancer and Unified Access Gateway instances deployed on the desktop tenant subnet to enable this access. In this case, the instances have two NICs each: one NIC on the management subnet and one NIC on the desktop subnet.

The following screenshot is an example of the step when it is initially displayed.

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 Unified Access Gateway configuration, complete the fields in the **External UAG** section.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable External UAG?</td>
<td>When <strong>Yes</strong> is selected, access to desktops and applications is enabled for users located outside of your corporate network. The pod includes a Microsoft Azure public load balancer and Unified Access Gateway instances to enable this access.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Leaving the default <strong>Yes</strong> setting is recommended.</td>
</tr>
<tr>
<td></td>
<td>When set to <strong>No</strong>, clients must either connect directly to the pod and not through Unified Access Gateway, or they connect through an internal Unified Access Gateway configuration. In the case of clients connecting directly to the pod and not through Unified Access Gateway, some post-deployment steps are required. In this case, after the pod is deployed, follow the steps in Upload SSL Certificates to a Horizon Cloud Pod for Direct Connections.</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.</td>
</tr>
<tr>
<td></td>
<td><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>DMZ Subnet</td>
<td>When <strong>Use Existing Subnet</strong> is set to <strong>Yes</strong> in the preceding 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></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 <strong>Use Existing Subnet</strong> is set to <strong>No</strong> 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 deployed public load balancer.</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 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</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 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>Certificate</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. The following screenshot is an example with this step completed.</td>
</tr>
</tbody>
</table>

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

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

   **Important** Keep in mind that in the current release, you can only add the RADIUS two-factor authentication for the external configuration at this same time that you are setting that external configuration. After the external configuration is set on the pod, the Administration Console disables the toggle for adding RADIUS two-factor authentication for that external configuration.
In the Internal UAG section, if you want the internal Unified Access Gateway configuration, set the Enable Internal UAG? toggle to Yes and complete the fields that appear.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Internal UAG?</td>
<td>When Yes is selected, trusted access to desktops and applications is enabled for HTML Access (Blast) connections for users located inside of your corporate network. The pod includes a Microsoft Azure internal load balancer and Unified Access Gateway instances to enable this access.</td>
</tr>
<tr>
<td>FQDN</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.</td>
</tr>
<tr>
<td>Important</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>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 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.</td>
</tr>
<tr>
<td></td>
<td>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>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 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>Certificate</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>

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

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

Important Keep in mind that in the current release, you can only add the RADIUS two-factor authentication for the internal configuration at this same time that you are setting that internal configuration. After the internal configuration is set on the pod, the Administration Console disables the toggle for adding RADIUS two-factor authentication for that internal configuration.

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. See Complete the Step 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 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>
</tbody>
</table>
| Routes         | 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. |

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. Set the **Enable 2 Factor Authentication** toggle to **Yes**.

   When the toggle is set to **Yes**, 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 set the toggle to **Yes** in the **External UAG** section.

   ![Screenshot of configuration fields](image)

   **2 Factor Authentication Settings**

   - **Enable 2 Factor Authentication?**
     - **Yes**
   - **2 Factor Auth Method**
     - **Add New Radius**
   - **Name**
   - **Properties**
     - **Display Name**
   - **Display Hint**

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><strong>Display Name</strong></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><strong>Display Hint</strong></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 <strong>Enter your DisplayHint user name and passcode</strong>, where <strong>DisplayHint</strong> 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 <strong>Example Company user name and domain password below</strong> for would result in a prompt to the end user that says <strong>Enter your Example Company user name and domain password below</strong> for user name and passcode.</td>
</tr>
<tr>
<td><strong>Name ID Suffix</strong></td>
<td>Even though this field is visible, it is not used in this release.</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>
</tbody>
</table>
| Maintain Username        | Select Yes to maintain the user's RADIUS username during authentication to Horizon Cloud. When Yes is selected:  
  - 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 you select No, the user is able to type a different user name in the login screen. |

**Note** 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 in the Horizon Cloud Administration Guide.

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>
</tbody>
</table>
| 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. |

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. Set the Auxiliary Server toggle to Yes and complete the fields as described in Step Primary Server section.
Optionally Create the Pod's Required Subnets on your VNet in Microsoft Azure

Instead of having the pod deployment process create the required subnets, you can create them in advance on your VNet.

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 desktop 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 has one or more Unified Access Gateway configurations, the Unified Access Gateway VMs also use IP addresses from this subnet.

**Important** The VMs for your VDI desktops, the RDS images, and every server in the pod's RDS farms consume these IP addresses. Because this desktop 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 will 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.

- If you are going to have an external Unified Access Gateway configuration, 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 when the external Unified Access Gateway configuration is specified in the deployment wizard. 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.

**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 your VNet that you are using for your pod deployment.
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>Name</td>
<td>Specify a name for the subnet.</td>
</tr>
<tr>
<td>Address range (CIDR block)</td>
<td>Type a CIDR for the subnet.</td>
</tr>
</tbody>
</table>

5. Click OK.
   The subnet is added to the VNet.
6. Repeat steps 3 through 5 to add the remaining required subnets.
   The VNet has the required subnets.

Caution The subnets you manually create on your VNet in advance for the pod deployment must remain empty. Do not put any resources on these subnets or otherwise use any of the IP addresses. If an IP address is already in use on the subnets, the pod might fail to deploy.

Run the Horizon Cloud Pod Deployment Wizard to Deploy the Pod into VMware Cloud

After your Horizon Cloud environment gets its very first cloud-connected pod and you have completed the Active Directory domain steps to register Horizon Cloud with the domain intended for that first pod, the Administration Console provides access to its Capacity page. At that point, you can subsequently deploy additional pods using the Capacity page. To deploy pods into your VMware Cloud SDDC after your very first ever cloud-connected pod, you run the pod deployment wizard from the Capacity page.

Note To use the automated wizard for deploying a pod into VMware Cloud, your Horizon Cloud customer account must have the appropriate licensing. For licensing information, contact your VMware account representative.

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 and have completed all of the required pre-deployment tasks. The items you need to provide in the wizard vary according to the pod configuration options you want. Those items also vary depending on whether you have existing pods created previously in VMware Cloud capacity using the Add VMware Cloud Capacity wizard or if your existing pod or pods are of different pod types, such as an on-premises pod or a pod in Microsoft Azure. This point is important: if your existing pods were created using the Add VMware Cloud Capacity wizard before, and you are reusing existing elements for this subsequent pod, such as:

- The VMware Cloud SDDC
- The same Active Directory domain configuration and the same accounts for the Active Directory administrator fields in the wizard

Then you might not have to perform some of the preparatory tasks.

If any of your existing pods were not previously created using the Add VMware Cloud Capacity wizard, then you must complete the preparatory tasks before running the wizard. See the topic Deployment Preparation when Your Very First Ever Horizon Cloud Pod is a Horizon 7 Pod into VMware Cloud Capacity and its subtopics for the detailed pre-deployment tasks.

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 Administration Console, start the pod deployment wizard.
   a. Open the Administration Console’s Capacity page by navigating to Settings > Capacity.
   b. Click New > Pod.

   The Add Capacity window opens.

2. In the Add Capacity window, click Select under VMware Cloud on AWS.

   The Add VMware Cloud on AWS Capacity wizard opens to the first step, which is VMware Cloud.

   The following screenshot illustrates the wizard open at its first step.
On the VMware Cloud tab, enter information as follows.

## VMware Cloud Authorization

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Cloud OAuth Refresh Token</td>
<td>Enter the VMware Cloud Refresh token you obtained earlier. (See <a href="#">Obtain Your Account API Token</a>)</td>
</tr>
<tr>
<td>Organization</td>
<td>This field auto-populates with your organization name.</td>
</tr>
<tr>
<td>SDDC</td>
<td>Select the SDDC you created earlier from the drop-down menu.</td>
</tr>
<tr>
<td>vCenter</td>
<td>This field auto-populates with your vCenter URL.</td>
</tr>
<tr>
<td>Have you changed the default vCenter Credentials?</td>
<td>If you have changed the default credentials on the vCenter, leave this set to Yes and enter the username and password in the fields below.</td>
</tr>
<tr>
<td></td>
<td>If you have not changed the default credentials, select No. The username and password fields below do not display.</td>
</tr>
<tr>
<td>vCenter Username</td>
<td>Enter vCenter username (field only displays if you selected Yes above).</td>
</tr>
<tr>
<td>vCenter Password</td>
<td>Enter vCenter password (field only displays if you selected Yes above).</td>
</tr>
<tr>
<td>Confirm vCenter Password</td>
<td>Re-enter vCenter password (field only displays if you selected Yes above).</td>
</tr>
</tbody>
</table>

**Note** After the fields above are populated, there might be a brief wait while the system validates required information.
Horizon Backend Network

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Backend Network</td>
<td>To create a new network:</td>
</tr>
<tr>
<td></td>
<td>a Click the Create link.</td>
</tr>
<tr>
<td></td>
<td>b (Optional) Edit one or both values in the dialog (Network Name and Subnet).</td>
</tr>
<tr>
<td></td>
<td>c Click OK.</td>
</tr>
<tr>
<td></td>
<td>A message appears indicating that the network has been created successfully, and the Horizon Backend Network field is populated with the name of the new network.</td>
</tr>
<tr>
<td></td>
<td>To reuse an existing network, select it from the Horizon Backend Network drop-down menu.</td>
</tr>
<tr>
<td></td>
<td>The Backend Network IP Pool field auto-populates with the selected network's information.</td>
</tr>
<tr>
<td>Note</td>
<td>If your Active Directory domain is not located in the current VMware Cloud (that is, in a peer VMware Cloud or on-premises), then you cannot create a new network. In this case, you must reuse the appropriate existing network to ensure that the VPN connection to your Active Directory will work.</td>
</tr>
<tr>
<td>Backend Network IP Pool</td>
<td>If you have created a new network, this field auto-populates when the network has been successfully created.</td>
</tr>
<tr>
<td></td>
<td>If you are reusing an existing network, enter IP pool information.</td>
</tr>
</tbody>
</table>

4 Configure the Deployer VM by performing the steps below.

Before beginning the steps, open a separate browser window or tab, log in to vCenter in your SDDC, and then open the vSphere Client. Do not exit the wizard or close the browser displaying it. You will need to move between the wizard and vSphere during the following procedure. For more information on deploying VMs in vSphere, see the VMware vSphere documentation.

a Under Configure Deployer at the bottom of the wizard page, do one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click the Download OVA link</td>
<td>to download the OVA file locally. If you choose this option, you will upload the file in vSphere in a future step.</td>
</tr>
<tr>
<td>Right-click the Download OVA</td>
<td>link and select Copy link address. If you choose this option, you will paste this URL in vSphere in a future step.</td>
</tr>
</tbody>
</table>

b In the vSphere Client, navigate to Cluster-1 in your SDDC data center.

c Right-click Compute-ResourcePool and select Deploy OVF Template.

The Deploy OVF Template dialog displays.

d On the first tab, Select an OVF template, do one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you downloaded the OVA file</td>
<td>locally in the earlier step, select the Local file radio button, click Choose Files, and upload the file. When the upload is complete, click Next.</td>
</tr>
<tr>
<td>If you copied the Download OVA</td>
<td>link address in the earlier step, paste the link address under URL and click Next.</td>
</tr>
<tr>
<td>If the Source Verification</td>
<td>dialog displays, click Yes.</td>
</tr>
</tbody>
</table>
f On the **Select a name and folder** tab, create a unique VM name based on the name pattern auto-populated in the **Virtual machine name** field. For example, if the name pattern is `hlcm-deployer`, you could make the unique name `hlcm-deployer-10`.

g In the selection tree, select **Workloads** and click **Next**.

h On the **Select a compute resource** tab, select Compute-ResourcePool, wait for the compatibility checks to complete, and click **Next**.

i On the **Review details** tab, confirm that all of the information shown is correct and click **Next**.

j On the **License agreements** tab, read the license agreement, and if you accept it check the box and click **Next**.

k On the **Select storage** tab, select WorkloadDatastore, wait for the compatibility checks to complete, and click **Next**.

l On the **Select networks** tab, under Destination Network select the Horizon Backend Network that you selected in the deployment wizard and click **Next**.

m Return to the Add VMware Cloud on AWS Capacity wizard. Click the **Copy Key** link under Configure Deployer.

n Return to the Deploy OVF Template dialog in vSphere. On the **Customize template** tab, paste the key you copied into the Activation_Key field and click **Next**.

o Do one of the following:

- If you had the wizard create a new backend network, click **Next**.
- If you reused an existing backend network, enter the appropriate values in the four fields under Networking Properties, and then click **Next**.

p On the **Ready to complete** tab, confirm that all of the information shown is correct and click **Finish**.

The Deployer VM you configured appears under Compute-ResourcePool in the tree on the left of the vSphere page.

q Click the Deployer VM and wait until the Deployer VM deploy task has completed. This process is displayed under Recent Tasks at the bottom of the page.

r Right-click the Deployer VM and select **Power > Power On**.

s Return to the Add VMware Cloud on AWS Capacity wizard. Wait until the green checkmark appears next to **Waiting for deployer** at the bottom of the page and click **Next**.

The Add VMware Cloud on AWS Capacity wizard displays the second step, which is Pod Setup.
5 On the Pod Setup tab, enter information as follows.

- **Details**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod Name</td>
<td>Enter a friendly name for this pod. This name is used in the Administration Console to identify this pod. <strong>Note</strong>: This name must be unique in your environment. It cannot match any pod listed on the Capacity page.</td>
</tr>
<tr>
<td>Location</td>
<td>Select an existing city name or click <strong>Add</strong> to specify a new city. The system groups your pods according to city name and depicts them on the Administration Console's Dashboard page's Horizon Global Footprint map. When you click <strong>Add</strong>, 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. <strong>Note</strong>: You must select a city from the system's autocomplete list.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description for this pod.</td>
</tr>
</tbody>
</table>

- **Active Directory Information**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Specify the domain name of your Active Directory domain that you configured for use with this pod. <strong>Note</strong>: The name you enter must be a valid fully-qualified host name. This domain must be reachable from all the other cloud-connected pods that are already in your Horizon Cloud environment. All cloud-connected pods in your environment must have line of sight to all of the Active Directory domains that are registered for this environment. Because these steps are for running this wizard when you already have at least one cloud-connected pod, at this point, your environment already has at least one registered Active Directory domain. The list of registered domains is in the Administration Console's Active Directory page.</td>
</tr>
<tr>
<td>Administrator Username</td>
<td>User name of an Active Directory service account. This service account must be a member of the Domain Admins group in the Active Directory you specify in <strong>Domain Name</strong>.</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Password of the account you specify in <strong>Administrator Username</strong>.</td>
</tr>
<tr>
<td>Confirm Administrator Password</td>
<td>Re-enter that password.</td>
</tr>
<tr>
<td>DNS Server IPs</td>
<td>Enter list of valid IP addresses, separated by commas.</td>
</tr>
</tbody>
</table>

- **Horizon Connection Server Information**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Server Name Pattern</td>
<td>Auto-populates with a default name pattern, which you can edit if you want.</td>
</tr>
<tr>
<td>Horizon Administrator Group</td>
<td>(Optional) Select the administrator group.</td>
</tr>
</tbody>
</table>
## Horizon Cloud Connector

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate for Connection Server 1</td>
<td>(Optional) Click the link and select a certificate.</td>
</tr>
<tr>
<td>Certificate for Connection Server 2</td>
<td>(Optional) Click the link and select a certificate.</td>
</tr>
</tbody>
</table>

## Windows Template / OVA

Leave the default value. Windows Server 2016 is the only template currently supported.

6. Click **Next**.

The Add VMware Cloud on AWS Capacity wizard displays the third step, which is App Volumes.

7. On the App Volumes tab, enter information as follows.

### App Volumes Manager Information

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Volumes Manager Name Pattern</td>
<td>Auto-populates with a default name pattern, which you can edit if you want.</td>
</tr>
<tr>
<td>Network</td>
<td>Auto-populates with the network name.</td>
</tr>
<tr>
<td>SQL Server</td>
<td>IP address of your SQL Server.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select Windows Integrated Authentication or SQL Server Authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: You should confirm that the Active Directory administrator has required permissions to access the SQL database.</td>
</tr>
<tr>
<td>Username</td>
<td>User name of an Active Directory service account. This service account must be a member of the Domain Admins group in the Active Directory domain you specified on the wizard's Active Directory tab.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of that Active Directory service account.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Re-enter that password.</td>
</tr>
<tr>
<td>Name of SQL Database</td>
<td>To use an existing database, enter the name of that database. To create a new database, enter a unique name for the new database.</td>
</tr>
<tr>
<td>Overwrite Existing database (if Any)</td>
<td>If you are using an existing database, leave the default value of No. If you are creating a new database, it is recommended that you select Yes to overwrite any existing database.</td>
</tr>
</tbody>
</table>

8. Click **Next**.

The Add VMware Cloud on AWS Capacity wizard displays the fourth step, which is Gateway Settings.
9 On the Gateway Settings tab, enter information as follows.

- **UAG Information**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAG Name Pattern</td>
<td>Auto-populates with a default name pattern, which you can edit if you want.</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Specify a password for the Unified Access Gateway administrator.</td>
</tr>
<tr>
<td>Confirm Administrator Password</td>
<td>Re-enter that password.</td>
</tr>
<tr>
<td>Certificate</td>
<td>(Optional) Click the link and select a certificate.</td>
</tr>
</tbody>
</table>

- **DMZ External Network**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Network</td>
<td>If you created a new Backend Network in the first step of the wizard (VMware Cloud tab), then you must create a new External Network as well. This option is selected for you and cannot be changed. If you reused an existing Backend Network in the first step of the wizard (VMware Cloud tab), then select an existing network from the External Network drop-down menu.</td>
</tr>
<tr>
<td>Network Name</td>
<td>If you are creating a new network, this field auto-populates with a default network name, which you can edit if you want. If you are reusing an existing network, this field does not display.</td>
</tr>
<tr>
<td>Subnet</td>
<td>If you are creating a new network, this field auto-populates with a default value, which you can edit if you want. If you are reusing an existing network, this field does not display.</td>
</tr>
<tr>
<td>External Network IP Range</td>
<td>Auto-populates with a range of IP addresses. You can edit these values, and must edit them if they are not contained in the network above. At least three IP addresses are required, and it is best to leave this as a range of 10 IP addresses to allow maximum flexibility for the future.</td>
</tr>
</tbody>
</table>

- **DMZ Internal Network**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Network</td>
<td>If you created a new Backend Network in the first step of the wizard (VMware Cloud tab), then you must create a new Internal Network as well. This option is selected for you and cannot be changed. If you reused an existing Backend Network in the first step of the wizard (VMware Cloud tab), then select an existing network from the Internal Network drop-down menu.</td>
</tr>
<tr>
<td>Network Name</td>
<td>If you are creating a new network, this field auto-populates with a default network name, which you can edit if you want. If you are reusing an existing network, this field does not display.</td>
</tr>
<tr>
<td>Subnet</td>
<td>If you are creating a new network, this field auto-populates with a default value, which you can edit if you want. If you are reusing an existing network, this field does not display.</td>
</tr>
<tr>
<td>Internal Network IP Range</td>
<td>Auto-populates with a range of IP addresses. You can edit these values, and must edit them if they are not contained in the network above. At least two IP addresses are required, and it is best to leave this as a range of 10 IP addresses to allow maximum flexibility for the future.</td>
</tr>
</tbody>
</table>
10 Click **Next**.

The Add VMware Cloud on AWS Capacity wizard displays the fifth step, which is Summary.

The system validates the following information:

- Active Directory
- Internet
- ESXi
- Capacity
- SQL Server
- vCenter
- IP Address

The system verifies the values you specified in the wizard and validates items such as whether it can reach your specified Active Directory domain and SQL Server. If any of these validations fails, the deployment is blocked until you make the necessary changes to information you entered in the wizard or to any environmental settings that caused the validation to fail. The exception is the capacity validation. If the validation of the capacity fails, the deployment can still go forward.

11 Confirm that all of the information displayed is correct. If necessary, you can return to earlier steps in the wizard by clicking the **Back** button, making changes, and then returning to the Summary tab.

12 When all of the information on the Summary tab is correct, click **Submit**.

The system takes 40 to 60 minutes to process the deployment, after which the pod will appear in the Administration Console.

**What to do next**

Perform all required post-deployment tasks, as described in **Post-Deployment Tasks After Deploying a Pod into VMware Cloud**.

**Deployment Preparation when Your Very First Ever Horizon Cloud Pod is a Horizon 7 Pod into VMware Cloud Capacity**

Before you log in to the Horizon Cloud Administration Console and run the Add VMware Cloud Capacity wizard for the first time, you must perform some preparatory tasks. The topics in this section describe both some information that is useful to have prior to preparing to deploy the pod and the preparatory tasks.

**Set Up the Software-Defined Data Center (SDDC) in VMware Cloud**

If you do not already have an existing VMware Cloud Software-Defined Data Center (SDDC) into which you want Horizon Cloud to deploy the pod, you must set one up before running the pod deployment wizard.
For useful background information about deploying and managing an SDDC in VMware Cloud, see the topic **Deploying and Managing a Software-Defined Data Center** and its subtopics in the VMware Cloud documentation set.

1. Set up the new SDDC, using the steps as described in the VMware Cloud documentation topic **Deploy an SDDC from the VMC Console**.

   Of the listed regions in that **Deploy an SDDC from the VMC Console** topic, for this Horizon Cloud release, you can use one the following regions:
   - Asia Pacific (Sydney)
   - Asia Pacific (Tokyo)
   - Europe (Frankfurt)
   - Europe (Ireland)
   - Europe (London)
   - US West (Oregon)
   - US East (N. Virginia)
   - US East (Ohio)
   - US West (N. California)
   - US West (Oregon)

2. As described in the VMware Cloud documentation topic **Deploying and Managing a Software-Defined Data Center**, when creating a multiple-host SDDC, you must associate that SDDC with an AWS account. That account association puts a requirement for additional configuration on the AWS virtual private cloud (VPC) associated with the SDDC. This additional configuration is needed for the automated pod deployment process. After you create the SDDC, you must ensure the Amazon S3 storage service in the same region in which you created the SDDC is accessible from the SDDC compute network and the SDDC vCenter. The configuration strategy you use depends on the network setup in the AWS VPC that you associated with the SDDC. The AWS documentation provides various options for configuring access to the Amazon S3 storage service. Examples out of the various options are:
   - Create an AWS VPC gateway endpoint for the Amazon S3 service. See
   - Set up an internet gateway for the AWS VPC and configure it for communication between the SDDC in your VPC and the Amazon S3 storage service. See **Internet Gateways** in the Amazon VPC documentation.

Network Configuration Options for the Pod in VMware Cloud

In the pod deployment wizard, you will select from two options for network configuration. This section provides criteria for deciding whether you want to have the deployment wizard automatically create new networks or use existing networks that were previously created in the SDDC, and then describes those two options.
The table below provides some guidance for which option to use, according to your chosen Active Directory configuration. For the list of Active Directory options you can use in this release, see Active Directory Domain Configuration Options for Deploying a Horizon 7 Pod in VMware Cloud.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Create New Networks</th>
<th>Use Existing Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory is located in the same VMware Cloud SDDC where you are deploying the Horizon 7 pod.</td>
<td>Supported (Preferred)</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>This method is preferred because the deployment process handles the network configuration automatically.</td>
<td>In this case, you must manually configure the networks prior to running the automated deployment process.</td>
</tr>
<tr>
<td>Active Directory hybrid deployment: Active Directory is located in your on-premises environment and connected to the VMware Cloud SDDC through the VPN/DX connectivity.</td>
<td>Not Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>You must perform the network configuration manually.</td>
<td>You must add the backend network into the VPN route (route accessible to the on-premises Active Directory).</td>
</tr>
</tbody>
</table>

Create New Networks

If you choose to have the deployment wizard create new networks for you, it creates the networks listed below with configurations as shown. This will happen automatically in the deployment wizard. There are no additional pre-deployment tasks to complete if you are choosing this option.

**Table 3-3. Networks**

<table>
<thead>
<tr>
<th>Network</th>
<th>Type</th>
<th>Gateway/PREFIX LENGTH (default values for new network)</th>
<th>DHCP</th>
<th>DHCP IP RANGE</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>HzE-10-backend</td>
<td>Routed</td>
<td>10.101.10.1/24</td>
<td>Enabled</td>
<td>10.101.10.230 - 10.101.10.250</td>
<td>DHCP supported</td>
</tr>
<tr>
<td>HzE-10-internal-DMZ</td>
<td>Routed</td>
<td>172.26.10.1/24</td>
<td>Disabled</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>HzE-10-external-DMZ</td>
<td>Routed</td>
<td>172.16.10.1/24</td>
<td>Disabled</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3-4. Groups**

<table>
<thead>
<tr>
<th>Group Type</th>
<th>Name</th>
<th>Member Type</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>HzE-10-backend</td>
<td>IP address</td>
<td>10.101.10.0/24</td>
</tr>
<tr>
<td>Workload</td>
<td>HzE-10-backend</td>
<td>IP address</td>
<td>10.101.10.0/24</td>
</tr>
<tr>
<td>Workload</td>
<td>HzE-10-internal-DMZ</td>
<td>IP address</td>
<td>172.26.10.0/24</td>
</tr>
<tr>
<td>Workload</td>
<td>HzE-10-external-DMZ</td>
<td>IP address</td>
<td>172.16.10.0/24</td>
</tr>
<tr>
<td>Type</td>
<td>Name</td>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------</td>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Gateway Firewall Management</td>
<td>gateway HLCM-10-backend-esxi-</td>
<td>HzE-10-backend</td>
<td>ESXi</td>
</tr>
<tr>
<td>Gateway Firewall Management</td>
<td>HLCM-10-backend-vCenter-</td>
<td>HzE-10-backend</td>
<td>vCenter</td>
</tr>
<tr>
<td>Gateway Firewall Management</td>
<td>HLCM-10-backend-vCenter-ICMP</td>
<td>HzE-10-backend</td>
<td>vCenter</td>
</tr>
</tbody>
</table>
| Gateway Firewall Management  | HLCM-10-backend-out-All     | HzE-10-backend  | ANY         | ANY           | Allow  | You can modify or remove this rule according to your own requirements.
| Distributed Firewall         | HLCM-10-backend-dmz-        | HzE-10-backend  | HzE-10-external-DMZ, HzE-10-internal-DMZ | ANY (All Traffic) | Drop   |                                                                       |

Use Existing Networks

To use networks that you create in the SDDC prior to beginning the pod deployment process, perform the network configuration as shown below.

**Note** If you choose to use existing networks, you must have created all of the networks described below on the AWS SDDC before you start the deployment process. Failure to do so will result in having to stop and create them before restarting the deployment process.
### Table 3-6. Networks

<table>
<thead>
<tr>
<th>Network</th>
<th>Type</th>
<th>Gateway/Prefix Length</th>
<th>DHCP</th>
<th>DHCP IP Range</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;backend network&gt;</td>
<td>Routed</td>
<td>&lt;Specify Gateway IP/Prefix length of the logical network, for example, 192.168.1.1/24&gt;</td>
<td>Enabled</td>
<td>&lt;Specify the IP range or subnet in CIDR format, for example, 192.168.1.200-192.168.1.220 or 192.168.1.128/25&gt;</td>
<td>Reserve more than 10 static IP addresses in this network</td>
</tr>
<tr>
<td>&lt;internal-DMZ network&gt;</td>
<td>Routed</td>
<td>&lt;Specify Gateway IP/Prefix length of the logical network, for example, 192.168.2.1/24&gt;</td>
<td>Disabled</td>
<td>NA</td>
<td>Reserve at least 2 available static IP addresses</td>
</tr>
<tr>
<td>&lt;external-DMZ network&gt;</td>
<td>Routed</td>
<td>&lt;Specify Gateway IP/Prefix length of the logical network, for example, 192.168.3.1/24&gt;</td>
<td>Disabled</td>
<td>NA</td>
<td>Reserve at least 3 available static IP addresses</td>
</tr>
</tbody>
</table>

### Table 3-7. Groups

<table>
<thead>
<tr>
<th>Group Type</th>
<th>Name</th>
<th>Member Type</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>&lt;backend network management group&gt;</td>
<td>IP address</td>
<td>&lt;Valid IP/CIDR/Range&gt;</td>
</tr>
<tr>
<td>Workload</td>
<td>&lt;backend network workload group&gt;</td>
<td>IP address</td>
<td>&lt;Valid IP/CIDR/Range&gt;</td>
</tr>
<tr>
<td>Workload</td>
<td>&lt;internal-DMZ network workload group&gt;</td>
<td>IP address</td>
<td>&lt;Valid IP/CIDR/Range&gt;</td>
</tr>
<tr>
<td>Workload</td>
<td>&lt;external-DMZ network workload group&gt;</td>
<td>IP address</td>
<td>&lt;Valid IP/CIDR/Range&gt;</td>
</tr>
</tbody>
</table>
### Table 3-8. Firewall Rules

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Applied To</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Firewall Management</td>
<td>&lt;backend network&gt;-esxi-HTTPS</td>
<td>&lt;backend network workload group&gt;</td>
<td>ESXi</td>
<td>HTTPS (TCP 443)</td>
<td>Allow</td>
<td>NA</td>
<td>HLCM-10-backend-esxi-HTTPS is forbidden for use as Edge Firewall Management Gateway name.</td>
</tr>
<tr>
<td>Gateway Firewall Management</td>
<td>&lt;backend network&gt;-vCenter-HTTPS</td>
<td>&lt;backend network workload group&gt;</td>
<td>vCenter</td>
<td>HTTPS (TCP 443)</td>
<td>Allow</td>
<td>NA</td>
<td>HLCM-10-backend-vCenter-HTTPS is forbidden for use as Edge Firewall Management Gateway name.</td>
</tr>
<tr>
<td>Gateway Firewall Management</td>
<td>&lt;backend network&gt;-vCenter-ICMP</td>
<td>&lt;backend network workload group&gt;</td>
<td>vCenter</td>
<td>ICMP (All ICMP)</td>
<td>Allow</td>
<td>NA</td>
<td>HLCM-10-backend-vCenter-ICMP is forbidden for use as Edge Firewall Management Gateway name.</td>
</tr>
</tbody>
</table>
### Hurricane Lane Cloud Management (HLCM)

**HLCM-10**

**Name**: backend-out-All

**Source**: <backend network workload group>

**Destination**: ANY

**Service**: ANY (All Traffic)

**Action**: Allow

**Applied To**: All uplinks

**Notes**: HLCM-10-backend-out-All is forbidden for the user to use as Edge Firewall Compute Gateway name. You can modify or remove this rule according to your own requirements.

### Distributed Firewall Environment Rules

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Applied To</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Firewall Environment Rules</td>
<td>Example: &lt;backend network&gt; - dmz-All</td>
<td>&lt;backend network workload group&gt;</td>
<td>&lt;internal-DMZ network workload group&gt;</td>
<td>ANY (All Traffic)</td>
<td>Drop</td>
<td>NA</td>
<td>This is an optional configuration.</td>
</tr>
</tbody>
</table>

**Obtain Your Account API Token**

In the first step of the deployment wizard, you must provide an API token that you obtain from your VMware Cloud Services account. This API token provides for the deployer to make secure authorized API connections. The deployer uses secure API connections to deploy and configure the VMware Horizon 7 on VMware Cloud on AWS software environment in your vSphere data center.

This API token from your VMware Cloud Services account was previously called an OAuth refresh token. This API token authorizes access per organization, not across all of your organizations.

**Note**: It is recommended that you check on the following issues.

- There is a separate refresh token for each VMware Cloud Services organization. Confirm that you are getting the refresh token for the correct organization.
- Confirm that your account has the necessary privileges to access VMware Cloud Services. These include NSX Cloud Admin and Administrator.
Prerequisites

You must be able to log in to the VMware Cloud Services portal. To obtain the required API token, you navigate to your account information in that portal and locate the API Tokens area within your account information. That API Tokens area displays the required refresh token.

Procedure

1. Log in to the VMware Cloud Services portal with your VMware Cloud Services account credentials.
2. On the portal's toolbar, click your user name and My Account > API Tokens.
3. In that API Tokens area, locate the organization that you want to use for the deployed environment.
4. Copy the existing refresh token using the displayed copy-to-clipboard action.
   If you do not see a refresh token, then generate a new token.
5. Paste the copied refresh token to a location where you can retrieve it for pasting into the required deployment wizard field.

Active Directory Domain Configuration Options for Deploying a Horizon 7 Pod in VMware Cloud

A Horizon Cloud environment requires registering at least one Active Directory domain with the cloud-connected pods in that environment. When using the wizard to automatically deploy a Horizon 7 pod into VMware Cloud, you must provide information about the Active Directory configuration you are going to use with that pod.

Important  Your Horizon Cloud environment can consist of Horizon 7 pods in VMware Cloud, Horizon 7 pods on-premises, and pods in Microsoft Azure. As a result, all of those cloud-connected pods must have line of sight to the same set of Active Directory domains. If your environment already has cloud-connected pods and you are using the Add Capacity wizard for the first time to automatically deploy a pod into VMware Cloud, you must ensure this pod will be able to have line of sight to the Active Directory domains that are already registered with your Horizon Cloud environment. See the Active Directory-related topics in the Horizon Cloud Administration Guide for more details.

In this release, for deploying the pod in VMware Cloud, you can choose from the following options.

- Active Directory inside your VMware Cloud environment - Set up by logging into the VMware Cloud vCenter and installing Microsoft Active Directory on a new virtual machine (VM).
- Active Directory in your on-premises environment via VPN or Direct Connect - Set up by configuring a VPN or Direct Connect between the VMware Cloud environment and the on-premises environment where the Active Directory is running.
- Active Directory in a peer VMware Cloud environment via VPN - Set up by configuring a VPN between the VMware Cloud environment where the Horizon 7 pod is located and the peer VMware Cloud environment where the Active Directory is running.

Note  The Active Directory must be network accessible from the VMware Cloud SDDC.
The following links provide additional information that may be helpful:

- Microsoft Active Directory requirements
- Preparing Active Directory in the Horizon 7 documentation

**Note** Not all information in the links above is relevant for this deployment.

**Set Up SQL Server**
You must set up a SQL Server your VMware Cloud environment before using the automated deployment wizard to deploy the pod into your VMware Cloud SDDC. The pod's App Volumes feature uses SQL Server. One of the pod's deployment steps is to install App Volumes Manager, and App Volumes Manager requires a database.

For the pod's successful deployment and ongoing operations, your SQL Server configuration must meet the following requirements:

- **Location** - SQL Server must be in the same SDDC as the Horizon components.
- **Software requirements.** See Software Requirements in the App Volumes Installation Guide.
- **If you are going to specify Windows Authentication for SQL Server, you must provide a domain account that belongs to the Domain Admins group. This account is used by the pod deployer to run the App Volumes Manager install process, and App Volumes Manager creates a database in SQL Server using this domain account.**

To set up a SQL Server in your VMware Cloud environment:

1. In your VMware Cloud vCenter, create a new Windows VM and install Microsoft SQL Server.
   - Select either failover clustering or an always-on solution, based on your own preference.
   - Configure SQL to use either Server Authentication or Windows Authentication, based on your own preference.
     - If you are using Server Authentication, configure it by performing the following steps.
       a. In the Microsoft SQL Server Management Studio, select **Security > Logins** in the Object Explorer.
       b. Open Properties for the 'sa’ login.
       c. Select the Enabled radio button under Login.
       d. Click **OK** to save.
   - If you are using Windows Authentication, be sure to perform the optional step below to join the SQL Server to the Active Directory.

2. Enable remote server connections for your SQL Server:
   - b. On the Connections page of the Server Properties dialog, check the check box for 'Allow remote connections to this server'.
3 Enable and configure the TCP/IP protocol and set its properties:
   a In the SQL Server Configuration Manager, select SQL Server Network Configuration > Protocols for MSSQLSERVER in the tree on the left of the screen.
   b Confirm that Status for TCP/IP is Enabled.
   c Open properties for TCP/IP and navigate to the IP Addresses tab.
   d Under IP2, confirm that the IP Address is set to the IP address for your VM.
   e Under IPAll, confirm that TCP Port is set to 1433.
   f Click OK to save.

4 (Optional) If you are using Windows Authentication, join the SQL Server to the Active Directory.
   a In the Microsoft SQL Server Management Studio, select Security > Logins in the Object Explorer.
   b Add the domain account that App Volumes Manager installer will use to log in to the SQL Server and create its required database. This domain account must belong to the Domain Admins group.

5 Restart the VM.

**Note**
- Be sure to keep network latency to the SQL server low, in conformity with the App Volumes deployment requirements. For example, you can set up the SQL server in the same SDDC or on AWS in the same AWS region. For database setup guidelines, see VMware App Volumes 2.x Database Best Practices.
- It is very important that you set up your SQL server as described in the steps above to obtain proper functioning of your new pod in VMware Cloud.

**Optional: Obtain an SSL Certificate for UAG and Connection Server**

You can obtain a signed SSL certificate from a Certification Authority (CA) for the Unified Access Gateway and Horizon Connection Server. There is an option to select a certificate in the deployment wizard.

Follow the normal process to obtain the certificate, as described in VMware documentation. For example, here.

**Note**  PKCS#12 (PFX) format is required.

**Post-Deployment Tasks After Deploying a Pod into VMware Cloud**

This section describes the tasks you must perform after using the automated deployment wizard to deploy a pod into your VMware Cloud SDDC.

**Note**  Confirm that you have completed the entire deployment process before proceeding with the tasks below.
Some of these tasks are needed only when the deployed pod is your very first ever pod deployment in your Horizon Cloud environment.

**Configure Windows Licenses in the Horizon Environment**

After the deployment is complete, your SDDC will have five new Windows 2016 VMs installed: two Horizon Connection Server VMs and three App Volumes Server VMs. You must log into each of these VMs and configure the appropriate license. It is your responsibility to provide the necessary Windows Server licenses. Refer to the Microsoft product documentation about the pricing and licensing terms for Windows Server 2016.

**Register the Specified Active Directory Domain if it is Not Already Registered with Your Horizon Cloud Environment**

All of the cloud-connected pods in your environment must have line of sight to all of the cloud-registered Active Directory domains. In the pod deployment wizard, you specified an Active Directory domain.

Perform one of the following options, as appropriate:

- If this pod deployment was for your very first ever pod in your Horizon Cloud environment, after the pod deploys, the only page in the Administration Console is the Getting Started page. Register that Active Directory domain by expanding the General Setup section of that page and click **Configure**. For the detailed steps, see Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment.

- If this pod deployment was for deploying a pod after you already have existing pods in your environment, but the Active Directory domain you specified in the wizard is not already one of the domains on the Administration Console's Active Directory page, navigate to that page and register the domain. For a successful registration, all of the existing pods must already have line of sight to that domain.

**Obtain the Unified Access Gateway Floating IP Address for End-User Connections**

If you deployed the pod with the Unified Access Gateway configuration, before your end users can access their desktops or remote applications, you must set up the appropriate CNAME records in your DNS server that maps the deployed configuration's floating IP address to the FQDN that your end users will use to make their connections. That FQDN should be the same one that you entered in the deployment wizard and which was in the certificate that you specified in the deployment wizard. The following code line demonstrates an example of the DNS server mapping, where `UAG-floating-IP-address` is the floating IP address. Your DNS server record maps the floating IP address with the FQDN that your end users will use, and which is used in the uploaded certificate.

```
ourApps.ourOrg.example.com UAG-floating-IP-address
```

To obtain the configured floating IP address, see Obtain the Horizon 7 Pod's Unified Access Gateway Floating IP Address to Map in your DNS Server.
Access the Deployed Horizon 7 Pod's Unified Access Gateway Admin User Interface

If you deployed the pod with Unified Access Gateway configured, you might want to access the Unified Access Gateway admin user interface for the Unified Access Gateway instances to view configuration settings and customize options for your needs. For steps, see Accessing the Admin User Interface for the Deployed Pod's Unified Access Gateway Instances.

Obtain the Horizon 7 Pod's Unified Access Gateway Floating IP Address to Map in your DNS Server

When a Horizon 7 pod deployed in VMware Cloud is deployed with the Unified Access Gateway configuration, before your end users can access their desktops or remote applications, you must set up the appropriate CNAME records in your DNS server that maps the deployed configuration's floating IP address to the FQDN that you entered in the deployment wizard. That FQDN should be the same one that you entered in the deployment wizard and which was in the certificate that you specified in the deployment wizard.

By default, the deployer process deploys and configures the Unified Access Gateway instances in a high availability (HA) configuration that uses two Unified Access Gateway instances and the Unified Access Gateway internal load balancer with a floating IP address.

In the pod 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.

Your DNS server must map the FQDN to the floating IP address of the Unified Access Gateway internal load balancer. 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.

The following code line demonstrates an example of the DNS server mapping, where UAG-floating-IP-address is the floating IP address.

```
ourApps.ourOrg.example.com UAG-floating-IP-address
```

This floating IP address is displayed in the Administration Console's Notifications page after the pod is successfully deployed.

**Prerequisites**

Verify your Horizon 7 pod is successfully deployed using the automated wizard and you have completed the appropriate post-deployment tasks, as described in Post-Deployment Tasks After Deploying a Pod into VMware Cloud.

**Procedure**

1. In the Administration Console, navigate to Monitor > Notifications.
2 Look for a notification labeled Horizon UAG Access.

The notification contains the floating IP address. The following screenshot is an example to illustrate the type of notification to look for. In this example, the floating IP is 172.16.10.12.

![Horizon UAG Access](https://172.16.10.12)

3 In your DNS server, map that floating IP address to the FQDN that was provided in the wizard when the pod was deployed.

ourApps.ourOrg.example.com UAG-floating-IP-address

Accessing the Admin User Interface for the Deployed Pod's Unified Access Gateway Instances

When you deploy the Horizon 7 pod with the Unified Access Gateway configuration, you might want to perform administrative tasks on its Unified Access Gateway instances, such as uploading certificates to each instance. To perform such tasks, you access each instance's admin user interface. Because the deployment process deploys the pod's Unified Access Gateway instances using a two-NIC deployment, you must follow these steps to access an instance's admin user interface using a jump box virtual machine (VM) that you deploy into the pod's internal-DMZ network and that instance's IP on that internal-DMZ network.

By default, the deployer process deploys and configures the Unified Access Gateway instances in a high availability (HA) configuration and using a two-NIC deployment. This HA configuration uses two Unified Access Gateway instances, the Unified Access Gateway internal load balancer with a floating IP address, and two network interface cards (NICs) on each Unified Access Gateway instance. The deployer also enables the Unified Access Gateway High Availability feature. Detailed information about this type of Unified Access Gateway configuration is available in the following Unified Access Gateway 3.5 product documentation topics.

- The two-NIC Unified Access Gateway configuration is described in DMZ Design for Unified Access Gateway with Multiple Network Interface Cards. The two-NIC configuration separates the unauthenticated user traffic from the back-end and management traffic.
The Unified Access Gateway High Availability feature is described in Unified Access Gateway High Availability.

The pod’s networks are described in Network Configuration Options for the Pod in VMware Cloud.

In this deployed configuration, each Unified Access Gateway instance has a NIC is connected to the internal-DMZ network and the other NIC is connected to the external-DMZ network. To access an instance's Unified Access Gateway admin user interface, you need to perform these steps by logging in to your VMware Cloud environment and accessing the SDDC.

You can delete the jump box VM when you no longer need it.

**Prerequisites**

Verify your Horizon 7 pod is successfully deployed using the automated wizard and you have completed the appropriate post-deployment tasks, as described in Post-Deployment Tasks After Deploying a Pod into VMware Cloud.

Verify that you can connect to the SDDC's vCenter Server using the vSphere Client. Before deploying the pod, you created that SDDC as described in Set Up the Software-Defined Data Center (SDDC) in VMware Cloud. For the steps for opening the vSphere Client and logging in to the SDDC's vCenter Server, see the Connect to vCenter Server topic in the VMware Cloud documentation.

**Procedure**

1. Obtain the IP address that the Unified Access Gateway instance has on the internal-DMZ network.

   You need to know this IP address to access that instance's admin user interface. The pod’s internal-DMZ network is described in Network Configuration Options for the Pod in VMware Cloud.

2. Deploy a jump box VM on the internal DMZ network.

   This Windows VM will serve as the jump box VM that can communicate with the Unified Access Gateway instances using their NIC connections to the internal-DMZ network.

   a. Connect to the vCenter Server for the pod's SDDC.

   b. In that vCenter Server environment, create a new Windows VM with the VM network as the internal DMZ network.

      If you selected to have the pod deployer create the networks, the internal DMZ network is named with the pattern HzE-10-internal-DMZ, as described in Network Configuration Options for the Pod in VMware Cloud.

      **Note** Make sure the VM's Windows operating system will have an up-to-date browser. The Unified Access Gateway admin user interface works best in the most current version of the browser. For the browsers supported for that admin user interface, see Unified Access Gateway System and Network Requirements in the Unified Access Gateway documentation.

3. When the new VM is created, log in to its operating system.
In the VM's operating system, open the instance's Unified Access Gateway admin user interface by using a browser to navigate to https://UAG-instance-IP-on-internal-DMZ-network:9443/admin/index.html, where *UAG-instance-IP-on-internal-DMZ-network* is that IP address from step 1.

**Restarting a Failed Deployment**

If your VMware Horizon® 7 on VMware Cloud™ on AWS pod deployment fails, you can restart it, but you must clean up your environment first.

Before you restart a failed deployment, first do the following:

1. Shut down all VMs deployed under the HzE-10-backend resource pool (HzE-avm-1, HzE-avm-2, HzE-avm-3, HzE-cc, HzE-cs-1, HzE-cs-2, HzE-uag-1, HzE-uag-2).
2. Delete all VMs under the HzE-10-backend resource pool (HzE-avm-1, HzE-avm-2, HzE-avm-3, HzE-cc, HzE-cs-1, HzE-cs-2, HzE-uag-1, HzE-uag-2).
4. Delete the VM Folder named HzE-10-backend.
5. Check if the auto-generated Content Library (hlcm_subscribed_private_10) has been deleted. If not, delete the Content Library manually.
6. Shut down the Deployer VM.
7. Delete the Deployer VM.
8. (Optional) If the networks have been created by the HLCM service, delete network configurations as follows:
   a. Firewall rules: HLCM-10-backend-esxi-HTTPS, HLCM-10-backend-vCenter-HTTPS, HLCM-10-backend-vCenter-ICMP, HLCM-10-backend-out-All
   b. Management Groups: HzE-10-backend
   c. Workload Groups: HzE-10-backend, HzE-10-external-DMZ, HzE-10-internal-DMZ
   d. Network Segments: HzE-10-backend, HzE-10-external-DMZ, HzE-10-internal-DMZ

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

The Administration 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 Administration Console for your help desk administrators, they can log in to the Administration Console 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 server instances to identify issues that might potentially impact the sessions.

In the Administration Console, the following items support performing those help-desk-related tasks:

- Give your help desk workers’ My VMware accounts to the Administration Console access list, with the appropriate help-desk-related role. The first login screen when logging in to the Administration Console 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 Administration Console’s General Settings page or the Getting Started page. For the steps, see [Give Administrative Access to People in Your Organization](#).

- Give your help desk workers’ Active Directory accounts the appropriate Horizon Cloud help-desk-related role. The second login screen when logging in to the Administration Console uses 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 Horizon Cloud Administrative Roles to Active Directory Groups](#).

  **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 Administration 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 server 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 Horizon Cloud Administration 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 field. When you have typed at least three (3) characters in the search field, names that begin with those characters are displayed. You can continue typing in 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 on a user or a VM:

- For a user, the card for that user is displayed. For details, see The User Card in the Horizon Cloud Administration Console.
- 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.

The User Card in the Horizon Cloud Administration Console

Use the Horizon Cloud Administration Console's user card feature as a dashboard to work with a specific user's assigned resources, such as that user's desktops.

You use the Administration 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 Horizon Cloud Administration Console](#).

<table>
<thead>
<tr>
<th>User Card Tabs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sessions</strong></td>
<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 <a href="#">Actions You Can Take on Sessions</a>.&lt;br&gt;By default, only current sessions are shown.&lt;br&gt;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.&lt;br&gt;&lt;br&gt;<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.&lt;br&gt;Click on a session to open its dashboard. From a session's dashboard, you can monitor the user session for troubleshooting. See <a href="#">Working with the Session Dashboard</a>.</td>
</tr>
<tr>
<td><strong>Assignments</strong></td>
<td>Lists the user's assignments.&lt;br&gt;&lt;br&gt;<strong>Note</strong> URL redirection customization assignments are not listed in the user card.</td>
</tr>
<tr>
<td><strong>Desktops</strong></td>
<td>Lists the user's:&lt;br&gt;- Active sessions to VDI floating desktops&lt;br&gt;- Active sessions to RDSH session desktops&lt;br&gt;- VDI dedicated desktops that have been assigned to this user, even when the user does not have an active session to that desktop.&lt;br&gt;&lt;br&gt;<strong>Note</strong> The system assigns a VDI dedicated desktop to a user in one of two ways:&lt;br&gt;- You explicitly assign that specific dedicated desktop to this particular user, using the Assign action in the VDI dedicated desktop assignment's page&lt;br&gt;- 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. &lt;br&gt;On this tab, you can use the standard virtual machine (VM) action buttons to perform actions on the desktops' underlying virtual machines.</td>
</tr>
<tr>
<td><strong>Applications</strong></td>
<td>Lists the user's entitled remote applications.</td>
</tr>
<tr>
<td><strong>Activity</strong></td>
<td>Displays the user's activity for selected time periods.</td>
</tr>
</tbody>
</table>
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 7</th>
<th>Horizon 7</th>
<th>Microsoft Azure</th>
<th>Microsoft Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>VDI Desktop</td>
<td>Session-based Desktop</td>
<td>VDI Desktop</td>
<td>Session-based Desktop</td>
</tr>
<tr>
<td>Send Message</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>Remote Assistance</td>
<td>Available for sessions from a Horizon 7 pod. Initiate a remote assistance session.</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Restart</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>Disconnect</td>
<td>Disconnect the session.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</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>Available for sessions from a Horizon 7 pod. Reset 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 on 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.

The following screenshot shows an example of some of the types of data and actions that are available in the session dashboard.
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 server 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 to Horizon Cloud. 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.
Starting with this release, you can use the Horizon Cloud Administration Console to perform tasks with your cloud-connected VMware Horizon 7 pods that enable you to create cross-pod desktop assignments for your end users.

In addition to its features for unified visibility, health monitoring, and help desk services for cloud-connected VMware Horizon 7 pods, Horizon Cloud lets you create desktop assignments that entitle end users to use desktop pools located in those pods.

This chapter includes the following topics:

- Changing the State of a Pod
- Creating Desktop Assignments
- Managing Desktop Assignments
- Disconnecting Pods

**Changing the State of a Pod**

The Capacity page displays the current state of cloud-connected pods under the State column. In this release, a pod can be in either Monitored or Managed state.

**Monitored State**

Monitored state is the default state of a pod after you first connect the pod to Horizon Cloud. 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 Dashboard Page.
- The Capacity page displays details about the pod such as its status, location, and state. See Capacity Page.
- The Administration Console provides a user-based search feature from which you can perform help-desk operations to support your users. See Chapter 3 Unified Visibility, Health Monitoring, and Help Desk Operations Using the Horizon Cloud Administration Console.
Managed State

If a monitored pod meets certain requirements, you can change the pod's state to Managed. See Change a Pod to Managed State.

A managed pod offers all the features available for a monitored pod. In addition, you can create and manage desktop assignments for a managed pod. For more information, see Managing Desktop Assignments.

Change a Pod to Managed State

If a monitored pod meets certain requirements, you can change the pod to Managed state. Changing a pod to Managed state lets you create desktop assignments for the pod.

Prerequisites

- Ensure that the Horizon 7 pod is at version 7.9 or later.
- Ensure that the pod has been cloud-connected to Horizon Cloud using Horizon 7 Cloud Connector version 1.3 or later.
- Ensure that the pod belongs to a pod federation as defined by the Cloud Pod Architecture feature.

For information about how to initialize the Cloud Pod Architecture feature and define a pod federation, see Administering Cloud Pod Architecture in Horizon 7 on the VMware Horizon 7 Documentation landing page.

**Important** For a pod to join a pod federation successfully, its Connection Servers must meet specific network requirements. You must ensure that your network allows for TCP traffic to specific ports on the pod's Connection Servers. For details about the required settings for these TCP ports, see the Horizon Connection Server section in the Network Ports in VMware Horizon 7, particularly the table rows that describe the ports needed for Cloud Pod Architecture. If network traffic is not allowed to these ports, the join step might fail.

- If one or more pods are already in Managed state, ensure that the new pod belongs to the same pod federation as the already managed pods.

For information about how to join a pod to a pod federation, see Administering Cloud Pod Architecture in Horizon 7 on the VMware Horizon 7 Documentation landing page.

Procedure

1. Select **Settings > Capacity**.
2. Open the Summary page for the pod by clicking the pod's name.
3 Click **Change State**.

The Change State dialog box appears.

**Note** If the pod does not meet the prerequisites for changing to Managed state, an error message appears in front of the Change State dialog box. Click **Close** to close the error message, and perform the prerequisite actions to prepare the pod. Then retry the steps to change the pod's state.

4 In the Change State dialog box, click **Save**.

The Capacity page now displays the pod’s state as Managed.

### Change a Pod to Monitored State

To change a 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 Desktop Assignment**.

2. Disconnect the pod from Horizon Cloud. For detailed instructions, see **Disconnect a Pod**.

   The pod is disconnected from Horizon Cloud, and the pod's name disappears from the Horizon Cloud Administration Console.

   **Note** You do not need to perform the steps described in **Clear the Cloud-Managed Properties from a Pod**.

3. Redeploy the pod to Horizon Cloud. For more information, see **Deploying Pods Using the Capacity Page**.

   The redeployed pod appears on the Capacity page in Monitored state.

### Creating Desktop Assignments

A desktop assignment consists of a collection of desktop pools from one or more cloud-connected pods that are made available to users or groups of users. Users and groups that receive a desktop assignment can access and use the desktop pools in that assignment.

### Worksheet for Creating a Desktop Assignment

When you create a desktop assignment, you can configure certain options. Use this worksheet to prepare your configuration information before you create the assignment.
### Table 4-1. Worksheet: Configuration Options for Creating a Desktop Assignment

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Type</td>
<td>Select one of the following:</td>
<td></td>
</tr>
</tbody>
</table>
|               | - **Floating**: 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 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 desktop assignments, the user might see different host names for each desktop session.  
- **Dedicated**: 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.  
  **Note**: This setting becomes read-only when you are editing a desktop assignment. |                          |
| Desktop Name  | Enter a user-friendly name for the 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. |                          |
| Description   | Enter a description of the desktop assignment.                                                                                                                                                                |                          |
| Scope         | To specify where Horizon can search for desktops in response to a user's desktop request, select one of the following options:  
  - **Any Site** allows Horizon to search for available desktops located in any geographic site.  
  - **Restrict to One Site** instructs Horizon to search only for available desktops located in the user's default geographic site. |                          |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Site Connection Affinity  | Site Connection Affinity specifies a certain geographic site as the default site for a user or group. When the user or group requests a desktop, Horizon 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, Horizon continues searching for desktops beyond the default site. Select one of the following options:  
  - **Nearest Site** specifies the nearest geographic site as the default site for the user or group.  
  - **Home Site** specifies the user or group's home site configured in Horizon Administrator as the default site for that user or group. For information about configuring home sites for users and groups, see *Administering Cloud Pod Architecture in Horizon 7* on the VMware Horizon 7 Documentation landing page.  
    - To allow the user or group to access desktops beyond their configured home site, do not enable **Home Site Restriction**.  
    - To restrict the user or group to their configured home site only when accessing desktops, enable **Home Site Restriction**.  
  Important: If you enable **Home Site Restriction**, the user or group must have a home site configured in Horizon Administrator before they can access any desktops. You can use home sites to manage the desktop allocation for roaming users and groups. For example, if a user has a home site in San Francisco but is visiting London, Horizon begins looking in the San Francisco site to satisfy the user's desktop request rather than allocating a desktop closer to the user. The **Home Site** and **Home Site Restriction** settings apply globally to users and groups accessing the desktop assignment. You can also override these settings for a particular user or group. For more information, see Create a New Desktop Assignment. |
| Operating System          | Specify the operating system of the desktop pools that you want to include in the assignment.                                                                                                                                                                                                       |
|                           | **Note** This setting becomes read-only when you are editing a desktop assignment.                                                                                                                                                                                                                 |
| Default Display Protocol   | Select the default display protocol to use when clients connect to a desktop. The choices are Microsoft RDP, PCoIP, and VMware Blast.                                                                                                                                                                      |
| Allow Users to Choose Protocol | Specify whether users can choose display protocols other than the default. It is recommended that you do not allow users to choose a display protocol.                                                                                                                                                        |
|                           | **Note** This setting becomes read-only when you are editing a desktop assignment.                                                                                                                                                                                                                 |
| HTML Access               | To allow users to connect to remote desktops from a Web browser, enable this option. For more information about this feature, see the VMware Horizon HTML Access Installation and Setup Guide. To use HTML Access with VMware Identity Manager™, you must pair Connection Server with a SAML authentication server, as described in the document. VMware Identity Manager™ must be installed and configured for use with Connection Server. |
| Clean Up Redundant Sessions | To close duplicate user sessions automatically, enable this option. If you disable this option, a user must manually log out of a duplicate session to close it.                                                                                                                                       |
### Create a New Desktop Assignment

To make a collection of desktop pools available to end users, you create a desktop assignment. The desktop pools in an assignment can reside on one or more cloud-connected pods that are in Managed state.

**Prerequisites**

- Using Horizon Administrator or Horizon Console, add desktop pools to the cloud-connected pods that you want to include in the desktop assignment. For more information, see the [VMware Horizon 7 Documentation](https://www.vmware.com/support/pubs/horizon_7.html).
- Place the cloud-connected pods in Managed state. For more information, see [Change a Pod to Managed State](https://www.vmware.com/support/pubs/horizon_7.html).
- Using the [Worksheet for Creating a Desktop Assignment](https://www.vmware.com/support/pubs/horizon_7.html), gather the configuration information that you must provide to create the desktop assignment.

**Procedure**

1. In the left pane of the Administration Console, click **Assignments**. If you have configured the Administration Console for hybrid cloud capacity, select **On-Prem & VMware Cloud** from the Assignments menu.

2. On the Assignments page, click **New**.

   The New Desktop Assignment wizard appears.

3. On the Definition page, for **Select Pod(s)**, select the check box next to each pod containing a desktop pool that you want to add to the assignment. You can select multiple pods to create an assignment consisting of desktop pools from different pods.

   Specify additional settings for the pod, using the configuration information that you gathered in the [Worksheet for Creating a Desktop Assignment](https://www.vmware.com/support/pubs/horizon_7.html). Then click **Next**.

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Users to Restart VMs</td>
<td>A restart operation restarts the virtual machine with a graceful operating system restart. This action applies only to an automated pool or a manual pool that contains vCenter Server virtual machines.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This setting becomes read-only when you are editing a desktop assignment.</td>
<td></td>
</tr>
<tr>
<td>Allow Multiple Sessions Per User</td>
<td>With this option enabled, a user connecting to the same desktop pool from different client devices gets different desktop sessions. The user can only reconnect to an existing session from the same client device. With this option disabled, users are always reconnected to their existing session no matter which client device is used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This setting becomes read-only when you are editing a desktop assignment.</td>
<td></td>
</tr>
</tbody>
</table>
4 On the Desktop page, for **Select Desktop Pools**, 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.

Specify additional settings, using the configuration information that you gathered in the Worksheet for Creating a Desktop Assignment. Then click **Next**.

5 On the Users page, specify the users and user groups that will receive the desktop assignment.

a Specify the Active Directory domain in which the users and groups reside.

**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 users 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**.

c Optionally, configure a home site override for the user or group by using the **Assign Home Site** menu. With a home site override, Horizon begins searching for available desktops in the override site instead of the user or group’s home site when the user or group accesses this desktop assignment.

**Note** The **Assign Home Site** menu is available only if you specified the user or group’s home site as the Site Connection Affinity default site on the Definition page of the wizard. See Worksheet for Creating a Desktop Assignment.

To specify a home site override, click **Assign Home Site** and select an option from the menu:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[configured site 1], [configured site 2] ...</td>
<td>The Assign Home Site menu displays all the sites that have been configured in Horizon Administrator for pods contained in the desktop assignment. Select the configured site that you want to specify as the override site for the user or group.</td>
</tr>
<tr>
<td>Default First Site</td>
<td>When you initialize the Cloud Pod Architecture feature, it places all pods into a default site called Default First Site. Later, an administrator can move pods from the Default First Site to a configured site. Select Default First Site to specify it as the override site for the user or group.</td>
</tr>
<tr>
<td>Clear Home Site</td>
<td>Select this option to remove the current home site override and use the configured home site instead.</td>
</tr>
</tbody>
</table>

For example, suppose that a user has a home site in San Francisco but you specify New York as the home site override. When this user accesses the desktop assignment, Horizon first searches for available desktops in New York instead of the user’s home site in San Francisco.

d Click **Next**.

6 Review the settings on the Summary page, and then click **Finish**.
Managing Desktop Assignments

You can perform several actions on the desktop assignments listed on the Assignments page.

Note Horizon Cloud Administration Console does not restrict you from using Horizon Administrator or Horizon Console to edit desktop pools associated with a desktop assignment. Horizon Cloud Administration Console also does not sync its desktop pool data with data from Horizon Administrator or Horizon Console. Therefore, Horizon Cloud Administration Console might display inconsistent information about desktop assignments at times.

For example, if you use Horizon Administrator or Horizon Console to delete a desktop pool associated with a desktop assignment, Horizon Cloud Administration 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 a desktop assignment.

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 Create a New Desktop Assignment. For detailed descriptions of the options that you can configure for a new desktop assignment, see Worksheet for Creating a Desktop Assignment.

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. For detailed descriptions of the options, see Worksheet for Creating a 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 Desktop Assignment.

The desktop pools included in an assignment remain intact after the assignment is deleted.
Information You Can View Within a Desktop Assignment’s Summary Page

From the Assignments page, you can click the name of a desktop assignment to view its detailed Summary page.

Capacity and Usage

The Summary page shows information about the current capacity and usage of the desktop assignment.
### Usage Type

<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. \n- 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. \n- 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)\times100 = 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 desktop assignment's
and Users Settings current settings, organized under the categories Definition, Desktops, and Users. For instructions on how to modify the settings, see Edit a Desktop Assignment. For detailed information about a specific setting, see Worksheet for Creating a Desktop Assignment.

Edit a Desktop Assignment

You can use the Edit button on the Assignments page to change the configuration settings for an existing desktop assignment.

Procedure

1. In the left pane of the Administration Console, click Assignments. If you have configured the Administration 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 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 desktop assignment as needed.

   For instructions on how to use the wizard, see Create a New Desktop Assignment. For detailed descriptions of configuration settings, see Worksheet for Creating a Desktop Assignment.

   Note Some configuration settings cannot be changed for an existing desktop assignment. For example, you cannot change the desktop type from Floating to Dedicated. Instead, you must create a new desktop assignment and specify the desktop type at the time of creation.

Delete a Desktop Assignment

You can permanently delete a desktop assignment from the Assignments page.

When you delete a desktop 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 Administration Console, click Assignments. If you have configured the Administration 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 desktop assignment does not happen immediately and can take some time to finish completely. On occasion, the deletion might fail, leaving the desktop assignment in “ERROR DELETE” state. If such a failure occurs, complete the deletion process by clearing the cloud-managed property from the global entitlement that corresponds to the desktop assignment. See [Clear the Cloud-Managed Properties from a Pod](#).

---

**Disconnecting Pods**

You can disconnect a pod from Horizon Cloud. When you disconnect a pod, the pod is no longer cloud-connected and you can no longer monitor or manage it from the Horizon Cloud Administration Console.

To disconnect a pod, you must first remove the pod from any desktop assignments.

If you disconnect an on-premises pod when it is offline or unavailable, you must also remove the pod’s **Cloud Managed** label by editing the Horizon 7 global database.

**Disconnect a Pod**

Use the Disconnect button on the Capacity page to disconnect a pod from Horizon Cloud.

**Prerequisites**

Remove the pod from any desktop assignments that include that pod. See [Edit a Desktop Assignment](#).

**Procedure**

1. Select **Settings > Capacity**.
2. Open the Summary page for the pod by clicking the pod’s name.
3. Click **Disconnect**.

   A notification message appears in the following cases:

   - If the pod is included in one or more desktop assignments, a message appears stating that you cannot disconnect the pod. You must first remove the pod from any desktop assignments before retrying the disconnection procedure.
   - If the pod is offline or unavailable, a message alerts you that the pod will still retain its cloud-managed property in the Horizon 7 global database after the disconnection process. You can specify whether to proceed with or cancel the disconnection process.

If you proceed with the disconnection process, the pod is disconnected from Horizon Cloud, and the pod’s name disappears from the pages in Horizon Cloud Administration Console.

**What to do next**

If the pod was offline or unavailable during the disconnection process, remove the pod’s cloud-managed properties from the Horizon 7 global database. See [Clear the Cloud-Managed Properties from a Pod](#).
Clear the Cloud-Managed Properties from a Pod

If an on-premises pod is offline or unavailable when you disconnect it, you must remove the pod's cloud-managed properties from the Horizon 7 global database. 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 Disconnect a Pod.

Procedure

1. Log in to the pod’s Connection Server with domain administrator privileges.
3. Configure a connection to the Horizon 7 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 7 global database is established.
4. Click the following entries to expand their display:
   - 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 the target pod and select Properties.

      The pod appears in the list with its Horizon Administrator or Horizon Console name.
   c. Set the value of the pae-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 pae-CloudManaged attribute to 0.

      Setting the value to 0 clears the cloud-managed property from the global entitlement.
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 Horizon Cloud Administration Console to create master 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. For the suggested workflow of activities for a pod in Microsoft Azure, see Suggested Workflow for When Your Very First Cloud-Connected Pod is from Deploying 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 deploying 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.

**Note** You preconfigure your Microsoft Azure environment with that VNet, and you can either create the subnets required by the pod in advance 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 pod 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.

**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 Administration 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
- VMs for the Unified Access Gateway and load balancer instances
- VMs for the master RDS-enabled server images
- VMs for the master VDI desktop images
- VMs for the assignable (published) images that are made from the master 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, 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 master 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. Do not manually change settings for the resources that are automatically created and deployed during workflows, assigned IP addresses or names, and so on. Do not manually power off VM instances directly using the Microsoft Azure portal. Do not manually delete the manager VM or Unified Access Gateway VMs. If you change the generated settings or manually power off VMs or manually delete VMs, unpredictable results can occur.

The following diagram illustrates a pod deployed with the Unified Access Gateway instances residing on the demilitarized (DMZ) network. This configuration is also called the external Unified Access Gateway configuration. 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. RG means resource group.
You can also deploy a pod with an internal Unified Access Gateway configuration. When your pod has this 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. The following diagram is a close-up of the internal Unified Access Gateway configuration.
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 servers 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 "master" account, and avoid the chances of hitting the Microsoft Azure limits that are imposed on a single subscription.
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>
<tbody>
<tr>
<td>Microsoft Azure glossary: A dictionary of cloud terminology on the Azure platform</td>
<td>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). \n\n<strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Use portal to create an Azure Active Directory application and service principal that can access resources</td>
<td>Use this article to learn about the relationship between an application and a service principal in a Microsoft Azure cloud.</td>
</tr>
<tr>
<td>Azure Resource Manager overview</td>
<td>Use this article to learn about the relationships between resources, resource groups, and the Resource Manager in Microsoft Azure.</td>
</tr>
<tr>
<td>Azure VNet</td>
<td>Use this article to learn about the Azure Virtual Network (VNet) service in Microsoft Azure. See also Azure Virtual Network FAQs.</td>
</tr>
<tr>
<td>Azure VNet Peering</td>
<td>Use this article to learn about virtual network peering in Microsoft Azure.</td>
</tr>
<tr>
<td>Microsoft Azure ExpressRoute Overview</td>
<td>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.</td>
</tr>
<tr>
<td>About VPN Gateway Planning and design for VPN Gateway Create a Site-To-Site connection in the Azure portal</td>
<td>Use these articles to learn about how to configure VPNs in Microsoft Azure.</td>
</tr>
<tr>
<td>What is Azure Load Balancer?</td>
<td>Use this article to learn about the Azure load balancers that are used when the pod is deployed with Unified Access Gateway configured.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure
- Using Microsoft Azure Disk Encryption with Your Farms and VDI Desktops
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 master virtual machine (VM) must be created, 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-enabled server images) or VDI desktops (in the case of non-server 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.

To create the image:

1. First you create a master virtual machine (VM) either using the automated wizard or manually:
   - The recommended and standard way is to use the Import Desktop wizard's option to create the master VM using one of the supported VM configurations from the Microsoft Azure Marketplace. Using the wizard automates building the master 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 Inventory page, start the Import Desktop wizard by clicking Import and then select the From Marketplace option. For steps, see Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace.

**Important** If your pod in Microsoft Azure is configured to use a proxy, you must create the base master VM using the alternative manual method, and not the automated Import Desktop method.

- 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 the Master Virtual Machine in Microsoft Azure.

**Important** If you use this alternative method, you are responsible for ensuring the resulting master 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 Desktop Wizard and Deciding to Remove Windows Store Apps When Using the Import Desktop Wizard.

2 When the master VM is visible on the Imported VMs page and the page indicates the agent-related status is active, then you customize the master 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 Master Image VM's Windows Operating System and Install NVIDIA Graphics Drivers in a GPU-Enabled Master Image.

**Important** When you use the automated wizard to create the master VM, the wizard joins the VM to the Active Directory domain that is selected in the wizard and then installs the agent software. Starting with pod manifest versions 1220 and later, domain accounts can log in to domain-joined VMs that have the agent software. However, when your pod has not yet upgraded to manifest version 1220 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 master image to customize it until you configure the DaaS Direct Connect Users local group with those domain accounts you want used for customizing the image. For details, see When Your Pod is Not Yet Upgraded to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image.

3 Then you use the New Image workflow in the Administration Console to convert that master VM to an assignable desktop image. For steps, see Convert a Configured Master Virtual Machine to an Assignable Image.
After the master 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-enabled Windows Server image, RDSH farms based on that image. You can create both types of farms from the same published RDS-enabled server image: desktop farms to provide session-based desktops and application farms to provide remote applications. When you have a farm, you can use it to make assignments to users. See Farms in Horizon Cloud.

- From a Windows client image, VDI desktop assignments based on that image. See Create a Floating VDI Desktop Assignment and Create a Dedicated VDI Desktop Assignment.

### Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace

For a pod in Microsoft Azure, you can use the Import Desktop wizard to create the master 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. The resulting VM is also joined to your AD domain as part of the automated process.

By default, the system sets **Optimize Windows Image**, regardless of operating system, and **Remove Windows Store Apps**, for Windows 10 operating systems, to **Yes**. Keeping those toggles set to **Yes** 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.

**Important** If your pod in Microsoft Azure is configured to use a proxy, you must create the base master VM using the alternative manual method, and not the automated Import Desktop method.

By default, in the **Advanced Options** section, the wizard sets **Yes** to install those agent-related custom setup options that are both appropriate according to your other selections in the wizard and which are supported for use in the Horizon Cloud environment. If you want to change the default selections, expand the **Advanced Options** section in the Import Desktop - Marketplace window and set the toggles according to your needs.

As an example, the **3D support in RDSH** agent option is selected by default in the **Advanced Options** section when you have selected a Microsoft Windows Server operating system in the **OS** drop-down list. However, when you have selected a Microsoft Windows client operating system that **3D support in RDSH** agent option is not selected for installation. Because that option is only applicable for RDSH use, and RDSH farms only use server operating systems, the Import Image wizard automatically sets the appropriate **3D support in RDSH** setting based on your **OS** choice.
Prerequisites

If you are creating an image with a Microsoft Windows 10 operating system, verify that you have valid licensing for that operating system. At this time, the Microsoft Azure documentation indicates that to legally run Windows 10 in Microsoft Azure, you must have licensing for Microsoft Windows 10, typically by purchasing an E3 or E5 license. Please verify licensing requirements and restrictions with your Microsoft Licensing distributor.

By default, this process installs the User Environment Manager FlexEngine component in its typical mode. User Environment Manager provides various options for achieving the persistence of end-user data, settings, and profiles of desktops provisioned by your pod. For more information, see the User Environment Manager product documentation.

Procedure

1. In the Horizon Cloud Administration Console, click Inventory > Imported VMs and then click Import.
2. In the Import Desktop window, click From Marketplace.

3. Select the destination location and pod for the desktop.

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.
4 Select the details for the base VM.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Select the Microsoft Windows operating system to use for the image's underlying VM.</td>
</tr>
<tr>
<td></td>
<td>- If you are going to use this image for VDI desktops, select one of the Windows 10 operating systems that are listed in the drop-down list. Do not select one of the server operating systems for a VDI desktop image.</td>
</tr>
<tr>
<td></td>
<td>- If you are going to use this image for RDSH session desktops or RDS-based remote applications, select one of the listed server operating systems.</td>
</tr>
<tr>
<td></td>
<td>Note This drop-down menu takes a few moments to populate the entries.</td>
</tr>
<tr>
<td>Include GPU</td>
<td>Set this toggle to <strong>Yes</strong> to specify a GPU-enabled VM for this master VM.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> If you select <strong>Yes</strong>, after the master 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 is created and the Imported VMs page shows the agent-related status as active.</td>
</tr>
<tr>
<td>Domain</td>
<td>Select the Active Directory domain that you want configured in this master VM. The master VM will be joined to this domain.</td>
</tr>
<tr>
<td>Enable Public IP Address</td>
<td>Set this toggle to <strong>Yes</strong> to configure a public IP address for this master VM. When set to <strong>Yes</strong>, the VM gets both a private IP address and a public one. When this toggle is set to <strong>No</strong>, 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 set to Yes to create a master 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 Desktop Wizard.                                                                                                                                                                                                                                                                                                                                 |
| **Remove Windows Store Apps** | This toggle is visible only when OS is set to a Microsoft Windows 10 operating system. By default, this toggle is set to Yes to create a master VM that:  
  - Disables the Windows Store Installer Service.  
  - Removes Windows Store applications that come in the base Windows 10 operating system by default. These Windows 10 default applications are ones provided by AppX packages in the Windows 10 operating system.  
  For more details, see Deciding to Remove Windows Store Apps When Using the Import Desktop Wizard.                                                                                                                                                                                                                                                                                                                             |
| **Important**             | Keeping the Yes 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.                                                                                                                                                                                                                                                                                                                                                                  |
5 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>Username</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. Important Ensure you can remember this local administrator account information (this name and the password that you specify in the Password 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 master image and when performing the New Image workflow to publish this master 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 (!@#$%^&*) |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify Password</td>
<td>Re-type the password.</td>
</tr>
<tr>
<td>Windows license question</td>
<td>The intent of this license question depends on whether you are using a Microsoft Windows Server or a Windows 10 client operating system for this master VM.</td>
</tr>
<tr>
<td></td>
<td>- When the OS choice is set to a Microsoft Windows Server operating system, set this toggle to Yes to specify both:</td>
</tr>
<tr>
<td></td>
<td>- That you are eligible to use the Azure Hybrid Benefit (also known as Azure Hybrid Use Benefit or HUB) with the selected OS choice</td>
</tr>
<tr>
<td></td>
<td>- That you want to apply that Azure Hybrid Benefit to this master image VM</td>
</tr>
<tr>
<td></td>
<td>When you set the toggle to Yes, you must also check the check box that is displayed.</td>
</tr>
<tr>
<td></td>
<td>As described in the Microsoft Azure documentation, the Azure Hybrid Benefit is designed by Microsoft to save you money when you already have valid Microsoft Windows Server licenses. The Azure Hybrid Benefit FAQ is located in the Microsoft Azure documentation at <a href="https://azure.microsoft.com/en-us/pricing/hybrid-benefit/faq/">https://azure.microsoft.com/en-us/pricing/hybrid-benefit/faq/</a>. According to the Microsoft Azure documentation, when you have a Windows Server license with Software Assurance or a Windows Server subscription for the selected server operating system, you can use the Azure Hybrid Benefit for the virtual server instances that have those Windows Server operating systems.</td>
</tr>
<tr>
<td></td>
<td>- When the OS choice is set to a Microsoft Windows 10 client operating system for this master VM, Horizon Cloud sets the VM to use the Windows Client license type by default and you cannot change this setting. By design, Horizon Cloud sets the same license type on the VM that would be set if you manually used the Microsoft Azure portal and created the VM from the Azure Marketplace with the selected Microsoft Windows 10 operating system. At this time, the Microsoft Azure documentation indicates that to legally run Windows 10 in Microsoft Azure, you must have licensing for Microsoft Windows 10, typically by purchasing an E3 or E5 license. Please verify licensing requirements and restrictions with your Microsoft Licensing distributor.</td>
</tr>
</tbody>
</table>

6. In the Name field, provide a name for the master VM and an optional description.  

**Important**  Do not enter a name that was previously used for a master VM that has been converted into an assignable image in your Horizon Cloud environment. For example, if a master image 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 Administration 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 (-).
Use the toggles in the **Advanced Options** section to customize the Horizon agent features that will be installed in the master VM.

When the option's toggle is set to **Yes**, the corresponding feature will be installed in the master VM.

**Note**. In addition to the options you see selected in this Import Desktop wizard, the wizard 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 server instances based on this image, and sends that data to the Horizon Cloud cloud monitoring service.
- **User Environment Manager client components.** Enables use of User Environment Manager features with the desktop VMs and server VMs that are provisioned based on this image.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.</td>
</tr>
<tr>
<td><strong>3D support in RDSH</strong></td>
<td>Applicable when the OS choice is set to a server operating system. Provides 3D graphics support to applications that run on a GPU-enabled RDSH server image.</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><strong>Smart Card</strong></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><strong>Thin Print</strong></td>
<td>Allows users to print to any printer available on their client computers, without installing additional drivers.</td>
</tr>
<tr>
<td><strong>Scanner Redirection</strong></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>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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>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 opens 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>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 master VM. Additional requirements are needed after the master VM is ready. For details, see the Horizon 7 topic System Requirements for Geolocation Redirection.</td>
</tr>
<tr>
<td>Help Desk</td>
<td>Provides the ability to collect performance-related desktop and session metrics from the virtual desktops. Those metrics can help you troubleshoot the health of the virtual desktops. Those metrics are used in the Administration Console's user card, which is part of the system's help-desk-related features.</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 7 product documentation.

8 Click **Import**.

The system begins creating and configuring the master VM. During this process, the VM is joined to the Active Directory domain that was selected in the **Domain** list. When the VM is created in the pod, it is listed on the Imported VMs page. Use the refresh icon to see the latest set of VMs on the page. Even though the VM is listed on the page after several minutes, the master VM is not ready for installing applications or drivers until the Imported VMs page indicates an active agent-related status. It can take approximately 30 minutes for the agent status to reach active state.

**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.
If the 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.

**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 Master Image 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 server VMs to be configured with the proxy.

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 Master Image.

If you want to use the features of NSX Cloud and its NSX-T Data Center components with the farm server instances or VDI assignment desktop instances based on this master image, 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 Master Image.

The import process installs the User 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 User Environment Manager with the desktop VMs and farm server VMs based on this image, configure a separate file server in your Microsoft Azure subscription that has at least SMB 2 enabled. Then configure User 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 User Environment Manager documentation topics in the User Environment Manager product documentation.

**Deciding to Optimize the Windows Image When Using the Import Desktop Wizard**

The Import Desktop wizard has an option for optimizing the Microsoft Windows operating system in the master virtual machine (VM). With that option selected, the image creation process results in a master VM that is optimized for Horizon Cloud. You can specify this option for both Microsoft Windows Server operating systems and Microsoft Windows 10 client operating systems.

The resulting settings depend on which Windows operating system is installed in the master 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 Operating Systems Only

When the optimizing option is selected, the image creation 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>

Deciding to Remove Windows Store Apps When Using the Import Desktop Wizard

The Import Desktop wizard has an option for removing Windows Store apps from the Microsoft Windows 10 operating system on the master virtual machine (VM). With that option selected, the image creation process results in a master 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.

The image creation process uses the Microsoft Windows 10 versions that are available in the Microsoft Azure Marketplace. As described in the Microsoft documentation at Understand the different apps included in Windows 10, Microsoft Windows 10 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, Windows 10 will also silently automatically download from the Windows Store and install various Windows Store Apps that it 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 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 any pre-installed Windows Store apps and preventing Windows 10 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 master VM's Windows 10 operating system.

- Configures these registry values to disable the Windows Store automatic download and the Microsoft Consumer Experience.

### Table 5-1. Registry values set for the **Remove Windows Store Apps** option

<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. The image creation script runs the following commands:

```
Get-AppxPackage -AllUsers | Remove-AppxPackage
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online
```
Customize the Master Image VM's Windows Operating System

After the master image virtual machine (VM) is created, but before you convert it into a published image in Horizon Cloud, you customize the VM's guest Windows operating system (OS) to install and configure the things you want and need in the image.

**Important** If you created the master VM using the Import Desktop wizard and you specified one of the following configurations, the system optimized the VM according to VMware best practices:

- Windows Server operating system and **Yes** for the **Optimize Windows Image** toggle
- Windows 10 operating system and **Yes** for the **Optimize Windows Image** and **Remove Windows Store Apps** toggles

If you did not use those options in the Import Desktop wizard, or if you manually created the master image VM, in addition to following the steps in the topics below according to the master image's specific operating system, you best also apply the following best practices before converting the master image to a published, sealed image. These best practices can help you avoid encountering issues that can typically occur during the sealing process, especially those related to the Microsoft Windows System Preparation (Sysprep) process.

To avoid known Sysprep errors from potentially occurring during the publishing process, prior to starting the publishing workflow:

- Manually configure the master 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**. For details, see Deciding to Optimize the Windows Image When Using the Import Desktop Wizard and Deciding to Remove Windows Store Apps When Using the Import Desktop Wizard.

- 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 master 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 Desktop wizard’s **Remove Windows Store Apps** toggle, see Deciding to Remove Windows Store Apps When Using the Import Desktop Wizard.

- Download the VMware OS Optimization Tool (OSOT) fling and use it to optimize the master image's Windows operating system. The OSOT is available at https://labs.vmware.com/flings/vmware-os-optimization-tool. You might also find helpful the information 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 OSOT.

Customize the Guest Windows Client Operating System of the Master VDI Desktop Virtual Machine

After the master image virtual machine (VM) for a VDI desktop is created, but before converting it into a published image in Horizon Cloud, 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.

After the Imported VMs page indicates that your master image virtual machine (VM) has its agent-related status as active, you connect to it using your RDP software and install the applications into the underlying Windows operating system.

Prerequisites

Verify the Imported VMs page indicates the agent-related status is active for the VM.

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 master 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 master image VM was created.

<table>
<thead>
<tr>
<th>VM was created using</th>
<th>Credentials to use to log in</th>
</tr>
</thead>
</table>
| Import Image wizard using the steps in Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace. | The Import Image wizard creates VMs that are joined to the Active Directory domain that was selected in the wizard. To log in to that VM, use one of the following:  
  - The credentials for the local administrator account that was specified in the Import Image wizard.  
  - The credentials for a domain account in that Active Directory domain. |
| Manual preparation steps in Manually Build the Master Virtual Machine in Microsoft Azure. | 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. However, if you have not yet upgraded your pod to the current release, 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 Upgraded 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 Windows operating system.
   - If the master image VM was created with a public IP address, you can use that IP address in your RDP software
If the master image 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 master image VM.
- Use your VPN and RDP into the master 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 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**

Follow the best practices to optimize the VM to prevent encountering sysprep or other errors during the process to convert the master image. See [Customize the Master Image VM's Windows Operating System](#).

Convert the master image VM to an assignable image, using the steps described in [Convert a Configured Master Virtual Machine to an Assignable Image](#).

**Customize the Guest Windows Server Operating System of the Master Server Image Virtual Machine**

After the master server image virtual machine (VM) is created, but before converting it into a published image in Horizon Cloud, you customize the guest Windows server operating system (OS) to install and configure all of the things you want to have in your end users' RDS desktops. At this time, you install all of the third-party applications you want available in the RDS 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.

After the Imported VMs page indicates that your master image virtual machine (VM) has its agent-related status as active, you connect to it using your RDP software and install the applications into the underlying Windows server operating system.

For Microsoft's best practices about installing applications directly on 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.

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 master 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 master image VM was created.

<table>
<thead>
<tr>
<th>VM was created using</th>
<th>Credentials to use to log in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Image wizard using the steps in Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace.</td>
<td>The Import Image wizard creates VMs that are joined to the Active Directory domain that was selected in the wizard. To log in to that VM, use one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual preparation steps in Manually Build the Master Virtual Machine in Microsoft Azure.</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></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Important** Starting with pod manifest 1230 and later, domain accounts can direct connect to domain-joined image VMs that have the agent software installed. However, if you have not yet upgraded your pod to the current release, 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 Upgraded 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 RDS-enabled Windows server operating system.

   - If the master image VM was created with a public IP address, you can use that IP address in your RDP software.
- If the master image 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 master image VM.
  - Use your VPN and RDP into the master 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 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.

   c  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.
d. Install the third-party user applications you want to provide to your end users in their RDS desktops or as remote applications.

e. 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`.

4. In the operating system, install any custom drivers you want in the RDS desktops.

5. 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.

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

Follow the best practices to optimize the VM to prevent encountering sysprep or other errors during the process to convert the master image. See Customize the Master Image VM's Windows Operating System.

Convert the master image VM to an assignable image, using the steps described in Convert a Configured Master Virtual Machine to an Assignable Image.

Install NVIDIA Graphics Drivers in a GPU-Enabled Master Image

If you created a master image VM with GPU, you must log into the VM's 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 image'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 master image VM must have been created with 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.

**Note**  When using the Microsoft Remote Desktop Client as your RDP software to connect to the master 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 master image VM was created.

<table>
<thead>
<tr>
<th>VM was created using</th>
<th>Credentials to use to log in</th>
</tr>
</thead>
</table>
| Import Image wizard using the steps in Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace. | The Import Image wizard creates VMs that are joined to the Active Directory domain that was selected in the wizard. To log in to that VM, use one of the following:  
  - The credentials for the local administrator account that was specified in the Import Image wizard.  
  - The credentials for a domain account in that Active Directory domain. |
| Manual preparation steps in Manually Build the Master Virtual Machine in Microsoft Azure. | 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. However, if you have not yet upgraded your pod to the current release, 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 Upgraded 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 master image VM was created with a public IP address, you can use that IP address in your RDP software.
   - If the master image 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 master image VM.
     - Use your VPN and RDP into the master 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 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 Master Virtual Machine to an Assignable Image**

To turn a configured master virtual machine (VM) into an assignable desktop image, use the Image page's New Image workflow. A desktop image must display the Published status on the Images page before the system can use it for assignments.

**Important** If your pod in Microsoft Azure is configured to use a proxy, you are responsible for providing a way for the farm server VMs or VDI desktop VMs that are created using this image to be configured with the proxy.

**Prerequisites**

Verify that a configured master VM is available in the pod in which you want to create the assignable image.

Verify that the Imported VMs page indicates that the master VM is powered on (green status) and its agent-related status is active.

Verify you have the credentials of an enabled local administrator account in the master image VM. The system uses the local administrator account in the image sealing process, which converts the master image into the published state. Typically, the VM's only enabled local administrator account is the one that you named when you created the master 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 base master VM, the VM's only local administrator account is the one you specified when you ran the Import Desktop wizard, or when you manually created the base master VM.
Procedure

1. In the Administration 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><strong>Location</strong></td>
<td>Select the location associated with the pod where you have the configured master VM.</td>
</tr>
<tr>
<td><strong>Pod</strong></td>
<td>Select the pod that has the configured master VM.</td>
</tr>
<tr>
<td><strong>Desktop</strong></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><strong>Image Name</strong></td>
<td>This field is auto-populated with the image name associated with the Desktop selection.</td>
</tr>
<tr>
<td><strong>Company Name</strong></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><strong>Timezone</strong></td>
<td>Retain the default.</td>
</tr>
<tr>
<td><strong>Admin credentials for the desktop</strong></td>
<td>Enter the credentials for the local administrator account that is enabled in the master VM. Usually the only enabled local administrator account is the one that was named when the master image VM was created. <strong>Note</strong> The publishing process includes running the Microsoft Windows Sysprep process. When the master image VM is 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.</td>
</tr>
</tbody>
</table>

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.

If the process is successful, the image’s status changes to Published.

**Note** When the master image VM 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 RDS-enabled Windows Server 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 a Microsoft Windows Server operating system, see Change RDS-Enabled Images Used for Farms
- 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 ... > Convert to Desktop. Then click New, enter the required information, and click Publish to publish the image.

**Manually Build the Master Virtual Machine in Microsoft Azure**

These steps are part of the alternative manual method for creating a master virtual machine (VM) for a pod in Microsoft Azure. Manually building a master virtual machine (VM) that conforms to the Horizon Cloud environment's requirements 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 Import Desktop wizard and instead want to manually build the master 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 for your master VM. The recommended automated way to build a master VM for a pod in Microsoft Azure is to use the Import Desktop wizard and its **From Microsoft Azure Marketplace** option. For details about using the automated wizard, see [Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace](#).

**Important** If you have a VM in Microsoft Azure that you want to use as the master’s base VM, you must ensure it conforms to the same criteria as when a base VM is created 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 the Administration 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. Those operating systems are described in the steps in [Create the Virtual Machine Manually in Your Pod in Microsoft Azure](#).
- Do not configure the base VM to use IPv6 IP addresses. The Administration Console will report an IP abnormal alert in the Desktop Health tab for VMs that are based on a master VM that uses IPv6 IP addresses.

To verify your base VM meets that criteria before you start to configure it further, log in to the Horizon Cloud Administration Console, 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 Master VM Prior to Installing the Agents](#).

**Procedure**

1. [Create the Virtual Machine Manually in Your Pod in Microsoft Azure](#)
2 Prepare the Manually Created Master VM Prior to Installing the Agents
When manually building a master 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 Agent-Related Software Components in the Base Virtual Machine
In the base virtual machine's Windows operating system, run the Horizon Agents Installer to install the agent-related components that are required and appropriate for Horizon Cloud.

4 Manually Pair the Configured Virtual Machine with Horizon Cloud
In the base virtual machine (VM), after running the Horizon Agents Installer, you must configure some DaaS agent properties to manually pair the VM with the pod before Horizon Cloud can convert the VM into an assignable image that can be used in Horizon Cloud.

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 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 Administration Console if they have `Storage-Use managed disk` set to `Yes`. 
For your master 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. For the specific list of operating systems, see the Release Notes document for the current in-production release.

**Note** The Import Image automated method of creating a master VM uses the following specific VM families when it creates a master VM. Typically you would choose to use these same patterns when you manually create a master VM. Because you will later choose the VM types for the actual RDSH servers and VDI desktops when you create the farms and VDI desktop assignments, there are few reasons to use VM sizes for the master VM that are larger than the ones that the Import Image process uses. Potentially, you might want to try a larger size if you are going to load applications into the master VM and test them out before sealing the master VM.

- Non-GPU Microsoft Windows Server operating systems: D2 V3 Standard type
- Non-GPU Microsoft Windows 10 operating systems: D4 V3 Standard type
- GPU-backed Microsoft Windows Server operating systems: NV6 Standard type
- GPU-backed Microsoft Windows 10 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 Image process will fall back to use the D2 V2 Standard (for server OSes) and D3 V2 Standard (for Windows 10).

For details about the sizes for Windows virtual machines in Microsoft Azure, see the Microsoft Azure documentation at [https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes).

**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 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 Administration 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 desktops or RDSH desktops or remote applications using this base VM. For the list of operating systems supported for use in the base VM, see the Release Notes document for the current in-production release.

**Important** If you want to have GPU-based RDSH desktops, select Microsoft Windows Server 2016. If you select Microsoft Windows Server 2012 R2 instead, an NVIDIA driver limitation will limit the number of end-user sessions you can have on each RDS desktop to a maximum of 20 sessions per desktop.

5. Click the one you want for the base VM.
6 In the new pane, if you see a menu for **Select a deployment model**, verify that the deployment model is set to **Resource Manager** and then click **Create**.

![Deployment Model Menu]

**Note**: Typically that menu is displayed only when the selected operating system is a server operating system.

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></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 classic VMs? Create VM from Azure Marketplace

**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>
</tr>
</thead>
<tbody>
<tr>
<td>HCS-38898853</td>
</tr>
</tbody>
</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>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Region**             | Select the region that matches the Microsoft Azure region in which your pod is deployed.  
  **Note** 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. |
| **Availability options** | Keep the default (No infrastructure redundancy).                                                                                                                                                           |
| **Image**              | Verify the selection matches the Windows operating system you want.                                                                                                                                          |
| **Size**               | Choose a size for the VM. If you want to choose according to the ones used by the system's automated Import Image wizard, those are:  
  - Non-GPU Microsoft Windows Server operating systems: D2 V3 Standard type  
  - Non-GPU Microsoft Windows 10 operating systems: D4 V3 Standard type  
  - GPU-backed Microsoft Windows Server operating systems: NV6 Standard type  
  - GPU-backed Microsoft Windows 10 operating systems: NV6 Standard type |
| **Username**           | Enter a name for the VM's default administrator account.                                                                                                                                                     |
| **Password**           | 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 (-). |
| **Confirm password**   |                                                                                                                                                                                                              |
| **Public inbound ports** | If you want to be able to install the agents by connecting to the VM over the Internet using RDP, select Allow selected ports and select RDP (port 3389).                                                                 |
| **SAVE MONEY section** | For Windows 10 operating systems, this section is set to use Windows Client License by default.  
  **Already have a Windows license?** For Windows Server operating systems, select the appropriate choice, depending on whether you already have the appropriate Windows Server licensing. |

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 server 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.

10 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.

**Important**

- As described in the prerequisites section above, you must set the **Virtual network** to the same one 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.
Option | Description
--- | ---
Virtual network | Click Virtual network and select the same virtual network 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`.

---

<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>
</table>

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

**NETWORK INTERFACE**

When creating a virtual machine, a network interface will be created for you.

**CONFIGURE VIRTUAL NETWORKS**

- **Virtual network**
  - VMW-HCS
  - Create new

- **Subnet**
  - VMW-HCS-podID-net-tenant (192.168.210/26)
  - Manage subnet configuration

- **Public IP**
  - (new) a4smanualwin10-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`).
### Setting | Value
---|---
Resource group | vmw-hcs-podID-base-vms
Use managed disks | Yes
Virtual network | The pod's virtual network.
Subnet | vmw-hcs-podID-net-tenant

---

14 Start deploying the VM by clicking the **Create** button at the bottom of the pane.

Microsoft Azure starts deploying the new VM into the resource group. When the VM is deployed successfully in Microsoft Azure, the Horizon Cloud Administration 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.
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 Master VM Prior to Installing the Agents.

Prepare the Manually Created Master VM Prior to Installing the Agents

When manually building a master 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 Master Server VM for Agent Installation

The following steps are those for preparing a manually created master server VM, which you will use for your pod’s RDSH farms. You perform these steps prior to installing 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 master server 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 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 find you cannot log in to the VM using that account.
3. Download the Horizon Agents Installer to the VM.
4. Download the DaaS SSL bootstrap file 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 the Master Virtual Machine in Microsoft Azure.

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 the Master Virtual Machine in Microsoft Azure. 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 the Horizon Cloud Administration Console 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.

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.
4 Click Yes to the certificate warning in the Remote Desktop Connection screen.

Because this 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 launches to its first-time configuration wizard.

5 Dismiss 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.
   i Start the process.

      The wizard starts installing the RDS role. When the screen indicates a restart is pending. close the wizard and close your RDP session.
   j In the Microsoft Azure portal, click Stop on the VM to power it off completely.
   k When the portal reflects the VM is completely stopped, click Start to power it on again.
   l 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 temporarily enable Internet Explorer to download the Horizon Agents Installer software, turn off the **IE Enhanced Security Configuration** for both administrators and users.

Download the Horizon Agent Installer software to the VM from [www.vmware.com](http://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.

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](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. When you later configure the agent-related components in the VM, this file is used as input to the `keytool.exe` utility.

**What to do next**

Complete the steps described in **Install the Agent-Related Software Components in the Base Virtual Machine** to install the agent-related software components.

**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 Master VM for Agent Installation**

The following steps are for manually preparing a master 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 master server 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.

3. Download the DaaS SSL bootstrap file 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 the Master Virtual Machine in Microsoft Azure](#).

**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 the Master Virtual Machine in Microsoft Azure](#). 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 the Horizon Cloud Administration Console 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**.

   ![Screenshot of Connect option](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](image)

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.

6. Download the Horizon Agent Installer software to the VM from [www.vmware.com](http://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.

7. 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](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. When you later configure the agent-related components in the VM, this file is used as input to the `Keytool.exe` utility.

**What to do next**

Complete the steps described in Install the Agent-Related Software Components in the Base Virtual Machine to install the agent-related software components.

**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 Agent-Related Software Components in the Base Virtual Machine

In the base virtual machine’s Windows operating system, run the Horizon Agents Installer to install the agent-related components that are required and appropriate for Horizon Cloud.

**Note** Keep the following points in mind as you perform this task:

- Installing a version of the Horizon Agents Installer that is older than the most recent version of the Horizon Agents Installer 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 The User Card in the Horizon Cloud Administration Console.

- 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 Administration Console.

- The User Environment Manager option is not enabled by default. Selecting that option installs the User 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 User Environment Manager Group Policy. For User Environment Manager usage information, see the User Environment Manager product documentation. User 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 User 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 Master VM Prior to Installing the Agents.
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.

However, if you do install the URL redirection option, do not install the options for either serial port redirection or scanner redirection. This Horizon Cloud release does not support use of the serial port redirection and scanner redirection options.

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.

- 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.
2 Click **Configure**.

The wizard's next step displays. The following screenshot is an example of this step when running on a server image.
Horizon Cloud Administration Guide

3 Scroll down to see the feature options.

The following screenshot is an example of this step when running on a server image.
4 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 *The User Card in the Horizon Cloud Administration Console*.

5 If prompted with a message about using USB redirection securely, click **OK**.

The final wizard step displays.

6 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)

**Success!**

**Installation list**
- Microsoft Visual C++ 2017 Redistributable - x86
- Microsoft Visual C++ 2017 Redistributable - x64
- VMware Horizon Cloud Components
- VMware Horizon Agent Components

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.

**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**.

If you selected to install the User Environment Manager option, configure a separate file server in your Microsoft Azure subscription that has at least SMB 2 enabled. Then configure User Environment Manager using that file server. Also configure the GPO settings. See the User Environment Manager documentation topics in the **User 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® 7 documentation set, such as **Disable Weak Ciphers in SSL/TLS**.

**Manually Pair the Configured Virtual Machine with Horizon Cloud**

In the base virtual machine (VM), after running the Horizon Agents Installer, you must configure some DaaS agent properties to manually 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 summary page in the Horizon Cloud Administration Console, obtain the pod's tenant appliance IP address. In the Administration Console, navigate to **Settings > Capacity** and click on the pod's name. On the Summary page, locate the **Tenant appliance IP address** property and note down that IP address.

- Verify that the agent-related components were installed in the base VM as described in **Install the Agent-Related Software Components in the Base Virtual Machine**.

- Verify that the DaaS SSL bootstrap file was downloaded to the VM, as described in **Prepare the Master Server VM for Agent Installation**. The file is named `image_bootstrap.7z` by default.
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. 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).

3. 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 the pod’s Tenant appliance IP address value that you obtained from the pod’s details page in the Administration Console.

4. Restart the DaaS agent service.
   The DaaS agent waits for the bootstrap credentials to be imported in the next step.
5 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.

6 Close your RDP connection.

7 In the Microsoft Azure portal, click **Stop** on the VM.

8 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 Administration 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 Master Image VM's Windows Operating System** and its subtopics:

- For server operating systems: **Customize the Guest Windows Server Operating System of the Master Server Image Virtual Machine**
For Windows 10 operating systems: Customize the Guest Windows Client Operating System of the Master VDI Desktop Virtual Machine

**Important**  It is strongly recommended that you optimize the image VM, including removing AppX packages from Window 10 images, as described in Customize the Master Image VM’s Windows Operating System, Deciding to Optimize the Windows Image When Using the Import Desktop Wizard, and Deciding to Remove Windows Store Apps When Using the Import Desktop Wizard.

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 DaaS agent is active. See Install NVIDIA Graphics Drivers in a GPU-Enabled Master Image.

After you are finished customizing the master VM, use the New Image workflow to convert the master VM to an assignable image. See Convert a Configured Master Virtual Machine to an Assignable Image.

### Using Microsoft Azure Disk Encryption with Your Farms and VDI Desktops

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
- Create a Floating VDI Desktop Assignment

**Note**

- This release does not support having disk encryption for floating VDI assignments that use image VMs with attached data disks.
- When creating a floating VDI desktop assignment, you cannot enable both disk encryption and NSX Cloud management.

### 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 Administration 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 server 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.

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 master image VMs automatically created by the Import Image wizard or master 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 server 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 server VM is available to all end users that connect to that server for their session-based desktops and remote applications. Also, because an end user might get connected to different server 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 master image before publishing the image.

At a high level, you:

1. Attach the created data disks to the master image 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 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 Assignable Images and its subtopics.

For the detailed steps of preparing a data disk for a master image VM used in Horizon Cloud, see Setting Up a Data Disk for a Master Image VM.
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 Administration 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 server 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 server and desktop VMs are created and deleted, according to the system's standard behavior.

Setting Up a Data Disk for a Master Image VM

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 master 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 master image VMs automatically created by the Import Image wizard or master 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 master 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 Image wizard creates a master VM without a data disk. If you manually created the master 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 master 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.

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 master 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 master image VM was created.

<table>
<thead>
<tr>
<th>VM was created using</th>
<th>Credentials to use to log in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Image wizard using the steps in Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace.</td>
<td>The Import Image wizard creates VMs that are joined to the Active Directory domain that was selected in the wizard. 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 in the Import Image wizard.</td>
</tr>
<tr>
<td></td>
<td>■ The credentials for a domain account in that Active Directory domain.</td>
</tr>
<tr>
<td>Manual preparation steps in Manually Build the Master Virtual Machine in Microsoft Azure.</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>

Important Starting with pod manifest 1230 and later, domain accounts can direct connect to domain-joined image VMs that have the agent software installed. However, if you have not yet upgraded your pod to the current release, 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 Upgraded 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 master VM in the Microsoft Azure portal.
   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.
      ![Screenshot of Azure portal search](image)
      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.
         Master 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 Administration 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>Name</td>
<td>Type a name for the data disk.</td>
</tr>
<tr>
<td>Resource Group</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 (<code>vmw-hcs-podID-base-vms</code>).</td>
</tr>
<tr>
<td>Note</td>
<td>You can locate the data disk in a resource group other than the pod's resource groups.</td>
</tr>
<tr>
<td>Location</td>
<td>Displays the Microsoft Azure region in which the VM is located.</td>
</tr>
<tr>
<td>Account type</td>
<td>Select the type you want.</td>
</tr>
<tr>
<td>Source type</td>
<td>Select None (empty disk).</td>
</tr>
<tr>
<td>Size</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

Create managed disk

* Name
la48win-1-disk1

* Resource group
`vmw-hcs-podID-base-vms`
Create new

* Location
West US 2

Availability zone
None

* Account type
Standard SSD

* Source type
None (empty disk)

* Size (GiB)
1023

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 master image VM was created with a public IP address, you can use that IP address in
          your RDP software
      ■  If the master image 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 master image VM.
          ■  Use your VPN and RDP into the master 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.

    At this point, the master 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 server 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 Horizon Cloud Release Notes for the current Horizon Cloud release.

**Note** When you have updated an existing pod from manifest versions prior to 1101 up to this release level, 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 server 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 Manager.</td>
<td>Refer to the NSX-T Data Center documentation topic here.</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 environment.</td>
<td>Refer to the NSX-T Data Center documentation topic here.</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>▪ Deploy PCG prerequisites</td>
<td></td>
</tr>
<tr>
<td>▪ Deploy PCG in a Microsoft Azure VNet</td>
<td></td>
</tr>
<tr>
<td>Create a master VM using the Import Desktop wizard.</td>
<td>See Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace. To make it easy to install the required NSX agent, a best practice is to select the option for a public IP address.</td>
</tr>
<tr>
<td>Connect to the master VM and install the required NSX agent.</td>
<td>Install the NSX Agent in the Master Image</td>
</tr>
<tr>
<td>Publish the image.</td>
<td>Convert a Configured Master Virtual Machine to an Assignable Image</td>
</tr>
<tr>
<td>Create farms and VDI desktop assignments using that image and the setting to enable NSX Cloud management for that farm or assignment.</td>
<td>▪ Create a Farm</td>
</tr>
<tr>
<td>When the RDSH server and VDI desktop VMs are created, they appear in your NSX Cloud inventory.</td>
<td>▪ Create a Dedicated VDI Desktop Assignment</td>
</tr>
<tr>
<td>▪ Create a Floating VDI Desktop Assignment</td>
<td></td>
</tr>
<tr>
<td>Enable the distributed firewalls rules in NSX Manager that will allow communication with the RDSH server and VDI desktop VMs</td>
<td>Because NSX Cloud will block these communications by default, you must enable some distributed firewall rules in NSX Manager to allow communication with the NSX-managed VMs that are provisioned from the pod. See Firewall Rules Required in NSX Manager for Pod-Provisioned VMs. If you are using NSX-T Data Center 2.4, in addition to enabling the firewall rules, you must also add a forwarding policy to route the traffic pertaining to the NSX-managed VMs over the Microsoft Azure cloud’s network (underlay). See Add the Required Forwarding Policy in NSX Manager for the Pod-Provisioned VMs.</td>
</tr>
<tr>
<td>Use NSX Cloud features with the RDSH server and VDI desktop VMs in your NSX Cloud inventory.</td>
<td>See this NSX Cloud topic and its subtopics in the NSX-T Data Center Administration Guide.</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 master 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 server instances or the VDI desktop assignment's virtual desktops. For details of those workflows, see:

- Create a Farm
- Create a Dedicated VDI Desktop Assignment
- Create a Floating VDI Desktop Assignment

Setting the **NSX Cloud Managed** toggle to **Yes** when creating a farm or VDI desktop assignment gives the resulting farm's server 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 in the Horizon Cloud Administration Console:

- 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 Master Image**

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 master image VM before you publish it. You install the NSX agent after the master 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 master 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.

**Note** When using the Microsoft Remote Desktop Client as your RDP software to connect to the master 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 master image VM was created.

<table>
<thead>
<tr>
<th>VM was created using</th>
<th>Credentials to use to log in</th>
</tr>
</thead>
</table>
| Import Image wizard using the steps in Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace. | The Import Image wizard creates VMs that are joined to the Active Directory domain that was selected in the wizard. To log in to that VM, use one of the following:  
  - The credentials for the local administrator account that was specified in the Import Image wizard.  
  - The credentials for a domain account in that Active Directory domain. |
| Manual preparation steps in Manually Build the Master Virtual Machine in Microsoft Azure. | 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. However, if you have not yet upgraded your pod to the current release, 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 Upgraded 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 master image VM was created with a public IP address, you can use that IP address in your RDP software  
   - If the master image 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 master image VM.  
     - Use your VPN and RDP into the master 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 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 a master image 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 xxxxxxxxxxxxxxxxxxxxxxxxxxx.xx.internal.cloudapp.net.

```
powershell -file 'nsx_install.ps1' -operation install -dnsSuffix xxxxxxxxxxxxxxxxxxxxxxxxxxx.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 Master Virtual Machine to an Assignable Image.

**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.
### 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.
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 in the Administration Console to manage your farms. You navigate to the Farms page using the Inventory icon.

Create a Farm

You create farms using the Farms page.

Note  The RDS-enabled image is also called an RDS host or an RDSH (Remote Desktop Services Host) image.

For an example of how rolling maintenance works for a farm, see Example of Farm Rolling Maintenance.

Prerequisites

- Verify that you have at least one image listed on the Images page, that image has an RDS-enabled Windows server 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.
- Verify whether you are eligible to use the Azure Hybrid Benefit (also known as Azure Hybrid Use Benefit or HUB) with the image's Microsoft Windows Server operating system. When you are eligible to use the Azure Hybrid Benefit with your VMs in Microsoft Azure, you can choose to apply your Azure Hybrid Benefit to this farm's server instances.
- Decide whether this farm will serve session-based desktops or remote applications. In this release, the same farm cannot serve both.
Decide whether you want the farm's servers 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.

**Important** If you are creating this farm in a pod that was upgraded from manifest version 740 or earlier, and you plan to use an image that existed in the pod before the pod upgrade, do not encrypt the farm. The encryption process fails if the image was created when the pod was at manifest version 740 or earlier. Such images do not have a working Microsoft Azure Agent, which is required for encrypting VMs. To re-use such an image for an encrypted farm, you must:

a. Duplicate the image. This action creates a new master VM based on the existing image. This new master VM has the required Microsoft Azure Agent.

b. Convert the duplicate to an image. This action creates a sealed image from the duplicate.

c. Use that new sealed image when creating the encrypted farm.

Decide whether you want the ability to use NSX Cloud features with the farm's server 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.

**Procedure**

1. In the Administration 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>Name</td>
<td>Enter a name for this farm.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description.</td>
</tr>
<tr>
<td>VM Names</td>
<td>Base name for all of the server 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>Farm Type</td>
<td>Specify the type of asset this farm provides to end users:</td>
</tr>
<tr>
<td></td>
<td>- Select Desktops to use this farm to provide session-based desktops.</td>
</tr>
<tr>
<td></td>
<td>- Select Applications 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 servers into your application inventory.</td>
</tr>
<tr>
<td>Location</td>
<td>Select the location associated with the pod that has the RDSH image. This selection filters the choices in the <strong>Pod</strong> field to only the pods in the selected location.</td>
</tr>
<tr>
<td>Pod</td>
<td>Select the pod.</td>
</tr>
</tbody>
</table>
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 any custom tags you have created. For more information about selecting model VMs, 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 value(s). By default, there is a single filter with the criterion 'Type' the value 'VMware Recommended'. The value changes to 'Favorites' when you have added favorite(s). 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**

  - Favorites - Model VMs you have marked as favorites on the VM Types & Sizes page (Settings > VM Types & Sizes). If you have not marked any VMs as favorites, do not select this option.
  - VMware Recommended - Model VMs recommended by VMware. This is a hard-coded list. 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.
  - GPU and High Performance - Model VMs with GPU.

  **Note** If you plan to select an image with GPU, you must use a model VM with GPU. If you plan to select an image without GPU, you must use a model VM without GPU.

- **Series**
Option | Description
--- | ---
When you select this option, you can then select a series of model VMs 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 for model VMs.

- **Memory**

When you select this option, you can then enter a memory range for model VMs.

- **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 those that you created on the VM Types & Sizes page (Settings > VM Types & Sizes). If you have not created any tags, do not select this option.

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.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td>Set the new filter by selecting a criterion and entering value(s).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the model VM you selected to create the farm becomes unavailable in the future, you will not be able to expand the farm. The farm remains fully functional except for this limitation. To see if a VM type is available, navigate to the VM Types &amp; Sizes page (<a href="#">Settings &gt; VM Types &amp; Sizes</a>).</td>
</tr>
<tr>
<td>Model</td>
<td>Select the VM model to use for the farm's server instances. This selection defines the set of underlying resources that will be used when the farm's server 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.</td>
</tr>
<tr>
<td>Image</td>
<td>Select the assignable RDSH image.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> If you set the <a href="#">NSX Cloud Managed</a> toggle to <a href="#">Yes</a>, 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 server instances, 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 start their session-based desktops from the Workspace™ ONE™ platform's portal, 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 <a href="#">Yes</a> so that the farm's server instances are automatically joined the domain when they are created.</td>
</tr>
<tr>
<td>Encrypt Disks</td>
<td>Select <a href="#">Yes</a> so that the farm's server instances have encrypted disks.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> 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>NSX Cloud Managed</td>
<td>Select <a href="#">Yes</a> so that you can use features of NSX Cloud with the farm's server instances. For a description of using NSX Cloud features with your farms in Microsoft Azure, see <a href="#">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 server instances, 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 server instances, 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. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min Servers</td>
<td>Specify the minimum number and maximum number of servers you want in this farm. When the farm is first created, the system deploys the number of servers specified in the Max Servers field, and then powers off the servers except the number specified for Min Servers. Only the minimum number of server instances is initially powered on. As end user demand increases, the system powers on additional servers, up to the Max Servers number. Then as end-user demand shrinks, the system powers off the servers, until it reaches the Min Servers number of servers. A server must be completely empty of user sessions before the system powers it off. When you specify zero (0) for Min Servers, it indicates that you want the system to power off all the farm's servers when there is no end-user demand for sessions to the farm. When you enter zero (0) for Min Servers, use the Power Of Protect Time field to specify the amount of time you want the system to wait after determining the remaining powered-on server has no user sessions before the system powers off that server.</td>
</tr>
<tr>
<td>Max Servers</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 server instance. 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 server 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.</td>
</tr>
<tr>
<td>Sessions per Server</td>
<td>Specify the number of concurrent end-user sessions per server 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 VMware Horizon Cloud Service™ on Microsoft Azure RDS Desktop and Application Scalability white paper located here in vmware.com. <strong>Note</strong> - Due to an NVIDIA driver limitation, if your GPU-enabled master image has Microsoft Windows Server 2012 R2 for its operating system, a farm using that image for its servers is limited to 20 sessions maximum per server. If you have that particular combination (image with GPU, Microsoft Windows Server 2012 R2, NVIDIA drivers, and an NV-series server model), do not specify more than 20 here.</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 server 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 need to use nested Organization Units, see Considerations For Using Nested Active Directory Domain Organizational Units. <strong>Note</strong> 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 farm's server VMs after the VM creation process. <strong>Note</strong> 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 The script is run after the Microsoft Windows System Preparation (Sysprep) process. When the system creates a server VM for the farm, the VM starts up and completes the Sysprep process in the Windows operating system. When the Sysprep process completes, the agent in the 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 server VM. On the next restart, the system logs in to the Windows operating system using the local administrator account and runs the script.</td>
</tr>
</tbody>
</table>
| **Windows License question** | This toggle and its associated check box indicate:  
  - Whether you are eligible to use the Azure Hybrid Benefit (also known as Azure Hybrid Use Benefit or HUB) with the image's Microsoft Windows Server operating system.  
  - Whether you want to use the Azure Hybrid Benefit with this farm's server instances.  
  The farm's server instances will be created with the HUB setting that is indicated here. By default, this toggle is set to match the HUB property set in the base image you specify in Image. For example, if the base image was created with the HUB setting as Yes, this toggle is automatically set to Yes. If the base image was created with the HUB setting as No, this toggle is automatically set to No.  
  If the toggle is set to No and you are eligible to use the Azure Hybrid Benefit, you can set this toggle to Yes to have the farm's server instances use the Hybrid Benefit. If you change this toggle to Yes, you must also check the check box that is displayed.  
  When this toggle is set to Yes, it means both:  
    - That you are eligible to use the HUB with the server instances' Microsoft Windows Server operating system  
    - That you want to have the farm's server instances use the HUB setting |
As described in the Microsoft Azure documentation, the Azure Hybrid Benefit is designed by Microsoft to save you money when you already have valid Microsoft Windows licenses. The Azure Hybrid Benefit FAQ is located in the Microsoft Azure documentation at https://azure.microsoft.com/en-us/pricing/hybrid-benefit/faq/.

According to the Microsoft Azure documentation, when you have a Windows Server license with Software Assurance or a Windows Server subscription for the selected server operating system, you can use the Azure Hybrid Benefit for your virtual server instances that have those Windows Server operating systems.

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>
</table>
| **Rolling Maintenance** | Select the maintenance type, either according to a time cadence (**Scheduled**) or based on user sessions to this farm’s servers (**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.  
**Note** 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 servers based on a count of short running sessions.  
In the **Concurrent Quiescing Servers** field, specify the number of servers that can be in the quiescing state at the same time. When a server is in quiescing state, the server continues to work for the user sessions already connected to that server, but it does not accept any new user connections.  
For a simple example, see Example of Farm Rolling Maintenance. |
| **Server Action**       | Select the action that the system should perform on the servers undergoing maintenance.  
- With **Restart**, the server VMs are restarted.  
- With **Rebuild**, the server VMs are first deleted and then reprovisioned from their RDS desktop image.  
If you choose to have the unused servers powered off, they will still consume some storage use in your cloud environment. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Management</td>
<td>These power management settings are related to the thresholds at which the system automatically increases and shrinks the number of powered-on server instances in the farm according to the session usage on the servers. When the usage increases above an upper bound, the system automatically powers up a new server instance. When the usage shrinks below a lower bound, the system drains the server until it is not being used. Then the system shuts down the server VM and deallocates it.</td>
</tr>
</tbody>
</table>

The power management selections balance capacity cost with faster availability:

- Select **Optimized Performance** when you want the system to power on the next server instance sooner rather than later. Even though you are spending more by having the next server ready to go before the user demand requires it, this setting increases the chance that when users log in, the server 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 server instance. The occupancy of the servers is higher before the system powers up the next server. Even though this selection minimizes capacity costs by getting higher use of the existing servers, 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 server.

- 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* white paper located [here](vmware.com).
<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>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>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 servers.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Empty Session Timeout</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Log Off Disconnected Sessions</strong> - Select when the system logs 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>
</tbody>
</table>
### Session Timeout Interval

This time interval is the amount of time the end users’ sessions can be idle before the system forces a log off 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 timeout settings that govern the end users’ Horizon Client or HTML Access logged-in session.

**Caution** 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.

The default interval is one day (1440 minutes).

**Note** 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 **OK** in the next 30 seconds. If the logout occurs, any unsaved user data, such as documents or files, is lost.

---

### Schedule Power Management

To help optimize savings and performance of the farm’s server VMs in Microsoft Azure, you can optionally configure schedules to adjust the minimum number of powered-on servers in this farm 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 or remote applications, you can have a schedule for zero or a low number of powered-on servers.

- 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 servers to be available to meet that demand.

You can specify up to 10 schedules for the farm. If any schedules have overlapping time periods but specify different minimum server numbers, the system uses the largest value of minimum servers for the overlapping time period.

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></td>
<td><strong>Note</strong> 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 Servers field, type the minimum number of servers you want powered on during the specified time period. During the specified time period, that number of servers 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 Servers 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 servers 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 server VM has to power on.</td>
</tr>
</tbody>
</table>

5. In the wizard's Summary step, review the settings and then click **Submit** to begin creating the farm. 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:

- If you created a desktops farm, you can use it to create a session-based desktop assignment.
- If you created an applications farm, you can use it to load applications from the servers' underlying RDS-enabled operating system into your Horizon Cloud applications catalog.

<table>
<thead>
<tr>
<th>Status</th>
<th>Farm Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Demo2</td>
<td>Remote Desktops</td>
</tr>
<tr>
<td></td>
<td>Demo1</td>
<td>Remote Desktops</td>
</tr>
</tbody>
</table>

**Note** Creation of an encrypted farm server 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.

**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.

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, Importing New Applications from an RDSH Farm Using Auto-Scan from Farm, and Create a Remote Application Assignment.

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 server 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 server instances, you can start implementing NSX policies on them.

Managing Farms in Horizon Cloud

You can perform several actions on the farms listed on the Administration 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 servers 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 Server** 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 Administration Console might display server 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 Server** value, the system might power on or power off server 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](#).

<table>
<thead>
<tr>
<th><strong>Take Offline</strong></th>
<th>Clicking this button opens a window in which you can select to take a farm offline for maintenance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bring Online</strong></td>
<td>Clicking this button opens a window in which you can select to bring an offline farm back online.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>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 <strong>Farms</strong> column.</td>
</tr>
</tbody>
</table>

**Note**  Deleting the farm deletes all the farm's underlying server 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 **Edit** 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.

### Servers page
The Servers page displays the existing server instances in the farm. The actions you can perform on a selected server are power on or off (depending on the server's current state) and delete.

### 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 currently in a state where the system allows you to cancel it, you can select the check box corresponding to that cancellable task. If you select all of the listed tasks by selecting the topmost check box, only those tasks that are currently cancellable are selected.

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>Not 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></td>
</tr>
<tr>
<td>Assignment Expansion</td>
<td>Supported</td>
<td>Not 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></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></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 Servers in a Farm**

You can perform certain actions on the individual servers 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 **Servers** at the top of the page.
   
   The Servers tab displays, showing a list of servers for 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 servers and clicking one of the buttons at the top of the page.

   **Note**  Server 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 servers.</td>
</tr>
<tr>
<td></td>
<td>- You can select more than one server 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 servers.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected server. To reduce the size of the farm when the server is deleted, select <strong>Yes</strong> under ‘Reduce farm size’ in the dialog.</td>
</tr>
</tbody>
</table>

**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 the Horizon Cloud Administration 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 5-2. Inbound Security Rules in the Pod’s Template NSG

<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 server 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 server virtual machines (VMs) and manages them for rolling maintenance.

In the New Farm wizard, this farm is sized as:

- **Min Servers** = 1
- **Max Servers** = 3
- **Sessions per Server** = 20

In the creation workflow:

1. All three server VMs are fully configured in Microsoft Azure: powered on and joined to the domain.
2. Then servers 2 and 3 are powered down to save the cost of running them.

Server 1 remains powered up and ready to provide user sessions.
As users log on, they are given sessions on server 1. When the occupancy of the available servers, server 1 here, reaches the power management threshold, then another server is powered on (server 2). When two servers are powered on, new user sessions are placed on the least loaded server so that sessions are load balanced between the two powered-on servers. When the number of user sessions reaches the next occupancy threshold as calculated across both powered-on servers, the next server powers on (server 3).

As users log off of their sessions:

1. When the occupancy drops below the low threshold, then one of the servers is marked for quiescing. Typically, the system marks the least loaded server for quiescing.

2. Once marked, existing sessions stay on that server, but no new user sessions are accepted for that server. At that point, any new sessions are only placed on the running servers.

3. When all of the users with existing sessions on the marked server have logged off their sessions, Horizon Cloud powers off that server.

The above steps repeat until the number of running servers reaches the **Min Servers** 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 server 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 servers 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 servers configured for the farm's **Concurrent Quiescing Servers** value. As set by the **Maintenance Type** configured for the farm's rolling maintenance, the system goes through each of the servers and performs the specified maintenance action. The action is not performed on servers that have active user sessions nor on more than the number set in **Concurrent Quiescing Servers**.

**Applications in Your Horizon Cloud Inventory**

The Applications page shows all of the RDSH-backed applications available for assignments. Click the **Inventory** icon and select **Applications** to access the Applications page.

The system categorizes the applications in your Horizon Cloud inventory as remote or custom depending on how the application is added into the inventory.

- Remote applications are those imported from the RDSH farms of type Remote Applications (as shown on the Farms page). From the Applications page, use the **New** button and the **Auto-Scan from Farm** choice to import these applications. When they are imported into the inventory, you can assign these remote applications to your users. See **Importing New Applications from an RDSH Farm Using Auto-Scan from Farm**.
Custom applications are applications in the RDSH images that you manually add into the inventory by using the **New** button on the Applications page and the **Manually from Farm** choice. Even though the best practice is to use the automated way, 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.

You can take the following actions on the Applications page.

<table>
<thead>
<tr>
<th>Action button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Add applications into the inventory from your RDSH images.</td>
</tr>
<tr>
<td>Edit</td>
<td>Select an application to make changes, like giving it a friendly name so you can easily identify it within the list on the Applications page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete an application.</td>
</tr>
<tr>
<td>Rename</td>
<td>Even though you see the <strong>Rename</strong> action in the page, this action is not used for RDSH-backed applications in a Microsoft Azure environment.</td>
</tr>
</tbody>
</table>

**Importing New Applications from an RDSH Farm Using Auto-Scan from Farm**

You make remote applications available for user assignments by importing them from an RDSH applications farm.

If you have more than one applications farm in your environment, repeat these steps to import the applications you want from each of those farms.

**Prerequisites**

Verify that you have at least one applications farm in your inventory by navigating to **Inventory > Farms**.

**Procedure**

1. On the Applications page, click **New**.

2. In the start screen, click **Auto-Scan from Farm**.

   The wizard opens to its first step.
3 Select the location, pod, and applications farm and click **Next** to proceed to the next step.

When you click **Next**, the system scans the selected farm for applications and then displays them for you to select.

4 Select the applications that you want to add to your application catalog.

This wizard step displays the applications that the system's auto-scan process found in the RDS-enabled Windows server operating system used for the farm's RDS servers.

5 Click **Next** to proceed to the next wizard step.

6 (Optional) Customize some of the configurable options for the applications you selected, and then click **Next** to proceed to the next wizard step.

7 Review the summary and click **Submit**.

The system adds the selected applications to the application catalog in your Horizon Cloud inventory.

**What to do next**

Repeat the steps to import the applications you want from your other farms.

**Manually Adding Custom Applications from an RDSH Farm**

Some applications cannot be automatically detected by scanning the farm. You can manually add those applications to your Horizon Cloud applications catalog.

If you have more than one such application, repeat these steps to add the applications you want.

**Prerequisites**

Verify that you have at least one applications farm in your inventory by navigating to **Inventory > Farms**.

**Procedure**

1 On the Applications page, click **New**.

2 In the start screen, click **Manually from Farm**.
3 In the Properties section, specify the following values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the application.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Name for the application that you want displayed to end users when they see the application in their clients, such as in Horizon Client or Workspace ONE.</td>
</tr>
<tr>
<td>Location</td>
<td>Select a location to filter the set of pods displayed in the Pod drop-down list.</td>
</tr>
<tr>
<td>Pod</td>
<td>Select a pod to filter the set of farms displayed in the Farm list.</td>
</tr>
<tr>
<td>Farm</td>
<td>Select the farm that has the RDSH server VM from which you want to add the application.</td>
</tr>
<tr>
<td>Application Path</td>
<td>Specify the path to the application in the RDSH server VM's operating system.</td>
</tr>
<tr>
<td>Icon File</td>
<td>Optional: Upload a PNG file (32 x 32 pixels) to use as the application's icon.</td>
</tr>
</tbody>
</table>

4 In the Advanced Properties section, specify these optional settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application available on Farm</td>
<td>Select Yes to have the system validate the application path. If the application is not located on the farm 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 server VM, you would select No so that the system does not try to find the application there.</td>
</tr>
<tr>
<td>Version</td>
<td>Optional: Version number of the application</td>
</tr>
<tr>
<td>Publisher</td>
<td>Optional: Publisher of the application</td>
</tr>
<tr>
<td>Start Folder</td>
<td>Specify the location in the RDS server VM's Windows operating system that you want the remote application to use as its start folder.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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>Parameters</td>
<td>Specify any command line parameters you want used when the remote application is launched.</td>
</tr>
</tbody>
</table>

5 Click **Submit**.

The system adds an entry for the application to the Applications page.

**What to do next**

Repeat the steps for any applications you want from your other farms.

**Create a Remote Application Assignment**

You create a remote applications assignment from the Assignments page.

**Prerequisites**

Verify that the remote applications are available in your inventory. The Applications page lists the available remote applications.
**Procedure**

1. In the Administration Console, click **Assign**.
2. Click **New**.
3. From the New Assignment start screen, click the Applications icon.

![Applications](image)

Assign Windows Applications to users and groups using remote applications.

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**.

The system creates the assignment and lists it on the Assignments page.
Creating Desktop Assignments in Horizon Cloud

You create desktop assignments in the Administration Console to provision virtual desktops to your end users.

Your Horizon Cloud environment must have at least one image VM in the Published state that the system will use as the operating system on the virtual desktops. In desktop assignments, the published image is used as the Microsoft Windows operating system in the desktops that get assigned to your end users by the desktop assignment.

A Horizon Cloud pod in a Microsoft Azure environment provides for these types of desktop assignments:

- VDI desktop assignments. For steps on creating VDI desktop assignments, see Create a Floating VDI Desktop Assignment and Create a Dedicated VDI Desktop Assignment.
- RDSH session desktop assignments. 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.

Types of Desktop Assignments

In the Horizon Cloud Administration Console, to provide virtual desktops to your end users, you define what are known as desktop assignments. Each desktop assignment associates a published image with a set of users.

For a pod deployed in Microsoft Azure, you can create:

- Dedicated and floating VDI desktop assignments to provide VDI desktops to your end users.
- Session desktop assignments.

**Note** Even though a VDI desktop can have multiple users assigned to it, the VDI desktop can be in use by only one user at a time.

<table>
<thead>
<tr>
<th>Session desktop assignment</th>
<th>Dedicated VDI desktop assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 server instances running in a pod's RDSH farms.</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- An administrator explicitly assigns that specific desktop to that particular user, using the Assign action.</td>
</tr>
<tr>
<td></td>
<td>- 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...</td>
</tr>
</tbody>
</table>
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.

**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 User Environment Manager® and configuring it for your environment. Images created using the automated Import Desktop wizard have the User Environment Manager agent installed by default. For information on configuring persistence of those items, see these resources:

- The *User Environment Manager product documentation*. 
Create an RDSH Session Desktop Assignment

You create session desktop assignments using the Assignments page.

For general information about desktop assignments, see Types of Desktop Assignments.

Prerequisites

Verify you have the following items:

- The Farms page lists at least one farm of remote desktops type. Only farms configured to deliver remote desktops can be used for a session desktop assignment.
- The farm you want to use is in the pod from which you want to deliver the session desktops.
- 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, look in the Assignment page’s Farms column and see if the farm is listed. If it is listed, then it is already being used in a session desktop assignment and you will have to create a new farm.

Procedure

1. Start the New Assignment workflow by clicking **Assign** and clicking **New**.
2. In the New Assignment start screen, click the Desktops icon.

![](image)

The New Desktop Assignment window opens to the first wizard step.

3. 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><strong>Location</strong></td>
<td>Select the location of the pod from which you want the session desktops to be provided.</td>
</tr>
<tr>
<td><strong>Pod</strong></td>
<td>Select the pod.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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>

4. 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**.

5. On the Summary step, review the configuration and then click **Submit**. The system begins the process of configuring the farm's server instances to provide session desktops to the selected users. On the Assignments page, the Status column reflects the current progress.

### Create a Floating VDI Desktop Assignment

You create floating VDI desktop assignments using the Assignments page. For general information about desktop assignments, see [Types of Desktop Assignments](#).

Use these steps to assign a floating VDI desktop to your end users. To assign another type of desktop, see the subtopics listed in [Creating Desktop Assignments in Horizon Cloud](#).

**Prerequisites**

- 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 Master Virtual Machine to an Assignable Image](#).

- Verify that you have valid licensing for the image’s Microsoft Windows 10 operating system. At this time, the Microsoft Azure documentation indicates that to legally run Windows 10 in Microsoft Azure, you must have licensing for Microsoft Windows 10, typically by purchasing an E3 or E5 license. Please verify licensing requirements and restrictions with your Microsoft Licensing distributor.
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.

**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.
- If you are creating this VDI desktop assignment in a pod that was upgraded from manifest version 740 or earlier, and you plan to use an image that existed in the pod before the pod upgrade, do not encrypt the assignment. The encryption process fails if the image was created when the pod was at manifest version 740 or earlier. Such images do not have a working Microsoft Azure Agent, which is required for encrypting VMs. To re-use such an image for an encrypted desktops, you must:
  1. Duplicate the image. This action creates a new master VM based on the existing image. This new master VM has the required Microsoft Azure Agent.
  2. Convert the duplicate to an image. This action creates a sealed image from the duplicate.
  3. Use that new sealed image when creating the encrypted desktop assignment.

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.

**Procedure**
1. Start the New Assignment workflow by clicking Assign and clicking New.
2  In the New Assignment start screen, click the Desktops icon.

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>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 any custom tags you have created. For more information about selecting model VMs, 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 value(s). By default, there is a single filter with the criterion 'Type' the value 'VMware Recommended'. The value changes to 'Favorites' when you have added favorite(s). 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**  
    
    [Image](image-url)  
    
    When you select this option, you can then select one of the following values from a second drop-down menu:  
    - Favorites - Model VMs you have marked as favorites on the VM Types & Sizes page (Settings > VM Types & Sizes). If you have not marked any VMs as favorites, do not select this option.  
    - VMware Recommended - Model VMs recommended by VMware. This is a hard-coded list. 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.  
    - GPU and High Performance - Model VMs with GPU.  
    - **Series**  
    
    [Image](image-url)  
    
    Note: If you plan to select an image with GPU, you must use a model VM with GPU. If you plan to select an image without GPU, you must use a model VM without GPU.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When you select this option, you can then select a series of model VMs 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.</td>
</tr>
<tr>
<td>CPUs</td>
<td>When you select this option, you can then enter a CPU range for model VMs.</td>
</tr>
<tr>
<td>Memory</td>
<td>When you select this option, you can then enter a memory range for model VMs.</td>
</tr>
<tr>
<td>Tag</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 those that you created on the VM Types &amp; Sizes page (Settings &gt; VM Types &amp; Sizes). If you have not created any tags, do not select this option.</td>
</tr>
</tbody>
</table>

You can set additional filters by performing the following steps for each filter:

- Click the Add link.
- Select either And or Or as the operator between the previous filter and the new one you are creating.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>c</strong></td>
<td>Set the new filter by selecting a criterion and entering value(s).   <strong>Note</strong> If the model VM you selected to create the farm becomes unavailable in the future, you will not be able to expand the farm. The farm remains fully functional except for this limitation. To see if a VM type is available, navigate to the VM Types &amp; Sizes page (Settings &gt; VM Types &amp; Sizes).</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.</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.  <strong>Important</strong> 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. 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 VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure and its subtopics.  <strong>Important</strong> 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 <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. 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 master image into a desktop.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>■ If you set the <strong>Encrypt Disks</strong> to <strong>Yes</strong>, 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.</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 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><strong>Assignment Name</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>VM Names</strong></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 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.</td>
</tr>
<tr>
<td><strong>Default Protocol</strong></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><strong>Preferred Client Type</strong></td>
<td>Select the preferred client type used when end users launch their desktops from the Workspace™ ONE™ platform's portal, either a Horizon Client or a browser for HTML Access.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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>
</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 need to use nested Organization Units, see Considerations For Using Nested Active Directory Domain Organizational Units. 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.</td>
</tr>
</tbody>
</table>
| **Run Once Script** | (Optional) Location of a script that you want run in the assignment's desktop VMs after the VM creation process. Note 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
```

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. |
<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 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 <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>Windows license question</td>
<td>For a Microsoft Windows 10 client operating system, Horizon Cloud sets the VDI assignment's desktop instances to use the Windows Client license type by default and you cannot change this setting.</td>
</tr>
<tr>
<td></td>
<td>You cannot change this setting because by design, Horizon Cloud sets the same license type on the VM that would be set if you manually used the Microsoft Azure portal and created the VM from the Azure Marketplace with the selected Microsoft Windows 10 operating system. At this time, the Microsoft Azure documentation indicates that to legally run Windows 10 in Microsoft Azure, you must have licensing for Microsoft Windows 10, typically by purchasing an E3 or E5 license. Please verify licensing requirements and restrictions with your Microsoft Licensing distributor.</td>
</tr>
</tbody>
</table>
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>Option</th>
<th>Description</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 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>a</td>
<td>Click the + icon to add the first row in the Schedule Power Management section.</td>
</tr>
<tr>
<td>b</td>
<td>Type an identifying name for the first schedule.</td>
</tr>
<tr>
<td>c</td>
<td>Select the days for the first schedule.</td>
</tr>
<tr>
<td>d</td>
<td>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><strong>Note</strong></td>
<td>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 dropdown and deselect that selected day.</td>
</tr>
<tr>
<td></td>
<td>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.</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 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.

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

You create dedicated VDI desktop assignments using the Assignments page.

For general information about desktop assignments, see Types of Desktop Assignments.

Use these steps to assign a dedicated VDI desktop to your end users. To assign another type of desktop, see the subtopics listed in Creating Desktop Assignments in Horizon Cloud.

Prerequisites

- 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 Master Virtual Machine to an Assignable Image.

- Verify that you have valid licensing for the image’s Microsoft Windows 10 operating system. At this time, the Microsoft Azure documentation indicates that to legally run Windows 10 in Microsoft Azure, you must have licensing for Microsoft Windows 10, typically by purchasing an E3 or E5 license. Please verify licensing requirements and restrictions with your Microsoft Licensing distributor.

- 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.

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.

- If you are creating this VDI desktop assignment in a pod that was upgraded from manifest version 740 or earlier, and you plan to use an image that existed in the pod before the pod upgrade, do not encrypt the assignment. The encryption process fails if the image was created when the pod was at manifest version 740 or earlier. Such images do not have a working Microsoft Azure Agent, which is required for encrypting VMs. To re-use such an image for an encrypted desktops, you must:
  1. Duplicate the image. This action creates a new master VM based on the existing image. This new master VM has the required Microsoft Azure Agent.
  2. Convert the duplicate to an image. This action creates a sealed image from the duplicate.
  3. Use that new sealed image when creating the encrypted desktop assignment.

- 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.
Procedure

1. Start the New Assignment workflow by clicking Assign and clicking New.

2. In the New Assignment start screen, click the Desktops icon.

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 of the required fields.

<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>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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 any custom tags you have created. For more information about selecting model VMs, 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 'Type' the value 'VMware Recommended'. The value changes to 'Favorites' when you have added favorite(s). 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, you can then select one of the following values from a second drop-down menu:

- Favorites - Model VMs you have marked as favorites on the VM Types & Sizes page (Settings > VM Types & Sizes). If you have not marked any VMs as favorites, do not select this option.
- VMware Recommended - Model VMs recommended by VMware. This is a hard-coded list. 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.
- GPU and High Performance - Model VMs with GPU.

**Note** If you plan to select an image with GPU, you must use a model VM with GPU. If you plan to select an image without GPU, you must use a model VM without GPU.

- Series
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When you select this option, you can then select a series of model VMs 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.</td>
</tr>
<tr>
<td>CPUs</td>
<td>When you select this option, you can then enter a CPU range for model VMs.</td>
</tr>
<tr>
<td>Memory</td>
<td>When you select this option, you can then enter a memory range for model VMs.</td>
</tr>
<tr>
<td>Tag</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 those that you created on the VM Types &amp; Sizes page (Settings &gt; VM Types &amp; Sizes). If you have not created any tags, do not select this option.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>c Set the new filter by selecting a criterion and entering value(s).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the model VM you selected to create the farm becomes unavailable in the future, you will not be able to expand the farm. The farm remains fully functional except for this limitation. To see if a VM type is available, navigate to the VM Types &amp; Sizes page (<a href="#">Settings &gt; VM Types &amp; Sizes</a>).</td>
</tr>
<tr>
<td>Model</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.</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 desktop instances are automatically joined the domain when they are created.</td>
</tr>
<tr>
<td>Encrypt Disks</td>
<td>Select <strong>Yes</strong> so that the desktop instances have encrypted disks.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> 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>NSX Cloud Managed</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></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></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>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 master image into a desktop.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> 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 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>
</tbody>
</table>

---

*VMware, Inc.*
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.</td>
</tr>
<tr>
<td>Preferred Client Type</td>
<td>Select the preferred client type used when end users launch their desktops from the Workspace™ ONE™ platform's portal, either a Horizon Client or a browser for HTML Access.</td>
</tr>
<tr>
<td>Min Desktops</td>
<td>Specify the minimum number and maximum number of desktops you want in this dedicated 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 of 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. 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 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>
</table>
| **Computer OU** | 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 need to use nested Organization Units, see Considerations For Using Nested Active Directory Domain Organizational Units.  
**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. |
| **Run Once Script** | (Optional) Location of a script that you want run in the assignment's desktop VMs after the VM creation process.  
**Note** 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
```

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. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Session Timeout Interval     | 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.  
**Caution** 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.  
The default interval is one week (10080 minutes).  
**Note** 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 **OK** in the next 30 seconds. If the logout occurs, any unsaved user data, such as documents or files, is lost. |
| Windows license question     | For a Microsoft Windows 10 client operating system, Horizon Cloud sets the VDI assignment's desktop instances to use the Windows Client license type by default and you cannot change this setting.  
You cannot change this setting because by design, Horizon Cloud sets the same license type on the VM that would be set if you manually used the Microsoft Azure portal and created the VM from the Azure Marketplace with the selected Microsoft Windows 10 operating system. At this time, the Microsoft Azure documentation indicates that to legally run Windows 10 in Microsoft Azure, you must have licensing for Microsoft Windows 10, typically by purchasing an E3 or E5 license. Please verify licensing requirements and restrictions with your Microsoft Licensing distributor. |
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>
</table>
| **Image Updates**     | The **Concurrent Quiescing Desktops** 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.  

**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. |
| **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 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.  
- 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. |
Option | Description
--- | ---

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 of minimum unassigned desktops for the overlapping time period.

**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.
### Option Description

- **e** 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.

  **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.

- **f** 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.

  **Important** The Min Desktops field in the power management schedules control 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).

  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.

  **Note** 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.

---

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**.

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 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 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 Horizon Cloud Administration 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.

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 7 documentation.

When your environment is integrated with VMware Identity Manager™, 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 Administration 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 master image VM was created using the Import Image 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 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>

4 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.

   a 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/*`

   b Press Enter to add your specified URL pattern to the list.

   c 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 <code>http</code>, <code>https</code>, <code>mailto</code>, <code>callto</code>, 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 Horizon Cloud inventory that you want handling the protocol specified in the <code>Scheme</code> field.</td>
</tr>
<tr>
<td>Strict Match</td>
<td>Select Yes to force an exact match between the name specified in the <code>Target Resource</code> 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 <code>Target Resource</code> field. For example, when the <code>Resource Type</code> is set to <code>Applications</code> and you specify Microsoft Outlook as the target resource to handle the <code>mailto</code> protocol, but the user does not have an assignment for any Microsoft Outlook applications, when <code>Strict Match</code> is set to No, the system will search for a compatible application assigned to that user to handle the <code>mailto</code> 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 in Horizon Cloud, see Configuring Agent-to-Client Redirection.

### Client-to-agent redirection

With client-to-agent redirection, Horizon Client opens a remote desktop or remote application that you specified to handle the URL. For details about configuring client-to-agent redirection in Horizon Cloud, 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 master 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 master 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 7 GPO Bundle ZIP file from the VMware download site at my.vmware.com/web/vmware/downloads.

   The file has a name in the form VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip where x.x.x is the version and yyyyyyy 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 in Horizon Cloud. In Horizon Cloud, you use the 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 Administration 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 5-3. 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</td>
<td>Determines whether users can disable the URL Content Redirection feature.  This setting is not configured by default.</td>
</tr>
<tr>
<td>Redirection plugin loading behavior</td>
<td></td>
</tr>
<tr>
<td>IE Policy: Automatically enable URL</td>
<td>Determines whether newly installed Internet Explorer plug-ins are automatically activated.  This setting is not configured by default.</td>
</tr>
<tr>
<td>Redirection plugin</td>
<td></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>
<tr>
<td>Url Redirection Protocol 'http'</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>- <code>brokerHostname</code>: 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>- <code>remotelItem</code>: display name of the remote desktop or application pool that can handle the URLs specified in <code>agentRules</code>.</td>
</tr>
<tr>
<td></td>
<td>- <code>clientRules</code>: the URLs that should be redirected to the client. For example, if you set <code>clientRules</code> to <code>*.mycompany.com</code>, all URLs that include the text <code>mycompany.com</code> are redirected to the Windows-based client and are opened in the default browser on the client.</td>
</tr>
<tr>
<td></td>
<td>- <code>agentRules</code>: the URLs that should be redirected to the remote desktop or application specified in <code>remotelItem</code>. For example, if you set <code>agentRules</code> to <code>*.mycompany.com</code>, all URLs that include <code>mycompany.com</code> are redirected to the remote desktop or application.</td>
</tr>
<tr>
<td></td>
<td>When you create agent rules, you must also use the <code>brokerHostname</code> option to specify the IP address or fully qualified domain name of the Connection Server host, and the <code>remotelItem</code> 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 <code>vdmutil</code> command-line utility.</td>
</tr>
<tr>
<td></td>
<td>This setting is enabled by default.</td>
</tr>
<tr>
<td>Url Redirection Protocol ' [...] '</td>
<td>Use this setting for any protocol other than HTTP, such as HTTPS, email, or <code>callto</code>.</td>
</tr>
<tr>
<td></td>
<td>The options are the same as for <code>Url Redirection Protocol 'http'</code>. 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.</td>
</tr>
<tr>
<td></td>
<td>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 <code>mycompany.com</code>, 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.</td>
</tr>
</tbody>
</table>

VMware, Inc. 259
Managing Assignable Images

After you create an assignable image, you can manage that image using the Administration Console. 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-enabled server images) or VDI desktops. 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.

Actions You Can Perform on Assignable Images

You can perform several actions on the assignable images listed on the Administration Console's Images page. These assignable images are also referred to as sealed images or published 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.
3 Click one of the action buttons to perform an action on this image.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename</td>
<td>Even though you see the Rename action in the page, this action is not used for images in a Microsoft Azure environment.</td>
</tr>
<tr>
<td>Duplicate</td>
<td>The duplicate workflow is typically used when updating a farm's or VDI desktop assignment's underlying master base image, for example, to install or update applications in the base 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 RDS-Enabled Images Used for Farms and Change Images Used for VDI Desktop Assignments. When you click Duplicate, you must enter a name for the new duplicated VM. After you enter a new name and click Save, the system clones the sealed image's VM to make a new master VM, and lists the new master VM on the Imported VMs page. When you see that the Imported VMs page reports the new master 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 New action or by selecting the image on the Imported VMs page and selecting Convert to Image. 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. You can monitor the progress of the duplicate image on the Imported VMs page or using the Activity page.</td>
</tr>
</tbody>
</table>
| Update Agent | 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  
- Update Agent Software for Images Used by Floating VDI Desktop Assignments  
Important 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. |
To perform one of the other available actions, click ... and select the drop-down option of your choice.

**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. They are used when manually creating a master VM, as described in Manually Build the Master Virtual Machine in Microsoft Azure.

<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 it is in use by an RDSH farm or a VDI desktop assignment. |
| 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 re-publish 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 you see this action in the Administration Console, this action is not used for images in a Microsoft Azure environment. |
| Bulk Assign Image| Assigns the image to multiple assignments/farms of the immediate parent image (the image from which the selected image was duplicated/updated). In the Bulk Assign Image dialog, select assignments/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 along with 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 WinSvr2016. This image belongs to a pod named East-Coast-Stores and is referenced by two RDSH farms.
Change RDS-Enabled Images Used for Farms

After you publish your initial RDS-enabled 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.

**Note** If you are changing the RDS-enabled image to update the Horizon Cloud agent-related components, you use a different procedure. See [Update Agent Software for RDSH Images](#).

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 master VM, and lists the new master VM on the Imported VMs page.

2. When you see that the Imported VMs page reports the new master 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 RDSH 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 Master Virtual Machine to an Assignable Image.

Note When using the Microsoft Remote Desktop Client as your RDP software to connect to the master 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 Administration 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 master VM, and lists the new master 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 master VM's agent is active.
4. When you see on the Imported VMs page that the new master VM's agent is active, use the VM's IP address and your RDP software to connect to the RDS-enabled Windows server 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 RDS-enabled Windows server 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 server operating system, perform your intended updates.
   
   If you are installing additional third-party applications, see the steps described in Customize the Guest Windows Server Operating System of the Master Server Image Virtual Machine.
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.

The farms you update automatically delete and re-create their server 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.

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 master VM, and lists the new master VM on the Imported VMs page.

2 When you see that the Imported VMs page reports the new master 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 Master Virtual Machine to an Assignable Image.

Note When using the Microsoft Remote Desktop Client as your RDP software to connect to the master 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 Administration 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 master VM, and lists the new master 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 master VM's agent is active.

4 When you see on the Imported VMs page that the new master 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 Customize the Guest Windows Client Operating System of the Master VDI Desktop Virtual Machine.
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.

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

After you create an assignment, you can manage the assignment using the Administration Console. The types of assignments in your environment depend on what you have created.

You work with assignments from the Administration Console's Assignments page. The types of actions you can use on an assignment depends on the assignment's type. As an example, on the Assignments page, 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.

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>
<tbody>
<tr>
<td>VDI desktop</td>
<td>Create a Floating VDI Desktop Assignment</td>
</tr>
<tr>
<td></td>
<td>Create a Dedicated VDI Desktop Assignment</td>
</tr>
<tr>
<td>Session-based desktop</td>
<td>Create an RDSH Session Desktop Assignment</td>
</tr>
<tr>
<td>Remote application</td>
<td>Create a Remote Application Assignment</td>
</tr>
<tr>
<td>URL redirection customization</td>
<td>See Create a URL Redirection Customization and Assign it to Users</td>
</tr>
</tbody>
</table>

At a page level, you can select the check box next to an existing assignment and click one of the buttons to perform its associated action on the assignment.

**Edit**

Clicking this button launches a wizard in which you can change the editable settings in the assignment. The 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 links.

Alternatively, instead of using the **Edit** button, you can click an assignment's name and update the settings from the assignment's summary page.

**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 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** Due to a known issue in this release, 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.
**Bring Online**
Clicking this button opens a window in which you can select to bring an offline assignment back online.

**Delete**
You use this button to delete the selected assignment. See Delete an Assignment.

**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. From the Assignments page, click a VDI desktop assignment's name to see its detailed pages. Initially the Summary page is displayed.

**Summary page**
The Summary page displays the VDI desktop assignment's current settings. For each page section, you can click Edit 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 instances in the VDI desktop assignment. The actions you can perform on a selected desktop are power on or off (depending on the desktop's current state) and delete.

- For a desktop in floating VDI desktop assignments, you can power it off (if the desktop is powered on), and log off or disconnect the currently connected user (if any). Even though additional actions might be visible, they are disabled.

  **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.

- For a desktop in dedicated VDI desktop assignments, you can power it on or off (depending on the desktop's current state), restart it, log off or disconnect the currently connected user (if any), assign the desktop to
a specific user (if the desktop is unassigned), and unassign the desktop (if the desktop is assigned to a user). Unassigning the desktop removes the mapping of the desktop to that user and makes it available to be mapped to a different user.

**Note**  Do not manually power on a desktop, even if the action is available in the Desksops 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. If you select all of the listed tasks by selecting the topmost check box, only those tasks that are currently cancellable are selected.

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>Not Supported</td>
</tr>
<tr>
<td>Note</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></td>
</tr>
<tr>
<td>Assignment Expansion</td>
<td>Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Note</td>
<td>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></td>
</tr>
<tr>
<td>Convert VM to Image</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Note</td>
<td>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></td>
</tr>
<tr>
<td>Note</td>
<td>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></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.

**View an Assignment**

Use the Assignments page to get an overview or detailed view of all the assignment types. You can view the details of individual assignments by clicking the respective assignment. For some assignment types, you can click on hyperlinks in the page to navigate to where you can perform actions on the individual assets used in that assignment.

**Procedure**

1. In the Administration Console, open the Assignments page by clicking **Assign**.
2. On the Assignments page, click the name of an assignment to see detailed information.
   
   The assignment opens to its Summary page. The information available is specific to each assignment type.
3 Navigate through the information depending on the assignment type.

<table>
<thead>
<tr>
<th>Assignment Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session-based desktop</td>
<td>View the information on the Summary page 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 servers.</td>
</tr>
<tr>
<td>Remote application</td>
<td>View the information on the Summary page 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 servers.</td>
</tr>
<tr>
<td>URL redirection customization</td>
<td>View the information on the Summary page and Optionally click <strong>Edit</strong> to update specific properties.</td>
</tr>
<tr>
<td>VDI desktop</td>
<td>View the information on the Summary page and click <strong>Desktops, 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>
<tr>
<td><strong>Note</strong></td>
<td>If this VDI desktop assignment was created in a pod in Microsoft Azure that has a pod manifest version lower than 1101, the <strong>License Type</strong> field displays <strong>No License</strong> even though the assignment has inherited the Windows 10 client license from the image used for this assignment. If you click the <strong>Edit</strong> link, the editing window shows that the Windows 10 client license is being used.</td>
</tr>
</tbody>
</table>

**Edit an Assignment**

You can edit any assignment type from the Assignments page. The specific properties you can change depends on the assignment type.

**Procedure**

1 In the Administration Console, click **Assign**.

2 Select the check box next to the assignment you want to edit and click **Edit**.

The corresponding assignment type's wizard appears.
3 Proceed through the wizard making your changes and click **Submit**.

For instructions on filling in the fields in the wizard, see the topic for creating the type of assignment you are editing. Those topics are listed in **Managing Assignments**.

## Delete an Assignment

You can delete assignments if they are no longer needed. From the Assignments page, **Delete** is under the ... menu (... > Delete).

The specific steps for deleting an assignment vary depending on the assignment type.

<table>
<thead>
<tr>
<th>Assignment Type</th>
<th>Details</th>
</tr>
</thead>
</table>
| Floating VDI desktop assignment        | Select the assignment on the Assignments page and click ... > Delete. 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 Administration 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.  
**Note** 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 **Min Desktops** and **Max Desktops** values. |
| 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 ... > Delete, select Yes under 'Reduce assignment size' 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 Assignments 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 Assignments 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 from the Assignments page by selecting it and clicking ... > Delete. |
| Session desktop assignment             | Select the assignment on the Assignments page and click ... > Delete. Because session desktop assignments are for entitling users to connect to the RDSH servers in a farm, no VMs are actually deleted when you delete this assignment type. The assignment record is removed from the system. |
| Application assignment                 | Select the assignment on the Assignments page and click ... > Delete. |
| URL redirection customization assignment| Select the assignment on the Assignments page and click ... > Delete. |
Resizing a VDI Desktop Assignment

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 for how to edit a VDI desktop assignment using the 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 View an Assignment.

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 Administration 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. |

### 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 Horizon Cloud Administration 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 your end-user clients' access to their VDI desktops using Blast and PCOIP and USB redirection.

**Table 5-4. Inbound Security Rules in the Pod's Template NSG**

<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.

**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 mark some VMs as favorites or add custom tags, both of 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, or Create a Dedicated VDI Desktop Assignment. The filter option functions identically in all three cases, so the information describing the option is the same in these three topics.

The VM Types and Sizes page (Settings > VM Types and Sizes) displays a list of all VMs available in the standard Microsoft Azure region. These VMs are then filtered based on the settings you make. VMware has also removed a few VMs that are not recommended for VDI use cases.

The information displayed for each VM is shown in the table below. Click the Edit button to change editable items for one or more VMs.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show</td>
<td>Indicates whether a VM is displayed in the Model drop-down menu in the farm and desktop assignment creation wizards. By default, this is selected for all VMs.</td>
</tr>
<tr>
<td>Favorite</td>
<td>Select to mark the VM as a favorite. You can filter by favorites when selecting a model in the farm and desktop assignment creation wizards.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the VM (not editable).</td>
</tr>
<tr>
<td>Tags</td>
<td>Free text field where you can enter your own custom tags. You can filter by these tags when selecting a model in the farm and desktop assignment creation wizards.</td>
</tr>
<tr>
<td>Details</td>
<td>Specifications of the VM (not editable). VM configurations particularly recommended by VMware are also marked with a green “Recommended” badge.</td>
</tr>
</tbody>
</table>

**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 master 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 Administration
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 Administration 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
Administration 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 User Environment Manager Agent Software**

Starting with this Horizon Cloud release, installation of the User 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 master image VM, when you run the Import Desktop
workflow or manually create a master image VM. When you **Create a Master Virtual Machine
Automatically from the Microsoft Azure Marketplace**, the Horizon Agents Installer runs behind the
scenes to install the agents. When you **Manually Build the Master Virtual Machine in Microsoft Azure**, 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 User 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 User 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 starting with this release, the User 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 prior to this release, the User 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 User Environment Manager install file path depends on how you installed the User Environment Manager agent in that manually created VM:

- If you installed the User Environment Manager agent using the Horizon Agents Installer version 19.2, the User 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 User Environment Manager agent using the separate stand-alone User Environment Manager installer, the User 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 User 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**

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 at 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

Before you can use the Update Agent action on an RDSH image in your Horizon Cloud environment, the image must already have agent-related software at the following versions or later:

- Version 7.3.2 for the Horizon View Agent (64-bit)
- Version 17.2 for the Horizon DaaS Agent

You can see the agent version number in the properties on the image's details page. From the Images page, click on the image to open its details page.

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.

   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. In each farm's details page, click the General Settings **Edit** link to open a window, 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.

The following screenshots illustrate the location of the **Edit** link on the farm's details page and the window that subsequently opens when you click that link.

In this window, use the **Image** drop-down to select the new duplicate image that has the updated agents. In this example, the farm goes from using its original `pat2016` image to the new `pat2016-1` image that resulted from the agent update workflow.
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, use the Assignment page’s Update Agent action. You make the agent update on the specific dedicated VDI desktop assignment. This method is different than for agent updates for floating VDI desktop assignments.

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.

Before you can use the Update Agent action on a dedicated VDI desktop assignment in your Horizon Cloud environment, that assignment must be using an image that has agent-related software at the following versions or later:

- Version 7.3.2 for the Horizon View Agent (64-bit)
- Version 17.2 for the Horizon DaaS Agent

If the assignment's agent-related software is at an earlier version, the Assignments page will not show the blue dot indicator next to the assignment. You can see the agent version number in the Agent Software section of the dedicated VDI desktop assignment's summary page. From the Assignments page, click the assignment to open its details page.

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.

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 upgrade 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**.

   - 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 Administration Console's Assignments page 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.
### 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.
### Examples

<table>
<thead>
<tr>
<th><strong>Available VMs to Users</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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>
<tr>
<td>Assignment has 20 desktops and <strong>Available VMs to Users</strong> = 80%</td>
<td>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.</td>
</tr>
<tr>
<td>Assignment has 100 desktops and <strong>Available VMs to Users</strong> = 80%</td>
<td>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 40.</td>
</tr>
<tr>
<td>Assignment has 100 desktops and <strong>Available VMs to Users</strong> = 25%</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

**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.

**Caution** For a dedicated VDI desktop assignment, the recommended way to update the Horizon agent software is to run the agent update operation on the assignment itself, from the Assignments page (see Update Agent Software for Dedicated VDI Desktop Assignments). Even though you can technically follow the steps here on the Images page to run the agent update operation and make the updated duplicate image, when you edit a dedicated VDI desktop assignment to use such an image, only unassigned desktop VMs in that dedicated VDI desktop assignment are recreated to use the updated image. The system does not touch the assigned desktop VMs. When you edit a dedicated VDI desktop assignment to use an image that is different from the dedicated VDI desktop assignment's original one, assigned desktop VMs remain using the original image until they become unassigned again.

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.

![Images Table]

**Prerequisites**

Before you can use the **Update Agent** action on an image in your Horizon Cloud environment, the image must already have agent-related software at the following versions or later:

- Version 7.3.2 for the Horizon View Agent (64-bit)
- Version 17.2 for the Horizon DaaS Agent

You can see the agent version number in the properties on the image’s details page. From the Images page, click on the image to open its details page.
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**.
(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.

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. In each assignment's details page, click the General Settings Edit link to open a window, 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 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 see them in 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 subscription information, as needed.

You primarily use the Capacity page to work with your pods. For details about the Capacity page, see Capacity Page.

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 Dashboard Page.
Obtain the Pod’s Load Balancer Information to Map in your DNS Server

When a deployed Horizon Cloud pod in Microsoft Azure has a Unified Access 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's deployed Microsoft load balancer information. For an external Unified Access Gateway configuration, you 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, you map the FQDN that you entered in the deployment wizard to the pod's Microsoft Azure internal load balancer's private IP address.

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 Unified Access Gateway configuration

When you specify using an external Unified Access Gateway configuration in the pod deployment wizard, the deployed Unified Access Gateway is configured with a Microsoft Azure public load balancer and load balancer public IP address that has an auto-generated public FQDN in the form vwm-hcs-podID-uag.region.cloudapp.azure.com, where podID is the pod's UUID and region is the Microsoft Azure region where the pod is located.

For the external Unified Access Gateway configuration, 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.

Internal Unified Access Gateway configuration

When you specify using an internal Unified Access Gateway configuration in the pod deployment wizard, the deployed Unified Access Gateway is configured with a Microsoft Azure internal load balancer and private IP address.

For the internal Unified Access Gateway configuration, your DNS server must map your FQDN to the internal load balancer's 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.

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 Administration 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 Unified Access Gateway configuration. If the pod only has an internal configuration, then only the **Internal UAG** section appears and not the section for the internal 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>Internal</td>
<td>The displayed value is the Microsoft Azure internal load balancer's private IP address. This numeric IP address is assigned to the internal load balancer from the pod's desktop subnet.</td>
</tr>
<tr>
<td>External</td>
<td>The displayed value is the Microsoft Azure external load balancer'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 <code>podID</code> is the pod's ID value. That pod ID is displayed on its details page.</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 internal-load-balancer-private-IP</td>
</tr>
<tr>
<td>External</td>
<td>ourApps.ourOrg.example.com vwm-hcs-podID-uag.region.cloudapp.azure.com</td>
</tr>
</tbody>
</table>

**Upload SSL Certificates to a Horizon Cloud Pod for Direct Connections**

Upload SSL certificates to the pod itself to ensure that Horizon Clients making direct connections to the pod in Microsoft Azure can have trusted connections.

These steps are for uploading an SSL certificate so that it gets installed on the pod's manager VM. Putting an SSL certificate on the pod's manager VM supports the scenarios that need trusted connections to the pod:

- Your pod is not configured with Unified Access Gateway at all and you are having end-user client connections direct to the pod.
- You are not using the internal Unified Access Gateway configuration and are having end-user client connections direct to the pod, such as using a VPN.
- You plan to use VMware Identity Manager™ with the pod.

If the pod has a Unified Access Gateway configuration, your end-user connections can go through the load balancer to the pod's Unified Access Gateway instances and use the certificate that you provided for the Unified Access Gateway configuration.

In general, uploading an SSL certificate to the pod directly is a recommended practice, because that ensures Horizon Clients that might make direct connections to the pod environment can have trusted connections, and is the supported configuration for using VMware Identity Manager™ with the pod.

However, connections direct to the pod using HTML Access (Blast) appear as untrusted connections in the end user's browser. The end-user browsers display the typical untrusted certificate error when they make their connections direct to the pod. To have connections using HTML Access (Blast) avoid the displayed untrusted certificate error, you must have those connections use the load balancer and Unified Access Gateway instances from the pod's Unified Access Gateway configuration. If you do not want to expose your fully qualified domain name to the Internet, you can deploy an internal Unified Access Gateway configuration. This internal Unified Access Gateway configuration uses a Microsoft internal load balancer to which end users who are internal to your corporate network can point their connections.

**Important** During the procedure of uploading the certificate, the environment is temporarily unavailable and you cannot perform administrator operations. Upload the certificates after confirming that no users are on the system and no running tasks exist, such as importing base images, publishing images, provisioning farms or desktops, assigning desktops, and so on.
Prerequisites

**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 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.

Verify the following items.

- In your DNS server, you have mapped a fully qualified domain name (FQDN) to the pod's tenant IP address. You can locate the pod's tenant IP address from the pod's details page, navigating from the Administration Console's Capacity page. This mapping is needed so that clients can use that FQDN for trusted connections to the pod.

- You have a valid trusted SSL certificate based on that FQDN.

- That SSL certificate is in the following format needed for you to provide it into the Administration Console's Upload Certificate window. Because the Administration Console's Upload 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 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.

The following screenshot illustrates the Upload Certificate window and how it expects those three separate files.
The CA certificate file and the SSL certificate files for this upload must be in PEM format, which is a BASE64-encoded DER representation of an X.509 certificate. They 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-----
```

The private key must not have a password or passphrase associated with it. The .key file looks like the following example:

```
-----BEGIN RSA PRIVATE KEY ----- 
MIIEpQIBAAKCAQEAoJmURboiFut+R34CNFibb9fjtI+cp0arUzqe8oGKFzEE/jmj
...............
-----END PRIVATE KEY-----
```

**Procedure**

1. Select **Settings > Capacity**.
2. Open the pod's summary page by expanding the pod's row and clicking its name.
3. Click **More > Upload Certificate**.

   The Upload Certificate window opens. The following screenshot is an example of the window.

   ![Upload Certificate Window](image)

4. For each of the certificate files listed in the Upload Certificate dialog box, 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 in the window, click **Save**.

   The following screenshot is an illustration of the window with all certificate files listed before saving them to the system.
The Administration Console will be unresponsive for 5 to 10 minutes for all administrators while the certificates are applied.

6 When the system is responsive again, refresh the browser page and use your credentials to reauthenticate.

7 Verify that the certificates are shown as valid in the Pod Certificates section of the pod's details page.

**Update the Subscription Information Associated with Deployed Pods**

In some circumstances, you might want to update the subscription information that is associated with your deployed pods. For example, if you created the subscription's application key to have it expire in one year, the year passes, and the key expires, you would have to use the Microsoft Azure portal to create a new key for the subscription. After creating the new key, then you need to update the subscription information in the Administration Console to enter the new key there.

For a description of the subscription information fields, see Deploying Horizon Cloud Pods into Microsoft Azure from the Capacity Page.

**Procedure**

1 In the Administration Console, click **Settings > Capacity**.

2 Click **Type** to display the **Type** view.

3 Open the Subscription Details window by clicking the hyperlink name that is displayed for the subscription.

4 Modify the values you want to update.

   You can change the **Subscription Name**, **Application ID**, and **Application Key**.

   **Note** The **Subscription ID** and **Domain ID** values cannot be updated.

5 Click **Save**.
Examine a Subscription’s Current Usage of Your Microsoft Azure Limits

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.

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 Administration Console, navigate to **Settings > Capacity**, and click **Type**.

2. Expand any collapsed sections until you see the name of the subscription that you want to examine.

   The percentage of your Microsoft Azure subscription's quota that the pods in that subscription are using is displayed next to the subscription’s name.

   ![Table of subscription usage](image)
Click on **show details** to see the subscription's usage of various Microsoft Azure limits.

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 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. The normal update process takes place without incurring any system downtime.

**Important** If the pod is already integrated with the cloud-hosted VMware Identity Manager™ and you are using the Linux connector version 2017.12.1.0, a best practice is to update the connector to the latest supported version before updating the pod. For 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). Follow the steps in Preparing to Upgrade VMware Identity Manager Connector. Then upgrade your pod.
Updating the software in your deployed pod results in appropriately updating the core pod management software and the Unified Access Gateway software. For example, a pod software update can include updates for the pod management software or for the Unified Access Gateway software or for both.

Use the Capacity page to see at a glance which pods have updates available for them. Navigate to Settings > Capacity. A visual indicator appears next to those pods that have updates available for them. When your cursor hovers over the indicator, a pop-up displays additional details.

The following screenshot illustrates where the indication of an available update appears in the Location view of the Capacity page.

You can see the update details for a specific pod by selecting Settings > Capacity and clicking the pod to open its summary page. When an update is available, an on-screen message describing the update appears at the Version No entry. The displayed version number corresponds to the version of the pod's software manifest.
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, Update Agent Software for Dedicated VDI Desktop Assignments, and Update Agent Software for Images Used by Floating VDI Desktop Assignments.

The pod software update process is performed in the following stages.

1. Downloading new software, an automatic process
2. Scheduling the update
3. Migrating to the new version

**Stage One: Download New Software**

The first stage, downloading new software, takes place when a new version of the pod's software is available. Horizon Cloud triggers the deployed pod to download the new version of the software. The deployer software builds an inactive parallel pod environment. This stage is transparent to you and does not cause any downtime.

When the first stage finishes, a visual indication that an update is available appears on the Capacity page next to the pods which are at a level lower than the update.
Stage Two: Scheduling Update of a Pod

The second stage is scheduling the update. You schedule the update on a pod from the pod's summary page, by selecting **Update > Schedule**.

**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 Administration Console displays the scheduled time in a top banner.

**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.
You can reschedule the time for the update at any time prior to the scheduled time, if required by your organization's needs.

**Note** If the Radius server is deployed in same VNET, then you must also 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, and does not have to be repeated for future updates.

### Stage Three: Migrating to the New Version

The third stage, migration to the new version, takes place at the scheduled time, at which point, the system triggers the migration. The process takes from five to ten minutes to complete, and migrates the data and configuration from the running environment to the new environment. After everything is migrated to the new environment, the pre-update environment is powered off.

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.

When the update 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.

**Note** After a pod update, the old pod environment remains in your Microsoft Azure resource groups in a powered-off state in case rollback is needed. The old powered-off pod environment is automatically deleted in the next update cycle.
Backup and Restore Service for 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 Administration 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 Administration 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.

### 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 Administration 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**.
In the Edit Pod window, edit the settings in the **NTP Servers** field.

Click **Save & Exit** to save the new settings to the system.

### Change the FQDN and Certificate Used for the Pod’s Unified Gateway Configuration

You can change the fully qualified domain name (FQDN) and certificate that is used by the Horizon Cloud pod's Unified Gateway configuration using the Administration Console's Edit Pod wizard. You launch that wizard from the pod's summary page.

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 both types of Unified Gateway configurations, the Unified Access Gateway instances are configured with FQDN and SSL certificate information. Follow these steps when you need to change the FQDN and certificate for either type of configuration, or for both.

**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:

- A fully qualified domain name (FQDN) 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.

- 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.

### Procedure

1. In the Administration 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 Complete the following steps for the change you want to make, in either the **External UAG** section or **Internal UAG** section.

   a Change the **FQDN** value to your new one.
   
   b Click **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 FQDN you entered 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, 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's Load Balancer Information to Map in your DNS Server for details.

**Add a Unified Access Gateway Configuration to a Pod, With or Without Two-Factor Authentication**

When you initially deployed a Horizon Cloud pod into Microsoft Azure without either Unified Access Gateway configuration types, or with only one type, you can add a Unified Access Gateway configuration to the pod using the Administration Console's Edit Pod wizard. You launch that wizard from the pod's summary page.
As described in Chapter 5 Introduction to Horizon Cloud Pods in Microsoft Azure, a pod can have an external Unified Access Gateway configuration or an internal one or both. You can use this workflow to add the type that the pod does not already have. You can also specify two-factor authentication settings for the Unified Access Gateway configuration that you are adding to the pod.

**Important** When modifying the pod using these steps, keep in mind the following points:

- If an existing Unified Access Gateway configuration on the pod is not already configured with two-factor authentication, you cannot use this workflow to add the two-factor authentication settings to that existing Unified Access Gateway configuration. This release does not support adding the two-factor authentication configuration to Unified Access Gateway instances after those instances are already deployed.

- 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**

To complete the fields in the Edit Pod wizard, you must provide the information as described in Prerequisites When Deploying With a Unified Access Gateway Configuration. If you are also specifying two-factor authentication settings for the configuration you are adding, you must provide the information described in Prerequisites WhenDeploying With a Two-Factor Authentication Configuration.

**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 Administration 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.
If you are adding the external configuration to a pod that does not have it, set the **Enable External UAG?** toggle to **Yes** and complete the fields in the **External UAG** section.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable External</td>
<td>When <strong>Yes</strong> is selected, access to desktops and applications is enabled for users located outside of your corporate network. The pod includes a Microsoft Azure public load balancer and Unified Access Gateway instances to enable this access.</td>
</tr>
<tr>
<td>UAG?</td>
<td><strong>Note</strong> Leaving the default <strong>Yes</strong> setting is recommended.</td>
</tr>
<tr>
<td></td>
<td>When set to <strong>No</strong>, clients must either connect directly to the pod and not through Unified Access Gateway, or they connect through an internal Unified Access Gateway configuration. In the case of clients connecting directly to the pod and not through Unified Access Gateway, some post-deployment steps are required. In this case, after the pod is deployed, follow the steps in <a href="#">Upload SSL Certificates to a Horizon Cloud Pod for Direct Connections</a>.</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.</td>
</tr>
<tr>
<td></td>
<td><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>DMZ Subnet</td>
<td>When <strong>Use Existing Subnet</strong> is set to <strong>Yes</strong> in the preceding 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>(CIDR)</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 <strong>Use Existing Subnet</strong> is set to <strong>No</strong> 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 deployed public load balancer.</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 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.</td>
</tr>
<tr>
<td></td>
<td>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>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **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. |
| **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**                   | If you are adding the internal configuration to a pod that does not have it, set the **Enable Internal UAG?** toggle to **Yes** and complete the fields in the **Internal UAG** section.                                                                                                                           |
| **Enable Internal UAG?**| When **Yes** is selected, trusted access to desktops and applications is enabled for HTML Access (Blast) connections for users located inside of your corporate network. The pod includes a Microsoft Azure internal load balancer and Unified Access Gateway instances to enable this access.                                                                 |
| **FQDN**                | 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.  
**Important** This FQDN cannot contain underscores. In this release, connections to the Unified Access Gateway instances will fail when the FQDN contains underscores. |
| **DNS Addresses**       | Optionally enter addresses for additional DNS servers that Unified Access Gateway can use for name resolution, separated by commas. When configuring this internal 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 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. |
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.

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.

6 In the section for whichever Unified Access Gateway configuration fields you completed in the previous steps, optionally configure the end users' desktops to use RADIUS two-factor authentication by using the following steps.

a Select Yes for the Enable 2 Factor Authentication? toggle.

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

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

In this release, RADIUS authentication is supported.

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

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

Option | Description
--- | ---
Display Name | Optionally provide a name that the system will display to the end users on the Horizon Cloud login screen to identify which RADIUS system they are using to authenticate for access.

Display Hint | Optionally enter a text string that the system will display in the message on the login screen to direct users to enter the correct RADIUS passcode.

Name ID Suffix | Even though this field is visible, it is not used in this release.

Number of Iterations | Enter the maximum number of failed authentication attempts that a user is allowed when attempting to log in using this RADIUS system.

Maintain Username | Select Yes to maintain the user's RADIUS username during authentication to Horizon Cloud. When Yes is selected:

- 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 you select No, the user is able to type a different user name in the login screen.
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>

(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. Set the Auxiliary Server toggle to Yes and complete the fields as described for the Primary Server section.

7 Click Save & Exit.

A confirmation message appears asking you to confirm the start of the workflow.

8 Click Yes to start the workflow.

Until the system is finished deploying the elements for the configuration you added, the pod summary page's section for that configuration type shows Pending status.

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

For the newly added Unified Access 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's Load Balancer Information to Map in your DNS Server for details.

If you specified RADIUS two-factor authentication for the configuration you added, you must configure your RADIUS system with the IP address of the added configuration's load balancer as a client allowed to make requests of that RADIUS system. The Unified Access Gateway instances authenticate requests from the RADIUS system through that address.

Removing a Subscription Entry

You can remove a subscription entry from your Horizon Cloud environment if no pods are associated with that subscription entry. Only when no pods are associated with a subscription entry does the Remove Subscription action display in the Administration Console on the Type view of the Capacity page.

Prerequisites

Important   In this release, access to the Capacity page is possible only when you have at least one deployed pod that has completed the Active Directory registration process. As a result, to remove the subscription information from your Horizon Cloud:

1 First deploy a pod using new subscription information. In the deployment wizard for the new pod, enter the new subscription information.

2 Delete the pods that are associated with the old subscription. Because the system prevents you from removing a subscription that pods are using, the Remove Subscription action is not displayed on the Capacity page if any pods are using the subscription.

When the Capacity page no longer displays any pods that were associated with the old subscription, the Remove Subscription action is displayed on the Capacity page.

Procedure

1 On the Administration Console’s Capacity page, display the Type view by clicking Type
2 Expand the Microsoft Azure section and locate the subscription you want to remove.

3 Click **Remove Subscription**.

4 In the confirmation box, click **Remove**.

The subscription entry is removed from the system. If you later decide to use the same set of subscription information for a pod, you re-enter the details when deploying a new pod.

**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 in 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 .pkcs 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 .pkcs 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:

```shell
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 n 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-----
-----BEGIN CERTIFICATE-----
.... (the intermediate CA certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
.... (the trusted root certificate)
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
.... (your server key from mycaservercertkeyrsa.pem)
----- END RSA PRIVATE KEY-----
```

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.

The resulting PEM file meets the requirements of the pod deployment wizard.
DNS, Ports, Protocols 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 Horizon Cloud to access the Domain Name Service (DNS) addresses it needs. In addition, your DNS must resolve specific names as described in this topic. Then, after the pod is successfully deployed, specific ports and protocols are required for ongoing Horizon Cloud operations.

DNS Requirements for the Pod Deployment Process and Ongoing Operations

You must ensure the following DNS names are resolvable and reachable from the pod's management and tenant subnets using the specific ports and protocols as listed 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 such that Horizon Cloud has the ability to contact the DNS addresses on the ports that it requires. Otherwise, the pod deployment process will fail.

Table 5-5. Pod Deployment and Operations DNS Requirements

<table>
<thead>
<tr>
<th>Source Pod Subnet</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, depending on which Horizon Cloud control plane is specified in your Horizon Cloud account: cloud.horizon.vmware.com cloud-eu-central-1.horizon.vmware.com cloud-ap-southeast-2.horizon.vmware.com</td>
<td>443</td>
<td>TCP</td>
<td>Horizon Cloud control plane. cloud.horizon.vmware.com is in the United States cloud-eu-central-1.horizon.vmware.com is in Europe cloud-ap-southeast-2.horizon.vmware.com is in Australia</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>
<tr>
<td>Source Pod Subnet</td>
<td>Destination (DNS name)</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>Management</td>
<td>d1mes20qfad06k.cloudfront.net</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.</td>
</tr>
<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's 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>Source Pod Subnet</td>
<td>Destination (DNS name)</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>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>
| 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 | 443  | 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>
<thead>
<tr>
<th>Source Pod Subnet</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>Source Pod Subnet</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant</td>
<td>d1mes20qfad06k.cloudfront.net</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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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>
<tr>
<td></td>
<td>- query-prod-ap-southeast-2.cms.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Ports and Protocols Required by the 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.
During those processes, that jump box VM communicates with the pod's manager VM using SSH to the manager VM's 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 VM's port 22 must be met. The manager VM's port 22 must be allowed between the jump box VM as a source and the manager VM as a destination. Because these VMs are assigned IP addresses dynamically, the network rule 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.

**Note**  Ongoing pod operations do not require availability of port 22 on the pod's manager 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 your pod's manager 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 Required 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.

**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 5-6. Pod Operations Ports and Protocols**

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port(s)</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<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, 8</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>321, 11</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>
</tbody>
</table>
### Ports and Protocols Required by the Jump Box During Pod Deployments and Pod Updates

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager VM</td>
<td>VMware Identity Manager™ service</td>
<td>443</td>
<td>HTTPS</td>
<td>Optional if you are not using VMware Identity Manager™ with the pod. Used to create a trust relationship between the pod and the VMware Identity Manager™ service. Ensure that the pod can reach the VMware Identity Manager™ environment you are using, either on-premises or the cloud service, on port 443. If you are using the VMware Identity Manager™ cloud service, see also the list of VMware Identity Manager™ service IP addresses to which the VMware Identity Manager™ Connector and the pod must have access in the VMware Knowledge Base article 2149884.</td>
</tr>
</tbody>
</table>
| Transient Jump box VM | Manager VM                          | 22    | TCP      | As described above in Ports and Protocols Required by the 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. As a result, during the pod deployment process and pod update process, the requirement that communication between the jump box VM and the manager VM's port 22 must be met. The manager VM's port 22 must be allowed between the jump box VM as a source and the manager VM as a destination. Because these VMs are assigned IP addresses dynamically, the network rule 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.  

**Note** Ongoing pod operations do not require availability of port 22 on the pod's manager 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 your pod's manager 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. |

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 Unified Access Gateway configuration, Unified Access Gateway instances are automatically deployed in your Microsoft Azure environment, along with a Microsoft public load balancer to those instances. The diagram Figure 5-1. Illustration of the Horizon Cloud Pod Architecture Using the External Unified Access Gateway Configuration depicts the location of the load balancer and the Unified Access Gateway instances. When your pod has this configuration, end users on the Internet can connect to that public 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 the pod's public load balancer using the ports and protocols listed below. For the deployed pod, the public load balancer is located in the resource group named vmw-hcs-podID-uag, where podID 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 internal load balancer to those instances. The diagram Figure 5-2. Illustration of the
**Internal Unified Access Gateway Configuration** depicts the location of the internal load balancer and the Unified Access Gateway instances. When your pod has this configuration, end users in your corporate network can connect to the pod's internal 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 internal load balancer using the ports and protocols listed below. For the deployed pod, the internal 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 Administration Console, as described in [Upload SSL Certificates to a Horizon Cloud Pod for Direct Connections](#).

In general, uploading an SSL certificate to the pod directly is a recommended practice, because that ensures Horizon Clients that might make direct connections to the pod environment can have trusted connections, and is the supported configuration for using VMware Identity Manager™ with the pod. However, connections direct to the pod using HTML Access (Blast) appear as untrusted connections in the end user's browser. The end-user browsers display the typical untrusted certificate error when they make their connections direct to the pod. To have connections using HTML Access (Blast) avoid the displayed untrusted certificate error, you must have those connections use the load balancer and Unified Access Gateway instances from the pod's Unified Access Gateway configuration. If you do not want to expose your fully qualified domain name to the Internet, you can deploy an internal Unified Access Gateway configuration. This internal Unified Access Gateway configuration uses a Microsoft internal load balancer to which end users who are internal to your corporate network can point their connections.

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](https://docs.vmware.com/en/VMware-Horizon-Client/index.html).

**Table 5-7. 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>Pod's public load balancer to the 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="https://docs.vmware.com/en/VMware-Horizon-Client/index.html">Understanding What URL Content URL Content Redirection Is</a>.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Pod's public load balancer to the Unified Access Gateway instances</td>
<td>4172</td>
<td>TCP, UDP</td>
<td>PCoIP via PCoIP Secure Gateway on Unified Access Gateway</td>
</tr>
</tbody>
</table>
### Table 5-8. 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>Pod's internal load balancer to the 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>Pod's internal load balancer to the 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>Pod's internal load balancer to the 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>Horizon Client</td>
<td>Pod's internal load balancer to the Unified Access Gateway instances</td>
<td>443</td>
<td>UDP</td>
<td>Blast Extreme via the Unified Access Gateway for data traffic.</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 public load balancer to the 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>Horizon Client</td>
<td>Pod's public load balancer to the 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>Pod's public load balancer to the Unified Access Gateway instances</td>
<td>8443</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>Pod's public load balancer to the Unified Access Gateway instances</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 5-10. 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>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.

<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 desktop or farm server VMs</td>
<td>Manager VM</td>
<td>4002</td>
<td>TCP</td>
<td>Java Message Service (JMS) when using enhanced security (the default)</td>
</tr>
<tr>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>Manager VM</td>
<td>4001</td>
<td>TCP</td>
<td>Java Message Service (JMS), legacy</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.

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

As part of deploying the pod in Microsoft Azure, the automated deployment process creates a set of network security groups (NSGs) and associates them with the individual network interfaces (NICs) that are on each of the pod’s core virtual machines (VMs). These core VMs are the pod’s manager VM, and the VMs that are deployed when the pod is configured with Unified Access Gateway. Each NSG contains a set of security rules that define the allowed traffic to and from that NIC.

As described in the Microsoft Azure documentation’s Security groups topic, a network security group filters 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 sections below describe the NSG rules that the pod deployer defines in the NSGs it creates and associates to the VMs’ NICs.

- **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**

<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 desktop or farm server VMs</td>
<td>Manager VM</td>
<td>3099</td>
<td>TCP</td>
<td>Desktop message server</td>
</tr>
<tr>
<td>User Environment Manager agent (FlexEngine) in the desktop or farm server VMs</td>
<td>Those file shares you set up for use by the User Environment Manager agent the desktop or farm server VMs</td>
<td>445</td>
<td>TCP</td>
<td>User Environment Manager agent access to your SMB file shares, if you are using User Environment Manager capabilities.</td>
</tr>
</tbody>
</table>
General Facts About These NSGs

This list applies to all of 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. You can locate the pod's identifier by navigating to the pod's details from the Horizon Cloud Administration Console's Capacity page.

- 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`. 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 upgrade, the NSGs and rules will be retained. They will not be deleted.

- The Horizon Cloud rules start at priority 1000, and the priorities go up in increments of 100. The Horizon Cloud rules end with a rule at priority 3000.

- 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.

- 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.

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. Each NIC has an NSG defined on it.

- 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`.
Table 5-11. Deployer-Created NSG Rules on the Pod Manager 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>
</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>
</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>
</tr>
<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>
</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>
</tr>
</tbody>
</table>

Table 5-12. 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>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowHttpsInBound</td>
<td>80</td>
<td>TCP</td>
<td>VirtualNetwork</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>1100</td>
<td>AllowAgentJmsInBound</td>
<td>3443</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>1200</td>
<td>AllowAgentJmsInBound</td>
<td>4001</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>1210</td>
<td>AllowRouterJmsInBound</td>
<td>4101</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>1300</td>
<td>AllowAgentUdpInBound</td>
<td>5678</td>
<td>UDP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td></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>
</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>
</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. Each NIC has an NSG defined on it.

- The management NIC has an NSG named in the pattern `vmw-hcs-podUUID-uag-management-nsg`.
- The tenant NIC has an NSG named in the pattern `vmw-hcs-podUUID-uag-tenant-nsg`.
- The DMZ NIC has an NSG named in the pattern `vmw-hcs-podUUID-uag-dmz-nsg`.

In your Microsoft Azure environment, these NSGs reside in the pod’s resource group named in the pattern `vmw-hcs-podUUID-uag`. 
Table 5-13. 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>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowHttpsInBound</td>
<td>9443</td>
<td>TCP</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</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>
</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>
</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>
</tr>
</tbody>
</table>

Table 5-14. 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>
</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>
</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>
</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>
</tr>
<tr>
<td>Outbound</td>
<td>1000</td>
<td>AllowHttpsOutBound</td>
<td>443</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>Outbound</td>
<td>1100</td>
<td>AllowBlastOutBound</td>
<td>22443</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>Outbound</td>
<td>1200</td>
<td>AllowPcoipOutBound</td>
<td>4172</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>Outbound</td>
<td>1300</td>
<td>AllowUsbOutBound</td>
<td>32111</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>Outbound</td>
<td>1400</td>
<td>AllowMmroOutBound</td>
<td>9427</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>Outbound</td>
<td>1500</td>
<td>AllowAllOutBound</td>
<td>Any</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</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>
</tr>
</tbody>
</table>
Table 5-15. 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>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowHttpsInBound</td>
<td>80 443</td>
<td>TCP</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>Inbound</td>
<td>1100</td>
<td>AllowBlastInBound</td>
<td>443</td>
<td>Any</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>Inbound</td>
<td>1200</td>
<td>AllowPcoipInBound</td>
<td>4172</td>
<td>Any</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
</tr>
<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>
</tr>
<tr>
<td>Inbound</td>
<td>3000</td>
<td>DenyAllOutBound</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</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. Each NIC has an NSG defined on it.

- The management NIC has an NSG named in the pattern `vmw-hcs-podUUID-uag-management-nsg`.
- The tenant NIC has an NSG named in the pattern `vmw-hcs-podUUID-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 5-16. 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>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>1000</td>
<td>AllowHttpsInBound</td>
<td>9443</td>
<td>TCP</td>
<td>Management subnet</td>
<td>Any</td>
<td>Allow</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>
</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>
</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>
</tr>
</tbody>
</table>
Table 5-17. 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>
</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>
</tr>
<tr>
<td>Inbound</td>
<td>1100</td>
<td>AllowHttpsInBound</td>
<td>80 443</td>
<td>TCP</td>
<td>VirtualNetwork</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>Inbound</td>
<td>1200</td>
<td>AllowBlastInBound</td>
<td>443 8443</td>
<td>Any</td>
<td>VirtualNetwork</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>Inbound</td>
<td>1300</td>
<td>AllowPcoipInBound</td>
<td>4172</td>
<td>Any</td>
<td>VirtualNetwork</td>
<td>Any</td>
<td>Allow</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>
</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>
</tr>
<tr>
<td>Outbound</td>
<td>1000</td>
<td>AllowHttpsOutBound</td>
<td>443 8443</td>
<td>TCP</td>
<td>Tenant subnet</td>
<td>Any</td>
<td>Allow</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>
</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>
</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>
</tr>
<tr>
<td>Outbound</td>
<td>1400</td>
<td>AllowMmrOutBound</td>
<td>9427</td>
<td>TCP</td>
<td>Any</td>
<td>Tenant subnet</td>
<td>Allow</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>
</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>
</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.

In the table below, 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 Capacity Page. The *poolID* refers to the unique identifier for a farm or VDI desktop assignment.
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.

### Table 5-18. Per-Pod Resource Groups Created By Horizon Cloud

<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 VM and its 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 master VMs created either by running the Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace or Manually Build the Master Virtual Machine in Microsoft Azure, and those VMs' associated resources. After a master VM is published, it 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 Pods in Microsoft Azure.</td>
</tr>
</tbody>
</table>
Table 5-19. Cross-Pod Resource Groups Created By Horizon Cloud

<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. 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 a VMware Identity Manager™ Environment

By integrating your pod with an on-premises or cloud-hosted VMware Identity Manager™ environment, you give your VMware Identity Manager™ users the ability to access their entitled desktops and applications using Workspace ONE.

VMware Identity Manager™ 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. VMware Identity Manager™ is available both as an on-premises product and as a service hosted by VMware.

For an overview of this integration from the perspective of the VMware Identity Manager™ environment, see the Providing Access to Horizon Cloud 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 VMware Identity Manager™ environment, you sync the pod's assignment information to the VMware Identity Manager™ service. Then you can see the desktops and applications in the VMware Identity Manager™ administration console and your end users can access their desktops from Workspace ONE. You can set up a regular sync schedule to sync the assignment information from Horizon Cloud to your VMware Identity Manager™ environment.

Note  The screenshots in the VMware Identity Manager™ documentation might look different from the user interface elements you see in your specific VMware Identity Manager™ environment.
The following list is a high-level summary of the end-to-end steps to enable your end users to access their entitled desktops and applications using the Workspace ONE portal.

1. Obtain a VMware Identity Manager™ environment, either by deploying the on-premises version or by subscribing to the cloud-hosted version to have a VMware Identity Manager™ tenant in the cloud.

   **Note** If you specified creation of a cloud-based VMware Identity Manager™ tenant during the pod deployment process, the VMware Identity Manager™ 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 (after the following steps 2 through 5 are completed).

2. Deploy VMware Identity Manager™ according to the VMware Identity Manager™ guidelines for the deployment model you are using.

   If you are using the cloud-hosted VMware Identity Manager™, you must install a VMware Identity Manager™ connector appliance on premises in your Active Directory network. Read all of the connector-related prerequisites starting with this Prerequisites section.

   **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 from the Capacity Page.

3. Ensure that you meet the VMware Identity Manager™ prerequisites for integration, as documented in the VMware Identity Manager™ product information appropriate for your situation. See the prerequisites information starting with this Prerequisites section.

   **Important** In addition to the prerequisites listed below in this documentation topic, you must also ensure that your configured VMware Identity Manager™ environment meets the prerequisites for integration with Horizon Cloud resources, as described in the VMware Identity Manager™ documentation.

<table>
<thead>
<tr>
<th>VMware Identity Manager™ environment</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud-hosted</td>
<td>Prerequisites for Integration</td>
</tr>
<tr>
<td>On-premises</td>
<td>Prerequisites for Integration</td>
</tr>
<tr>
<td></td>
<td>Use the blue rectangle menu in the upper right corner of the linked topic above to view the information for your version.</td>
</tr>
</tbody>
</table>
4 Enable the desktops from your Horizon Cloud environment to the VMware Identity Manager™ environment, as documented in the VMware Identity Manager™ product information appropriate for your situation:

<table>
<thead>
<tr>
<th>VMware Identity Manager™ environment</th>
<th>Link to Desktop Enablement Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud-hosted</td>
<td>Configure Horizon Cloud Tenant in VMware Identity Manager</td>
</tr>
<tr>
<td>On-premises</td>
<td>Use the blue rectangle menu in the upper right corner of the linked topic above to view the information for your version.</td>
</tr>
</tbody>
</table>

The final step of that Configure Horizon Cloud Tenant in VMware Identity Manager™ topic describes how to sync the entitled desktops and applications from your Horizon Cloud environment. However, do not perform that sync until after you complete the next step of configuring Horizon Cloud for VMware Identity Manager™ access.

5 Configure Horizon Cloud for VMware Identity Manager™ access. See Configure a Pod in Microsoft Azure for VMware Identity Manager™.

6 In your VMware Identity Manager™ environment, sync the entitled desktops and applications to VMware Identity Manager™. In the VMware Identity Manager™ administration console, navigate to the Virtual Apps Configuration page for the collection you created in Step 5 and click Sync.

7 Verify end-user access to desktops and applications by logging in to Workspace ONE as an end user and launching a desktop and application from the catalog. See Confirm End-User Access to Desktop Assignments in VMware Identity Manager™.

Prerequisites

To complete the integration process through the step of verifying end-user access to the pod-provided desktops or RDS-based remote applications using Workspace ONE, ensure that you have the following items.

- A fully configured Horizon Cloud pod that has trusted certificates uploaded to the pod's manager VM itself. You need to have a SSL certificate uploaded to the pod itself as described in Upload SSL Certificates to a Horizon Cloud Pod for Direct Connections.
- VDI desktop assignments, session desktop assignments, or remote application assignments are configured.
- Access to your organization's configured VMware Identity Manager™ environment, either an on-premises or a cloud-hosted environment. Your VMware Identity Manager™ environment must be configured with trusted certificates.

If you are deploying VMware Identity Manager™ on premises, follow the deployment information available from the VMware Identity Manager™ documentation page. For the specific versions of the on-premises VMware Identity Manager™ product that are supported for use with this release, see the VMware Product Interoperability Matrixes at https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
If you are using the cloud-hosted VMware Identity Manager™ and your VMware Identity Manager™ tenant is set up, a VMware Identity Manager™ 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 VMware Identity Manager™ tenant. You must install the VMware Identity Manager™ connector appliance in your Active Directory network. Follow the steps as documented in the VMware Identity Manager™ 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 Identity Manager™ connector appliance, a best practice is to upgrade the connector before upgrading the pod to the latest pod software level.

- Verify your configured VMware Identity Manager™ environment meets all of the prerequisites for integration with Horizon Cloud resources, as described in the VMware Identity Manager™ documentation.

<table>
<thead>
<tr>
<th>VMware Identity Manager™ environment</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud-hosted</td>
<td>Prerequisites for Integration</td>
</tr>
<tr>
<td>On-premises</td>
<td>Prerequisites for Integration</td>
</tr>
<tr>
<td></td>
<td>Use the blue rectangle menu in the upper right corner of the linked topic above to view the information for your version.</td>
</tr>
</tbody>
</table>

**Procedure**

1. **Configure a Pod in Microsoft Azure for VMware Identity Manager™**

   To integrate a pod in Microsoft Azure with your VMware Identity Manager™ environment, you must configure the pod with the appropriate VMware Identity Manager™ information. You use the Administration Console to configure this information.

2. **Confirm End-User Access to Desktop Assignments in VMware Identity Manager™**

   After you integrate your Horizon Cloud environment with your VMware Identity Manager™ environment, you can confirm that end users have remote access to their virtual desktops.

**What to do next**

After you have verified the integration is working, you can optionally enforce end users to access their desktops and applications using VMware Identity Manager™. See Enforce End-User Access Through VMware Identity Manager™.
Configure a Pod in Microsoft Azure for VMware Identity Manager™

To integrate a pod in Microsoft Azure with your VMware Identity Manager™ environment, you must configure the pod with the appropriate VMware Identity Manager™ information. You use the Administration Console to configure this information.

Prerequisites

Verify that your VMware Identity Manager™ environment is configured to point to the FQDN that you mapped to the pod's tenant appliance IP address in your DNS server.

Verify that an SSL certificate based on that FQDN is uploaded to the pod itself, as described in Upload SSL Certificates to a Horizon Cloud Pod for Direct Connections.

Verify that you have the following information:

- The SAML identity provider (IdP) metadata URL from your VMware Identity Manager™ environment. You obtain the environment's SAML IdP metadata URL using the VMware Identity Manager™ 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://VMwareIdentityManagerFQDN/SAAS/API/1.0/GET/metadata/idp.xml, where VMwareIdentityManagerFQDN is the fully qualified domain name (FQDN) of your VMware Identity Manager™ environment. For details, see the VMware Identity Manager™ product information appropriate for your situation:

<table>
<thead>
<tr>
<th>VMware Identity Manager™ 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>
<tr>
<td>On-premises</td>
<td>Configure SAML Authentication in the Horizon Cloud Tenant</td>
</tr>
<tr>
<td></td>
<td>Use the blue rectangle menu in the upper right corner of the linked topic above to view the information for your version.</td>
</tr>
</tbody>
</table>

- The FQDN that you tell your end users to make their connections to, for connecting to Horizon Cloud.

Procedure

1. Log in to the Administration Console.


3. Configure the following options.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager URL</td>
<td>Type your VMware Identity Manager™ environment's SAML IdP metadata URL, typically of the form <a href="https://VMwareIdentityManagerFQDN/SAAS/API/1.0/GET/metadata/idp.xml">https://VMwareIdentityManagerFQDN/SAAS/API/1.0/GET/metadata/idp.xml</a>, where VMwareIdentityManagerFQDN is the FQDN of your VMware Identity Manager™ 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 VMware Identity Manager™ configuration applies.</td>
</tr>
</tbody>
</table>
Setting | Description
---|---
Data Center | The drop-down displays a numeric related to the Horizon Cloud pod software version. Keep the default.
Tenant Address | Type the FQDN that you tell your end users to make their connections to, for connecting to Horizon Cloud.
Workspace ONE Redirection | When you also have the configuration to force end-user access to go through VMware Identity Manager, you can set this toggle to **YES** to have the end users' clients automatically redirect to their Workspace ONE environment. You can read about setting the options to force end-user access to go through VMware Identity Manager in [Configure the Option to Force End-User Access to Use VMware Identity Manager](#). 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 access through VMware Identity Manager, the client is automatically redirected to the Workspace ONE environment that is configured in VMware Identity Manager. 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 End-User Access Through VMware Identity Manager™](#). **Note** You can enable Workspace ONE 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.

4 Click **Save**.

A status of green indicates that the configuration is successful.

**What to do next**

In your VMware Identity Manager™ environment, sync the entitled desktops and applications to VMware Identity Manager™. In the VMware Identity Manager™ 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 VMware Identity Manager™.
- 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 **Capacity Page**.

**Confirm End-User Access to Desktop Assignments in VMware Identity Manager™**

After you integrate your Horizon Cloud environment with your VMware Identity Manager™ 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 VMware Identity Manager™.

Ensure that the entitled desktops are synced from the integrated Horizon Cloud pod to your VMware Identity Manager™ environment. In the VMware Identity Manager™ administration console, navigate to the Virtual Apps Configuration page and sync the Horizon Cloud collection.

Procedure

1. Use your organization's VMware Identity Manager™ URL to log in to Workspace ONE.
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 VMware Identity Manager™ 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 VMware Identity Manager™. After that authentication, the user is 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.
   c. Downloading the Horizon Cloud pairing bundle from the 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, Ports, Protocols Requirements for a Horizon Cloud Pod in Microsoft Azure.

2. Adding the Enrollment Server information to the 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 VMware Identity Manager™ environment configured. Complete the steps described in Integrate a Horizon Cloud Pod in Microsoft Azure with a VMware Identity Manager™ Environment.

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 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 Administration Console's Active Directory page.

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:
   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.

- Click **Start** and type `dsa.msc`. The Active Directory Users and Computers window displays.
- In the tree, right-click the **Users** folder for the domain controller and select **New > Group**. The New Object - Group window displays.
- In the **Group Name** field, enter a name for the new group. For example, TrueSSO Enrollment Servers.
- 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>

- Click **OK**. The new group appears in the tree in the Active Directory Users and Computers window.

- Right-click the group and select **Properties**.
- On the Member Of tab, add every computer on which you will be installing an Enrollment Server, and then click **OK**.
- Restart every computer on which you will be installing an Enrollment Server.

2 Configure the certificate template.

- Select **Control Panel > Administrative Tools > Certificate Authority**.
- In the tree, expand the local CA name.
- Right-click on the Certificate Templates folder and select **Manage**. The Certificate Templates Console displays.
- 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 Show resulting changes 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>■ 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 For automatic renewal of smart card certificates . . . check box</td>
</tr>
<tr>
<td></td>
<td>■ Select the Prompt the user during enrollment 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 Requests can use any provider available . . . radio button</td>
</tr>
<tr>
<td></td>
<td>■ Request hash - SHA256</td>
</tr>
<tr>
<td>Subject Name</td>
<td>■ Select the Build from this Active Directory Information radio button.</td>
</tr>
<tr>
<td></td>
<td>■ Subject name format - Fully distinguished name</td>
</tr>
<tr>
<td></td>
<td>■ Select the User principal name (UPN) check box.</td>
</tr>
<tr>
<td>Server</td>
<td>■ Select the Do not store certificates and requests in the CA database check box</td>
</tr>
<tr>
<td>Issuance Requirements</td>
<td>■ Require the following for enrollment - Select This number of authorized signatures 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 Allow 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 Administration Console’s Active Directory page.

The pairing bundle contains a certificate file for each Horizon Cloud pod in your 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:

```plaintext
podID_truesso.crt
```

where `podID` is the pod's ID that is displayed in the pod's summary page.

### Procedure

1 In the Administration 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 Enrollment Server.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 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 VM and Enrollment Server network traffic, as described in DNS, Ports, Protocols 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 Administration 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.

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.

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

If a farm's RDS server 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 RDS server 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 7 RDS ADMX files are added to your Active Directory. See Add the Remote Desktop Services ADMX File to Active Directory.

- Familiarize yourself with the group policy settings. 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 VDI desktops, RDS-based desktops, and remote applications served 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 5-20. Supported Configurations for RDSH Server 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 server 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 server VM</td>
<td>NVIDIA GRID GPU For driver details, see:</td>
<td>Graphics intensive or requiring advanced graphics features</td>
<td>Single 4K display</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 5-21. 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>

**Note**: Microsoft NV-series VMs allow use of up to four 4K displays for VDI desktops. Please see the NVIDIA GRID documentation for the specific GPU you are using to get supported resolutions and workload recommendations.

### 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 Identity Manager™ 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 and to see the respective documentation, see the Horizon Client documentation page at 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'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 server VM, set the Enable Client Retry option to Yes in the Administration Console's General Settings page. For details about that option, see Edit General Settings. 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 RDSH server VM is powered off, due to any power-management schedules configured in the VDI desktop assignment or RDSH 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 the Enable Client Retry option set to Yes in the Administration Console's General Settings, the client displays a message describing the connection will be made when the desktop is ready and the estimated time it might take.

   The following screenshot is an illustration of the message that displays in Horizon Client for Windows version 4.8 when the client retry mechanism is in place and the system is powering on the underlying VM.
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

If your environment is configured for HTML Access, users can access their VDI desktops, RDS desktops, and RDS-based remote applications by pointing their browser to the fully qualified domain name (FQDN) that your organization has associated with the pod for end-user connections.

These steps describe using a browser to launch a desktop provided by the pod.

**Note** If integration with a VMware Identity Manager™ environment is configured, end users might have to access their desktops and remote applications using that environment. See Enforce End-User Access Through VMware Identity Manager™.

**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, such as desktops.mycorp.example.com.

  For example, when your 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's Load Balancer Information to Map in your DNS Server.

- 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 server VM, set the **Enable Client Retry** option to **Yes** in the Administration Console's General Settings page. For details about that option, see Edit General Settings. 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, RDS 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.

   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 End-User Access Through VMware Identity Manager™

When you have integrated your Horizon Cloud environment with your VMware Identity Manager™ environment, you can specify that end users must use Workspace ONE to access their desktops. Requiring end users to access their desktops through Workspace ONE 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 VMware Identity Manager™ 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 your pod.

- From the Horizon Client application, by including that FQDN as a new server location in the client application.
From Workspace ONE, if your environments are integrated.

You can optionally configure your Horizon Cloud environment to require your end users use Workspace ONE 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 when this using VMware Identity Manager™ is enforced.

The feature to force end-user access to VMware Identity Manager works with the Workspace ONE redirection feature in the following ways.

<table>
<thead>
<tr>
<th>Force end-user access through VMware Identity Manager setting</th>
<th>Workspace ONE 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 their Workspace ONE environment.</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. 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 VMware Identity Manager 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 VMware Identity Manager™ environments are integrated.

**Procedure**

1. In the Administration 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>Force Remote Users to viDM</td>
<td>When set to Yes, users that are trying to access their desktops from locations outside of your corporate network must log in to Workspace ONE and access desktops from there.</td>
</tr>
<tr>
<td>Force Internal Users to viDM</td>
<td>When set to Yes, users that are trying to access their desktops from locations within your corporate network must log in to Workspace ONE and access desktops from there.</td>
</tr>
</tbody>
</table>

3. Click **Save** to confirm the configuration to the system.
(Optional) Set Workspace ONE redirection on the identity management configuration.

**Note** You can have Workspace ONE 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.

- On the Identity Management page, select the check box for the VMware Identity Manager™ configuration for which you want to set redirection and click **Edit** to open its configuration.
- Set the **Workspace ONE Redirection** toggle to **YES**.
- 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 from Workspace ONE.
About Menu Selections in the Administration Console

The menu icons provide a quick way to navigate to monitor activity and perform various functions in your Horizon Cloud environment. The icons are located along the left side of the Administration Console.

Table 6-1. Administrator Functions

<table>
<thead>
<tr>
<th>Icon</th>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="default-landing-page.png" alt="Icon" /></td>
<td>Default landing page</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 Dashboard Page.</td>
</tr>
</tbody>
</table>
| ![Icon](monitor.png) | 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. |
| ![Icon](assign.png) | Assign | Opens the Assignments screen from which you can work with assignments that entitle end-user access to those assignable items that are in your environment's inventory. |
About the Monitor Icon

Use the Monitor icon 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 the Monitor icon 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>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.</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.

- Use the Show filter to display events for only a certain period of time.
- Use the Pod filter to display events for a specific pod.
- View the total number of events.
- Use the Filter box to filter events.
- Refresh the list.
- Cancel tasks that are able to be cancelled.
- Download the displayed information as report file with the Export feature.

**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 Administration Console. After you make your selections for the downloaded report, the system starts preparing the report. A message appears basically saying the report is being compiled and it can take some time. During this time, you cannot dismiss the message to perform other tasks in the Administration Console. You must wait until the preparation is done and the next message appears with the message Report Generated Successfully and a Download button. Depending on the number of records, the preparation time can take several minutes. A report with 50,000 records takes approximately 10 minutes.

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.

<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>% Completion</td>
<td>Current percentage of event completed.</td>
</tr>
</tbody>
</table>
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 you select all of the listed tasks by selecting the topmost check box, only those tasks that are currently cancellable are selected.

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>Not 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></td>
</tr>
<tr>
<td>Assignment Expansion</td>
<td>Supported</td>
<td>Not 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></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></td>
</tr>
</tbody>
</table>

### User Events

The **Users** tab displays descriptions and times logged for end-user events.

### Audit Logs

The Audit Logs tab displays descriptions, status, and times logged for events that have occurred from administrator-initiated actions on your pods.
Reports Page

Use the Reports page to access various reports related to end users’ desktop and application sessions.

Important The Desktop Health, Utilization, Session History, Concurrency, and Top Applications 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, Session History, Concurrency, and Top Applications. 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 the following categories. You can also manually refresh this page, filter your search, and export data to a Microsoft Excel worksheet.

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 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 would display historical and aggregated viewing of that data, such as the Session History report, are not available.

The Enable User Session Information toggle for enabling or disabling monitoring user session information is on the General Settings page (Settings > General Settings).

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 Administration Console.
<table>
<thead>
<tr>
<th>Report Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Mapping</td>
<td>View details and sort by various categories, such as User name, Domain, Desktop Name, Desktop Model, Farm, and Mapping Type (User or Group). <strong>Note</strong> This report is populated only for users that have at least one direct assignment to a desktop. In the Administration 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.</td>
</tr>
<tr>
<td>Desktop Mapping</td>
<td>View details and sort by various categories, such as Desktop Name, Model, Assignment Name, Type, Farm, Active User, Mapped Users, and Mapped User Groups. <strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Desktop Health</td>
<td>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 usage %, memory usage %, disk IOPS, and active/disconnected sessions. For VDI desktops, the report includes CPU usage %, memory usage %, 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 usage %, memory usage %, and disk latency. Threshold values are 90% for CPU, 80% for memory usage, 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. <strong>Note</strong> This report's data is updated every minute by the data from the backend reporting system.</td>
</tr>
<tr>
<td>Report Type</td>
<td>Details</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Utilization</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- For Horizon 7 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.</td>
</tr>
<tr>
<td></td>
<td>- For pods in Microsoft Azure, information provided includes utilization of deployed capacity as well as session concurrency. Ancillary details covering client usage, protocol usage, 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When Enable User Session Information is turned off for your environment, the Unique User Summary feature of this report is not provided. The Enable User Session Information is set in the General Settings page.</td>
</tr>
<tr>
<td></td>
<td>The backend reporting system sends the data for this report at a specific UTC time:</td>
</tr>
<tr>
<td></td>
<td>- 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 complete.</td>
</tr>
<tr>
<td></td>
<td>- For the other time periods, the data is updated daily. The update starts at 2am UTC and takes about 15 minutes to complete.</td>
</tr>
<tr>
<td>Azure Concurrency</td>
<td>View per-assignment data for capacity, number of concurrent users, peak concurrency, and applications in use. You can filter this information by time period.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This report is available for pods in Microsoft Azure only.</td>
</tr>
<tr>
<td>URL Configurations</td>
<td>View information for currently configured URL redirects. For more information, see Create a URL Redirection Customization and Assign it to Users.</td>
</tr>
<tr>
<td>Agent Versions</td>
<td>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 versions need to 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.</td>
</tr>
<tr>
<td>Desktop Sessions</td>
<td>View session information for user sessions including desktop name, log-in time, session duration, log in duration, client IP, and client type across all your pools over a pre-defined time period.</td>
</tr>
<tr>
<td></td>
<td>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 complete. 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This report is not provided when Enable User Session Information is turned off for your environment, as set in the General Settings page.</td>
</tr>
</tbody>
</table>
Report Type | Details
---|---
VDI Application Sessions | View a list of applications that end users have used in VDI desktops and each application's total usage duration. Can be filtered by assignment and 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 complete.
- For the other time periods, the data is updated daily. The update starts at 2:30am UTC and takes about 15 minutes to complete.

User Usage Report | View a record of desktop and applications usage by the user over the pod for a predefined time period. This report helps you identify the number of sessions that the user has launched and their total active usage time.

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 Administration Console by clicking the bell icon located in the upper right corner of any page. Open the Notifications page to view all notifications, which includes 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 6-2. 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 status of the deployed pod in Microsoft Azure. These notifications include those 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>Notifications related to the cloud plane API requests to the pod resources in Microsoft Azure, such as API slow downs or time outs.</td>
</tr>
<tr>
<td>Primary bind account locked</td>
<td>Account-lockout 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>
</tbody>
</table>

About the Assignments Icon

The Horizon Cloud Administration Console navigation bar's Assignments icon provides access to use assignment-related workflows in your Horizon Cloud environment.
When you click **Assignments** in the navigation bar, the Administration Console displays differently depending on the pod types you have in your environment.

### When You Have Mixed Pod Types

When you have both Horizon 7 pods and pods in Microsoft Azure, clicking **Assignments** displays selection choices:

- **Microsoft Azure** - Click this choice to display the Assignments page that is specific for assignment-related workflows for pods in Microsoft Azure. See the *When All of Your Pods are In Microsoft Azure* section.

- **On-Prem & VMware Cloud** - Click this choice to display the Assignments page that is specific for assignment-related workflows for Horizon 7 pods. See the *When All of Your Pods are Horizon 7 Pods* section.

### When All of Your Pods are Horizon 7 Pods

When all of your pods are Horizon 7 pods, clicking **Assignments** displays the Assignments page, where you can initiate actions to create new desktop assignments and work with your existing assignments. For each listed assignment, you can click its name to 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 7 pods, see Chapter 4 *Workflows for Cloud-Connected VMware Horizon 7 Pods* and its subtopics.

### When All of Your Pods are In Microsoft Azure

When you have zero Horizon 7 pods, clicking **Assignments** displays the Assignments page, where you can initiate actions to create new assignments and work with your existing assignments. For each listed assignment, you can click its name to see more information about that assignment, such as which users it is assigned to and other details.

For detailed information about managing assignments for your pod in Microsoft Azure, see *Managing Assignments*.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Create assignments for items in your inventory, such as virtual desktops and applications.</td>
</tr>
<tr>
<td>Edit</td>
<td>Use this button to modify characteristics of the selected assignment.</td>
</tr>
<tr>
<td>Duplicate</td>
<td>Use this button to duplicate the selected desktop assignment and create a new one with the same specifications but a new name.</td>
</tr>
<tr>
<td>Take Offline</td>
<td>Use this button to take the selected assignment offline, typically for maintenance purposes.</td>
</tr>
<tr>
<td>Update Agent</td>
<td>Use this button to update the agent-related software in a dedicated VDI desktop assignment.</td>
</tr>
<tr>
<td>URL Redirection</td>
<td>Use this button to configure a set of URL handling rules and assign to users.</td>
</tr>
<tr>
<td>Delete</td>
<td>Use this button to delete the selected assignment.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recover</td>
<td>Even though you see the Recover action in the page, this action is not used for assignments in a Microsoft Azure environment.</td>
</tr>
<tr>
<td>Bring Online</td>
<td>Use this button to bring an offline assignment back online.</td>
</tr>
</tbody>
</table>

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.

**About the Inventory Icon**

Use the Inventory icon to navigate to pages where you can work 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 the Inventory icon to navigate to these pages.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>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.</td>
</tr>
<tr>
<td>Farms</td>
<td>Opens the Farms page. See Farms in Horizon Cloud.</td>
</tr>
<tr>
<td></td>
<td>At a page level, you can:</td>
</tr>
<tr>
<td></td>
<td>• View the RDSH farms available in your environment.</td>
</tr>
<tr>
<td></td>
<td>• Create an RDSH farm.</td>
</tr>
<tr>
<td></td>
<td>• Edit an existing farm</td>
</tr>
<tr>
<td></td>
<td>• Move a farm online or offline</td>
</tr>
<tr>
<td></td>
<td>• Delete a farm</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Edit various settings, such as the farm's name and its size.</td>
</tr>
<tr>
<td></td>
<td>• Power off and delete the servers in the farm.</td>
</tr>
<tr>
<td></td>
<td>• Work with sessions currently connected to the farm's servers.</td>
</tr>
<tr>
<td></td>
<td>• Examine activity that has taken place in the farm.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Images  | Opens the Images page. See Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure and Managing Assignable Images. In this page, you can:  
- View the assignable desktop images available in the system.  
- Create an assignable desktop image from a master VM that has been prepared with the required agents.  
- Download the DaaS bootstrap file. Use the Download Bootstrap button to download an encrypted bootstrap file for you 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.  
  When you select the check box for a specific listed assignable image, or click its name, you can perform the following actions on it:  
- Duplicate it.  
- Delete it.  
- Update its agent-related software, if a later version is available. |
| Imported VMs  | Opens the Imported VMs page. The virtual machines (VMs) displayed on this page include:  
- The master VMs that you created using the Import action button.  
- VMs that the system imported from the pods' podID-base-vms resource groups.  
You can move VMs from this page to the Utility VMs page, according to your organization's needs.  
See Imported VMs Page for details. |

**Imported VMs Page**

The Imported VMs page in the Administration Console 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 Version 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.
### Action | Description
---|---
Renamed | Even though you see the Rename action in the page, this action is not used for VMs from a Microsoft Azure environment.

#### VM power and guest operating system actions
- **Delete** | Delete the selected VM.
- **Migrate to Utility VMs** | Move the VM to the Utility VMs page. See Utility VMs Page
- **Convert to Image** | Convert the selected VM to an image that Horizon Cloud can use for farms or VDI desktop assignments. See Convert a Configured Master Virtual Machine to an Assignable Image.

**Note** Make sure the VM has all of the applications and drivers you want installed on it before converting it.

### About the Settings Icon

You use the Settings icon to navigate to pages for working with various aspects of your Horizon Cloud environment, such as utility virtual machines (VMs), identity management, your deployed pods, and related settings and configurations.

Click the Settings icon to access these pages in the Administration Console.

#### User Interface Page | Description
---|---
**General Settings** | Displays settings for networks, domains, connection timeouts, and so on, including the toggle to enable or disable monitoring user session information. You can edit settings from this page. See Edit General Settings for details.

**Active Directory** | 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 Complete Configuring True SSO for your Horizon Cloud Environment.

**Roles & Permissions** | Edit roles and permissions. See Assign Horizon Cloud Administrative Roles to Active Directory Groups.

**Capacity** | View details about your deployed pods, such as each pod's utilization and capacity usage, as well as 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 Capacity Page.

**Utility VMs** | Displays virtual machines (VMs) that are used for infrastructure services like DHCP. Usually a VM is listed on this page when you have moved it from the Imported VMs page. See Utility VMs Page.

**Identity Management** | Configure integration of your Horizon Cloud environment with your VMware Identity Manager™ environment.

**File Share** | This page is not currently supported to use for pods deployed in Microsoft Azure. As a result, this option does not appear.

**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** | Opens the Getting Started wizard. See About the Horizon Cloud Getting Started Wizard for details.
Edit General Settings

Use the General Settings page to modify settings that apply to your overall Horizon Cloud environment.

In this release, when your cloud-connected pods are all Horizon 7 pods, only the Default Domain and My VMware Accounts sections are displayed and available for editing. When you have pods deployed in Microsoft Azure, all the sections described here are displayed in the General Settings page.

**Note** When changing any of the following settings, it can take up to 5 minutes for the update to take effect.

- The settings in the Session Timeout section, listed in Horizon Client Timeout Settings.
- The Cleanup credentials when tab is closed setting in the HTML Access section.
- The Enable Client Retry setting in the Pool/Farm Options section.
- The settings in the Domain Security Settings section, listed in Domain Security Settings on General Settings Page.

**Procedure**

1. Select **Settings > General Settings**.
2. Click **Edit**.
3. Change these settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 logging in to the Administration 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, 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. |
| **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 Administration Console. When that time has elapsed, the administrator’s authenticated session ends and the administrator must log back in.  
- The other listed 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 must reauthenticate to Horizon Cloud. For details, see Horizon Client Timeout Settings. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Portal Configuration</td>
<td>The user portal feature is deprecated in this release.</td>
</tr>
<tr>
<td>My VMware Accounts</td>
<td>To give users the ability to log into Horizon Cloud, you can 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 Horizon Cloud Administrative Roles to Active Directory Groups.</td>
</tr>
</tbody>
</table>
| HTML Access            | The **Cleanup 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 reenter their credentials when they reconnect.  
  - A value of **Yes**, the option that emphasizes security, prompts end users to reenter their credentials.  
  - A value of **No**, the option that emphasizes ease of use, does not prompt end users to reenter their credentials. |
| 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. |
| Pool/Farm Options      | This 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.  
  a. Horizon Cloud starts powering on the underlying virtual machine in the cloud that will serve the end user's client request.  
  b. Horizon Cloud notifies Horizon Client to retry the connection when the agent in the virtual machine is up and running.  
  c. The client prompts the user with a message that describes the wait time estimated before the client retries the connection. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain Security Settings</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Important**

- These settings are applied to all the pods in your environment, 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 upgraded to this Horizon Cloud release’s pod manifest version. To get access to these controls, upgrade all your pods in Microsoft Azure to this release.
- Until all your pods are upgraded to this Horizon Cloud release level, 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 this release level, 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 Capacity Page. For this release’s pod manifest version, see the Release Notes for the current release.
### Option | Description
--- | ---
**Monitoring** | 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 [Dashboard Page](#) and [Reports Page](#).  

#### Contact Info
- Administrator contact information

4 Click **Save**.

---

**Horizon Client Timeout Settings**

Most of the session timeout settings in the General Settings page 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**  When changing any of these settings, it can take up to 5 minutes for the update to take effect.
## Timeout Description

<table>
<thead>
<tr>
<th>Timeout</th>
<th>Description</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 Horizon Cloud. These heartbeats report to the Horizon Cloud 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>
<tr>
<td>Client Idle User</td>
<td>Maximum time that a user can be idle in a connection between the end-point device and Horizon Cloud. When this maximum is reached, the user's authentication expires and all active Horizon Client, Horizon HTML Access, and Workspace ONE connections are closed. The user must reauthenticate to reopen a connection from their end-point device to Horizon Cloud.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Set the Client Idle User timeout to be at least double the Client Heartbeat Interval setting to avoid unexpected disconnects from desktops.</td>
</tr>
<tr>
<td>Client Broker Session</td>
<td>Maximum time that a Horizon Client, Horizon HTML Access, or Workspace ONE connection can be connected to Horizon Cloud 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. If the user performs an action that causes communication to the Horizon Cloud 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).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td>User Portal Timeout</td>
<td>This setting is deprecated and has no effect.</td>
</tr>
</tbody>
</table>

## 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 Horizon Cloud 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 Horizon Cloud 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
- This Release's Default Behavior Compared with Past Releases
- Relationship to Your Pods' Manifest Levels
- Single Active Directory Domain Scenarios and User Login Requirements
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 6-3. 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><strong>Yes</strong> - The system sends only the literal string value <em>DefaultDomain</em>.</td>
</tr>
<tr>
<td></td>
<td><strong>No</strong> - The system sends the list of registered Active Directory domain names to the client.</td>
</tr>
<tr>
<td><strong>Hide Domain Field</strong></td>
<td>This option controls the visibility in the client login screen of whatever domain-related information is sent to the client, based on the <strong>Show Default Domain Only</strong> setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Yes</strong> - Nothing about domains is displayed in the client login screen, regardless of what <strong>Show Default Domain Only</strong> is set to. Neither the literal string value <em>DefaultDomain</em> nor the domain names are displayed in the client login screen.</td>
</tr>
<tr>
<td></td>
<td><strong>No</strong> - The client login screen displays one of the following items, depending on the <strong>Show Default Domain Only</strong> setting.</td>
</tr>
<tr>
<td></td>
<td>**The literal text <em>DefaultDomain</em>, when <strong>Show Default Domain Only</strong> is <strong>Yes</strong>. This combination is optimized for user experience in Horizon Clients older than version 5.0, while also providing improved security.</td>
</tr>
<tr>
<td></td>
<td>**The list of domain names in a drop-down menu, when <strong>Show Default Domain Only</strong> is <strong>No</strong>.</td>
</tr>
</tbody>
</table>
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>
</table>
| The system sent the names of the registered Active Directory domains to the clients. | The system sends only a literal string value (*DefaultDomain*) to the clients and not the names of the registered Active Directory domains. | Show Default Domain Only  
Default setting: Yes |

**Note** Sending the literal string provides support for older Horizon clients which are implemented to expect a string list of domain names.

<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>
</table>
| 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. | The clients display that literal string *DefaultDomain*. | Hide Domain Field  
Default setting: No |

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 upgraded 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-upgraded 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 upgraded, the settings are available in the Administration Console. The post-upgrade defaults are set to the pre-upgrade behavior (**Show Default Domain Only** is **No** and **Hide Domain Field** is **No**). The post-upgrade default settings are different than the new-customer defaults. These settings are applied so that the pre-upgrade legacy behavior continues for your end users after the upgrade, 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 6-4. 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>
</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. The following screenshot is an example for how the resulting login screen looks like for the Windows client. | 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.  
- username  
- domain\username  
Using the command-line client launch and specifying the domain in the command works. |
|                                                        | No                | The client’s login screen has the standard user name and password fields. The domain field displays *DefaultDomain*. No domain name is sent. The following screenshot is an example for how the resulting login screen looks like for the Windows client. | 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.  
- username  
- domain\username  
Using the command-line client launch and specifying the domain in the command works. |
### Horizon Client 5.0 Login Screen Details

<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 name 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><strong>Note</strong> 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.</td>
<td>■ <em>domain\username</em></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 one available domain name. The domain name is sent.</td>
<td>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.</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>

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 upgrade the client to the 5.0 version. However, when you have more than one Active Directory domain, passing *DefaultDomain* does not work.
**Table 6-5. 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 6-6. 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>
</table>
| Yes                                                      | Yes               | 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. | 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. |
|                                                            | 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.  

- domain\username

Using the command-line client launch and specifying the domain in the command works. |
### Horizon Client 5.0 Login Screen Details

<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 <strong>User name</strong> text box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> 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 <strong>User name</strong> text box and select their domain from the list visible in the client.</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>

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 upgrade the client to the 5.0 version.
Table 6-7. 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>
<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.</td>
<td>An end user must include the domain name in the <strong>User name</strong> text box.</td>
</tr>
<tr>
<td></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.</td>
<td>This combination is unsupported for environments with multiple Active Directory domains.</td>
</tr>
<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 name to the client.</td>
<td>An end user must include the domain name in the <strong>User name</strong> text box.</td>
</tr>
<tr>
<td></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 one available domain name. The domain name is sent.</td>
<td>The end user can specify their user name in the <strong>User name</strong> text box and select their domain from the list visible in the client.</td>
</tr>
</tbody>
</table>

**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** This release does not support registering file shares for use with pods deployed in Microsoft Azure. As a result, no information is provide on this page for such pods.

### Utility VMs Page

The Utility VMs page in the Administration Console provides actions for virtual machines (VMs) that you might have added to your environment for infrastructure-related capabilities, such as DHCP, Domain Controller functions, and so on.

You can perform the following actions on the listed VMs by selecting the check box next to the VM and clicking the respective action.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename</td>
<td>Even though you see the <em>Rename</em> action in the page, this action is not used for VMs imported from a Microsoft Azure environment.</td>
</tr>
<tr>
<td>VM power and guest</td>
<td>Depending on the current state of the VM, these standard VM power operations are available: power on, power off, suspend, resume, reset. Operations on the guest operating system are restart and shutdown.</td>
</tr>
<tr>
<td>operating system actions</td>
<td></td>
</tr>
<tr>
<td>Migrate to Imported VMs</td>
<td>Move the VM to the Imported VMs. <a href="#">See Imported VMs Page</a>.</td>
</tr>
</tbody>
</table>
Identity Management Page

On the Identity Management page, you can add, edit, and configure those identity management providers you want to use with your Horizon Cloud environment.

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.
- Identity Manager URL - URL of the provider.
- Timeout SSO Token - Timeout value in minutes.
- Workspace ONE Redirection - Indicates whether automatic redirection to Workspace ONE 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 VMware Identity Manager. See Configure the Option to Force End-User Access to Use VMware Identity Manager.
- 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 Capacity Page.
- Tenant Address - 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 a VMware Identity Manager™ Environment and follow the steps in Configure a Pod in Microsoft Azure for VMware Identity Manager™.

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 Token</td>
<td>Timeout value in minutes.</td>
</tr>
<tr>
<td>Tenant Address</td>
<td>Address of the tenant appliance. 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>Workspace ONE Redirection</td>
<td>When editing the configuration, you can change the current setting of this toggle. When you also have the configuration to force end-user access to go through VMware Identity Manager, you can set this toggle to YES to have the end users’ clients automatically redirect to their Workspace ONE environment. Read about the options to force end-user access to go through VMware Identity Manager in Configure the Option to Force End-User Access to Use VMware Identity Manager. With the automatic redirection configured to YES, in the end-user clients, when the client attempts to connect to Horizon Cloud and is forcing access through VMware Identity Manager, the client is automatically redirected to the Workspace ONE environment that is configured in VMware Identity Manager. When the toggle is set to NO, automatic redirection is not enabled, and the clients display an informational message to the user instead.</td>
</tr>
</tbody>
</table>

**Note**  You can have Workspace ONE redirection enabled for only one of the identity management URLs per pod. If you try to enable this feature for multiple VMware Identity Manager URLs and the same pod, an error message is displayed.

4  Click **Save**.

**Configure the Option to Force End-User Access to Use VMware Identity Manager**

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 the Workspace ONE portal that is configured in their VMware Identity Manager environment.

**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 Identity Manager</td>
<td>Select <strong>YES</strong> 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 Identity Manager</td>
<td>Select <strong>YES</strong> 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 VMware Identity Manager, you typically also edit the corresponding identity provider configuration to specify that the end-user clients automatically redirect to the Workspace ONE environment. See **Edit Settings for a Configuration**.

The feature to force end-user access to VMware Identity Manager works with the Workspace ONE redirection feature in the following ways.
<table>
<thead>
<tr>
<th>Force end-user access through VMware Identity Manager setting</th>
<th>Workspace ONE 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 their Workspace ONE environment.</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. 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 VMware Identity Manager 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.

**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 Administration Console for the first time.

After you have finished registering one Active Directory domain and given the Horizon Cloud Super Administrators role to one Active Directory group, then you can perform administration tasks using the Administration Console, and register additional Active Directory domains, as appropriate for your organization's needs.

**Important** System workflows involving pods in Microsoft Azure require that the Horizon Cloud 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 server 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 **Suggested Workflow for When Your Very First Cloud-Connected Pod is from Deploying 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 6-8. Getting Started Wizard Selections

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Capacity       | Provides:  
  - A high-level overview of your environment's existing pods.  
  - Access to the Add Cloud Capacity wizard, used to deploy your first pod in a cloud capacity environment, such as the Microsoft Azure cloud. |
| General Setup  | Provides details and links for the initial configuration of various pod-wide settings, such as registering an Active Directory domain. See **General Setup Section of the Getting Started Wizard**. |
| Desktop Assignment | - When you have pods deploying in Microsoft Azure, this section provides links to task pages related to working with virtual machines (VMs) that are brought in your Horizon Cloud environment, and for publishing master images. Master images are used in farms and VDI desktop assignments. See **Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure** and its subtopics.  
  - When you have Horizon 7 on-premises pods or Horizon 7 pods in VMware Cloud on AWS, this section provides links to task pages related to configuring desktop assignments. Desktop assignments allow you to make desktop pools from multiple cloud-connected pods available to end users. See **Chapter 4 Workflows for Cloud-Connected VMware Horizon 7 Pods**. |
| App Assignment | **Note** In this release, this section is not displayed when your cloud-connected pods are only Horizon 7 pods on-premises or in VMware Cloud on AWS.  
  When you have pods deploying in Microsoft Azure, this section provides links to task pages related to applications and application assignments. See **Applications in Your Horizon Cloud Inventory** and its subtopics. |

When you have completed the required steps of registering at least one Active Directory domain and giving 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 Administration 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 Getting Started Wizard

In the first-time configuration for a pod connected to Horizon Cloud, 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.
### Selection | Description
---|---
**My VMware Accounts** | Give access for other people to log in to the Administration Console and your Horizon Cloud environment using their own My VMware accounts. See Give Administrative Access to People in Your Organization.

**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 Administration 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
- Add Additional Auxiliary Bind Accounts for a Cloud-Configured Active Directory Domain

**Roles & 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 Horizon Cloud Administrative Roles to Active Directory Groups.

**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 Dashboard Page and Reports Page.
Various pages in the Horizon Cloud Administration Console provide a filter field to filter the information that is displayed on those pages.

When a page has a filter field, as you type characters into the field, the system displays only the subset of the displayed records that contain characters that match that pattern.

**Note**  The system begins matching the pattern and filtering the records displayed in the page after you have typed three (3) characters into the filter field.

**On-Screen Filtering in the Reports Pages**

In the tabs of the Administration Console's Reports page, the filtering field 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 field 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 type 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 (Export).

The following screenshot is an example of the Desktop Mapping page where the system has more than 500 records and the pattern entered in the filter field displays the subset of the displayed records.

![Desktop Mapping Page Screenshot](image_url)

---

**Reports**

<table>
<thead>
<tr>
<th>USER MAPPING</th>
<th>DESKTOP MAPPING</th>
<th>DESKTOP HEALTH</th>
<th>UTILIZATION</th>
<th>SESSION HISTORY</th>
<th>CONC...</th>
</tr>
</thead>
</table>

This report has more than 500 items. Please use different filters to reduce the results or export to see the entire data.

<table>
<thead>
<tr>
<th>Desktop Name</th>
<th>Model</th>
<th>Assignment Name</th>
<th>Active User</th>
<th>Mapped Users</th>
<th>Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC11-0140</td>
<td>Standard (61v2)</td>
<td>VD/11</td>
<td>vdluser-508</td>
<td>-</td>
<td>vdlignc</td>
</tr>
<tr>
<td>VC11-0166</td>
<td>Standard (61v2)</td>
<td>VD/11</td>
<td>vdluser-506</td>
<td>-</td>
<td>vdlignc</td>
</tr>
<tr>
<td>VC11-0190</td>
<td>Standard (61v2)</td>
<td>VD/11</td>
<td>vdluser-542</td>
<td>-</td>
<td>vdlignc</td>
</tr>
<tr>
<td>VC11-0244</td>
<td>Standard (61v2)</td>
<td>VD/11</td>
<td>vdluser-544</td>
<td>-</td>
<td>vdlignc</td>
</tr>
<tr>
<td>VC11-0396</td>
<td>Standard (61v2)</td>
<td>VD/11</td>
<td>vdluser-542</td>
<td>-</td>
<td>vdlignc</td>
</tr>
</tbody>
</table>
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:

- Cannot Successfully Log In at the First Login Screen of the 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
- Give Feedback Menu Choice Does Not Work
- Considerations For Using Nested Active Directory Domain Organizational Units
- Horizon 7 Cloud Connector Known Considerations
- When Your Pod is Not Yet Upgraded to Manifest 1230 or Later, How to Configure the Ability for Domain Accounts to Remote Connect to the Imported Image

Cannot Successfully Log In at the First Login Screen of the Administration Console

When the My VMware account system is experiencing a system outage for maintenance, you are not able to log in to the Horizon Cloud Administration 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 Horizon Cloud Administration 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 Administration Console during that period fails.

Solution
◆ If you encounter issues logging in to the Administration Console's first 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 master VM, 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 Master Image 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 master VM, examine the VMware DaaS Agent service and ensure it has its startup type set to Automatic.
3 Reboot the master VM.
4 Try the conversion process again on the rebooted master 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 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 master image, 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 master VM, examine the VMware DaaS Agent service and ensure it has its startup type set to Automatic.

3. Reboot the master VM.

4. Try the conversion process again on the rebooted master 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 Administration 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 Administration 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 Administration Console. For example, if you log in to the Administration 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 server 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 server VMs is in offline status.

**Problem**

Even though the other servers in the farm show online status, the farm creation process cannot complete because one server continues to show offline status.

**Cause**

A temporary network connection loss causes the server's state to show as offline in Horizon Cloud, preventing completion of the farm creation workflow.

**Solution**

1. Navigate to the farm's Servers tab.
2. Select the check box next to the offline server and click **Delete**.

   The system deletes the server VM. Then after a few minutes, the system automatically recreates the server 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](https://answers.microsoft.com).
Give Feedback Menu Choice Does Not Work

When you click the Give Feedback menu choice in the Administration Console, nothing happens or a browser error message appears.

Problem

The Administration Console's Help menu (Help) has a Give Feedback choice. Depending on your settings for your local system's browser or mail application, when you click it, 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 Administration Console's URL to the exception list.
2. Configure your browser's mailto content type's action with a mail application, so that the Give Feedback choice 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 server 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 Administration 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 Horizon Cloud Administration Console.
   
   Only the OU= part of the string is required. The DC= part is optional.

**Horizon 7 Cloud Connector Known Considerations**

Keep these considerations in mind when you are using Horizon 7 Cloud Connector.

- Use of IPv6 with the Horizon 7 Cloud Connector virtual appliance is not supported.
- Proxy SSL configuration is not supported during the deployment of the Horizon 7 Cloud Connector virtual appliance.
- Information about the static IP and proxy settings for the Horizon 7 Cloud Connector virtual appliance is saved in certain container files. See Static IP and Proxy Configuration for the Horizon 7 Cloud Connector Virtual Appliance.
- If you update the static IP address for the Horizon 7 Cloud Connector virtual appliance, you must also perform some additional steps to ensure that the new address is shared with the components that depend upon the virtual appliance. See Update the Static IP for the Horizon 7 Cloud Connector Virtual Appliance.
Before deleting the Horizon 7 Cloud Connector virtual appliance from your vCenter environment, point your browser to the Horizon 7 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 7 Cloud Connector paired with the Horizon 7 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 7 Cloud Connector and Horizon Cloud uses outbound Internet port 443.

You set the password for the root user of the Horizon 7 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 7 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 7 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 7 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.

**Set a Password Expiry Policy for the Horizon 7 Cloud Connector Root User**

You can set the password for the root user of the Horizon 7 Cloud Connector virtual appliance during deployment. 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 7 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 7 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:

   ```sh
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:

   ```sh
chage -M 365 -W 30 root
   ```
To list the current password expiry policy of the root user, enter the following command:

```
chage -l root
```

### Static IP and Proxy Configuration for the Horizon 7 Cloud Connector Virtual Appliance

Information about the static IP and proxy settings for the Horizon 7 Cloud Connector virtual appliance is saved in certain container files.

#### Static IP Storage

The static IP address of the Horizon 7 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
```

#### Proxy Storage

The proxy settings of the Horizon 7 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
```

### Update the Static IP for the Horizon 7 Cloud Connector Virtual Appliance

If you update the static IP address for the Horizon 7 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 7 pod.

#### Prerequisites

Configure a new static IP address for the Horizon 7 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 7 desktops, run the following command.

   `docker exec csms /bin/bash -c "cd /usr/local/csms; ./scripts/address_changed.sh"`

When Your Pod is Not Yet Upgraded 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. As a result, you can use a domain account to log in and customize the master image. However, if you have not yet upgraded your pod to the current release, 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 master 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 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 master image 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 master image VMs in Microsoft Azure using your Remote Desktop Protocol (RDP) software. As part of the overall process of creating the master image VM, these items are put in place:

- The VM is joined to the domain that was specified in the Import Image wizard or when manually creating the master image.
- 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 master 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 master 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 master image that was created using the Import Image 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 master 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 master VM.

After the new GPO is linked to the domain, you can use one of those specified domain accounts to RDP to the master VM and customize it. Follow the steps as described in Customize the Master Image VM’s Windows Operating System and its subtopics.