Deployments and Onboarding to Horizon Cloud for Microsoft Azure and Horizon Pods

Updated for the service starting from January 7, 2021
VMware Horizon Cloud Service
You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/
Contents

Horizon Cloud Deployments and Onboarding Pods — Horizon Pods on VMware SDDCs and Horizon Cloud Pods on Microsoft Azure 5

1 Things to Know Before and During Your Use of Horizon Cloud 16
   Horizon Cloud — Environments, Operating Systems, and Compatibility 20
   For Current Customers with Existing Cloud-Connected Pods — About Horizon Cloud Service Releases 23
   Horizon Cloud — Known Limitations 34
   Horizon Cloud — Known Issues 39

2 Introduction to Horizon Cloud and Onboarding Pods to Become Cloud-Connected Pods 52
   VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist For New Pod Deployments - Updated As Appropriate for Pods That Deploy Starting From the January 2021 Service Release 57
   VMware Horizon Pods with Horizon Cloud - Requirements Checklist - Updated as Appropriate for Connecting Pods Starting from the January 2021 Service Release 74

3 Onboarding Your Very First Cloud-Connected Pod to Your Horizon Cloud Tenant Environment 80
   When Onboarding a Horizon Pod to Use Horizon Subscription Licenses or Cloud-Hosted Services with That Pod 82
   High-Level Workflow When You are Onboarding an Existing Horizon Pod That is Deployed in a VMware SDDC as Your First Pod to Your Horizon Cloud Tenant Environment 84
   DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod 88
   Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector 93
   Connect Horizon Cloud Service with an Existing Horizon Pod to Use Horizon Subscription Licenses or Cloud-Hosted Services or Both 97
   When Adding a Horizon Pod on Microsoft Azure as Your Very First Pod in Your Horizon Cloud Pod Fleet 134
   High-Level Workflow for Adding a Horizon Pod on Microsoft Azure as Your First Pod to Your Horizon Cloud Tenant Environment 140
   Preparing to Deploy a Horizon Cloud Pod on Microsoft Azure 147
   Using the Horizon Cloud Administration Console to Perform an Automated Deployment of a Pod into Microsoft Azure 240
   Troubleshooting If You Encounter Pod Deployment or First-Time Domain Bind Issues 280

4 Now That Your Very First Pod Is Completely Deployed and Connected to Horizon Cloud 304

VMware, Inc. 3
5 Revision History — Changelog — Onboarding to Horizon Cloud for Microsoft Azure and Horizon Pods  305
Horizon Cloud Deployments and Onboarding Pods — Horizon Pods on VMware SDDCs and Horizon Cloud Pods on Microsoft Azure

These documentation topics here apply when you have just received the Welcome to the VMware Horizon Service email and are ready to onboard your first pod. This onboarding set of topics outlines the relationship between the Horizon universal license and your Horizon Cloud tenant account. The license entitles you to use the cloud-hosted services as well as use the subscription licensing with your pods. This topic and its subtopics also outline the process for your first-time onboarding a pod to Horizon Cloud. This first-time onboarding flow is the key that enables you to exploit your Horizon subscription licenses, onboard your existing Horizon pods on VMware SDDCs to cloud-hosted services, deploy new Horizon Cloud pods on Microsoft Azure, and leverage all of the cloud-hosted services that VMware Horizon® Cloud Service™ currently provides for cloud-connected pods.

You onboard an existing Horizon pod that is located in a VMware SDDC to the cloud for two primary use cases: to activate a subscription license for that pod and enable your use of those cloud-hosted services that Horizon Cloud provides for that type of pod. You onboard a Horizon Cloud pod on Microsoft Azure by using the Horizon Cloud Administration Console to deploy that type of pod into your Microsoft Azure cloud subscription.

**Tip** If you already have at least one cloud-connected pod, instead of this onboarding set of topics, use the companion administration set of topics for information about how to onboard subsequent pods after doing your very first one.
Relationship Between Onboarding Your First Pod with the Horizon Universal License, the My VMware Account or VMware Cloud Services Org Associated with That License, Your Horizon Cloud Tenant, and the Welcome Email

Currently, a person's access to use this service can be set up in a variety of ways — a person's specific My VMware account might be registered to use the service, a person might belong to an org in VMware Cloud services within which access to the service is granted, or that person might belong to a Workspace ONE environment that is integrated with Horizon Cloud. VMware Cloud services uses the terms cloud service accounts and VMware IDs (see How Do I Sign Up for VMware Cloud Services).

**Note** VMware Cloud services is also known by the name VMware Cloud Services Engagement Platform. You might see those two names used interchangeably in the Horizon Cloud documentation and in the Horizon Cloud Administration Console.

At a high-level, the connect-the-dots between these elements is:

1. You make your subscription license purchase — either through VMware Sales or through your partner. Currently the Horizon universal license is the license to get. The license will be associated with the specific My VMware account or VMware Cloud services account that is used in the license request.

2. VMware sets up the new Horizon Cloud tenant account, associates it with the same account or VMware Cloud services org or Workspace ONE environment with which the Horizon universal license is associated, and specifies one of the regional Horizon Cloud control plane instances for the tenant account. The information in the license request is used to determine which regional control plane instance is appropriate for the tenant account. These regional control plane instances are related to the data centers that host the cloud control plane, as described in the service description document available from the Horizon Cloud Service Description and Service Level Agreement page.

3. VMware sends the Welcome to the VMware Horizon Service email to the email address associated with the purchase order or the trial request. For an example of this welcome email, see the following screenshot. Among other information, the email states the account and region that are associated with the tenant account. The stated region appears as one of the following strings: USA, Europe, Australia, USA-2, Europe-2, and Australia-2.

**Note** On June 9, 2020, the Welcome email was updated to standardized regional names. If you received your email before that date, your email contains one of these system-generated strings: USA, EU_CENTRAL_1, AP_SOUTHEAST_2, PROD1_NORTHCENTRALUS2_CP1, PROD1_NORTHEUROPE_CP1, and PROD1_AUSTRALIAEAST_CP1.
4 After the email is received, you read the information it contains and use the hypertext links in the Getting Started section to get to key destinations. Those URLs link you to the tenant environment portal (named the Horizon Cloud Administration Console or console for short), the Horizon Cloud Connector software download location, and online documentation.

**Important** After the email is first received, it is prudent to log in to the tenant environment portal and add additional people you want to enable to onboard pods and manage onboarded pods. Adding those people even before onboarding your first pod prevents delays involving timely access to your tenant account. As an example, a delay might occur if the original person is no longer available in your company and you have no one on your team who knows the credentials to log in. Access to your tenant account is needed to onboard pods, as well as to perform related workflows, such as reconfiguring the Horizon Cloud Connector. If access to your tenant account is interrupted as a result of the main person leaving your organization, you would have to open a support request to VMware to update the tenant account’s associated My VMware account, which could cause a delay in your logging in to the onboarding and management portals.

For the steps to add additional people to access the tenant environment, see [Add Administrators to Log in to Your Horizon Cloud Tenant Environment](#).

**Getting the license**

You must get the license first, because that is the point at which VMware generates your Horizon Cloud tenant account and environment.

**Your new Horizon Cloud tenant account in the cloud control plane**
Your Horizon Cloud tenant account is important to you even when your only use case is to use a subscription license with your existing Horizon pods, and not imagining using cloud-hosted services with your pods. The reason why this tenant account is important to you is that same tenant account is use for both:

- Logging in to the Horizon Cloud Connector onboarding and management portal. The Horizon Cloud Connector portal is used for onboarding a Horizon pod to the cloud to use the subscription license, as well as to enable cloud-hosted services. After you complete the initial onboarding of the Horizon pod, you can log in to the Horizon Cloud Connector portal at any time to manage features of the connector itself.

- Logging in to the cloud-based Horizon Cloud tenant environment portal, named the Horizon Cloud Administration Console or console for short. This administrative console is used to add additional administrators so that they can also use the Horizon Cloud Connector onboarding and configuration portal besides the initial account with which the license and access is associated. This console is also used to access the cloud-hosted services, such as the Cloud Monitoring Service’s monitoring dashboard and reports and the pod deployment wizard for deploying into Microsoft Azure.

**How that tenant account relates to the My VMware account or VMware Cloud services cloud services account associated with the license**

One of these accounts must be used to obtain the Horizon universal license in the first place. The initial account is registered with the newly created Horizon Cloud tenant account and environment, and is used for authentication to the Horizon Cloud tenant environment’s portals. When the tenant account is created, the **Welcome to the VMware Horizon Service** email is sent to the specific email address that is configured the My VMware account or VMware Cloud services cloud services account. The following screenshot is an illustration of the welcome mail. You must ensure that you or someone in your organization is able to get the welcome email from that email account which is associated with the initial account which was used to purchase the subscription license, so that you'll can make use of the links in that email to go to downloads for the Horizon Cloud Connector, open the administrative console, and so on.

The following screenshot illustrates a sample of the welcome email and calls out where an My VMware account is referenced.
Your new Horizon Cloud tenant environment and its portal

As soon as you get the welcome email from VMware, the account stated in that email can log in to that newly created Horizon Cloud tenant environment, even when you have zero cloud-connected pods. However, at this initial point, the administrative console provides access to a single initial screen and a small subset of cloud-hosted workflow actions within that screen.

The following screenshot shows the console at the point in time when your tenant account is first created. The list that follows describes the key actions you can take in that screen prior to onboarding your first pod.
Tip   Click on the **General Setup** bar in that screen to see two of the key actions that are listed below.

When your Horizon Cloud tenant record is configured with the option to onboard to VMware Cloud Services Engagement Platform and the tenant is not yet associated with an org in VMware Cloud services, a blue banner will appear at the top of the window that provides a way to activate that onboarding process. The following screenshot illustrates what you might see if your tenant record meets those conditions.

For information about that process, see [Onboard Your Horizon Cloud Tenant to VMware Cloud Services](#). If you are accessing this portal from your Workspace ONE environment by clicking the Horizon Cloud tile, that blue banner will not appear. When your tenant record is not configured with the option to onboard to VMware Cloud Services Engagement Platform, that blue banner will not appear.

- In the **VMware SDDC** row, click **Add** to learn how to download the Horizon Cloud Connector to connect a Horizon pod on VMware SDDC to your cloud tenant. A Horizon
pod on VMware SDDC is the pod type that is based on Horizon Connection Server software components. Such pods are those located in your VMware-supported SDDC, whether in an on-premises vSphere infrastructure or in a cloud-based VMware SDDC environment.

**Note**  After clicking **Add** from this row, please ensure you follow the **Download** links that are displayed in the screen. Those steps are described in **High-Level Workflow When You are Onboarding a Horizon Pod**. Those steps will provide the smoothest experience at this time as they have links to information about prerequisites, DNS and ports requirements, and the precise sequence of steps to follow.

- In the **Microsoft Azure** row, start the automated wizard that will deploy a pod into your subscription in Microsoft Azure. Such pods are based on the VMware Horizon Cloud pod-manager technology.

**Important**  Do not use this row if you want to cloud connect a pod that is located in Azure VMware Solution (AVS). For that scenario, you must follow the steps in **High-Level Workflow When You are Onboarding a Horizon Pod**.

- In the General Setup section, add the first set of administrators to whom you want to give the ability to log in to the Horizon Cloud Connector onboarding and configuration portal and the Horizon Cloud Administration Console (the portal to your tenant environment). The My VMware account that was used for setting up the tenant is prefilled there by default. As a result, you will see that row marked with a green check mark. However, that is only because there is always the one initial My VMware account associated with the tenant account when the tenant environment is created.

**Tip**  To prevent being locked out of both your tenant environment and the Horizon Cloud Connector onboarding and configuration portal due to the initial My VMware account going inactive for some reason — such as that person leaving your company or organization — it is prudent to add your first set of administrators as soon as you receive the **Welcome to Horizon Service** email, even before you onboard a pod for the first time.
In the General Setup section, verify the Cloud Monitoring Service (CMS) settings you want. The CMS is enabled by default, so you will see that row marked with a green check mark. At this point, you can choose to deactivate that feature even prior to onboarding any pods.

Tip Before you can access other actions and workflows in that portal beyond the above four, you must have an onboarded pod, that pod must be up and online and communicating with the cloud management plane, and have an Active Directory domain registered with your tenant environment. The console blocks access to other management actions until the Active Directory domain registration workflow is completed. For information about this workflow, see Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment.

Onboarding Requirements Checklists

If your first pod onboarding is to exploit your Horizon subscription license with a Horizon pod deployed in a VMware SDDC, before starting the steps described in this onboarding documentation set, first read VMware Horizon Pods with Horizon Cloud - Requirements Checklist - Updated as Appropriate for Connecting Pods Starting from the January 2021 Service Release. That topic describes various prerequisite elements needed to successfully connect a Horizon pod to Horizon Cloud. After that pod is cloud-connected, the Horizon subscription license is pushed from the cloud to the pod and you can start enabling the cloud-hosted services for that pod within the administrative console itself.

If your first pod onboarding is for a Horizon Cloud pod on Microsoft Azure — the pod-manager-based pod type — before starting the steps described in this onboarding documentation set, first read VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist For New Pod Deployments - Updated As Appropriate for Pods That Deploy Starting From the January 2021 Service Release. That topic describes various prerequisite elements needed to have a successful automated pod deployment of that pod type.

Revision History for these Onboarding Topics

This documentation set of topics is updated with each release of the product or when necessary. For the set of significant revisions made to date, see Chapter 5 Revision History — Changelog — Deployments and Onboarding to Horizon Cloud for Microsoft Azure and Horizon Pods.
Intended Audience

The information in this document is intended for experienced data center administrators with knowledge in the following areas.

- VMware Horizon and VMware Horizon Connection Server
- VMware Horizon Cloud Connector
- VMware Unified Access Gateway™
- VMware Workspace ONE® Access™
- Virtualization technology
- Networking
- VMware Cloud™ on AWS (VMware Cloud)
- VMware Horizon on VMware Cloud™ on AWS
- Azure VMware Solution (AVS)
- Microsoft Azure

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.
- In the console, clicking ☰ > Support, displays the link to that KB 2144012 also.
Selected Pod-Related Terminology Used in these Deployment Guide Documentation Topics

Throughout the Horizon Cloud documentation topics, you will see the following phrases. These phrases have the indicated meanings as follows.

**Horizon pod on VMware SDDC**

A pod that is constructed based on VMware Horizon product software, and which includes Horizon Connection Server software components. The Horizon Connection Server components are running in a supported form of an VMware SDDC (software-defined data center) that VMware supports for use with such pods. Some examples of such VMware SDDCs are an on-premises vSphere environment, VMware Cloud on AWS, or Azure VMware Solution, to name a few.

**Horizon pod on Microsoft Azure, Horizon Cloud pod on Microsoft Azure, Horizon Cloud pod**

A pod that is constructed by running the Horizon Cloud pod deployment wizard which deploys a pod-manager-based pod into your Microsoft Azure subscription. This type of pod is based on VMware Horizon Cloud pod-manager technology, and is supported to run in Microsoft Azure solely.

**Note**  A Horizon pod on Microsoft Azure is separate and distinct entity from a Horizon pod on Azure VMware Solution (AVS). Those two are based on completely different technology — one is based on Horizon Connection Server technology and one is based on the Horizon Cloud pod-manager technology.

**connection broker**

A connection broker is responsible for connecting end users' clients with a virtual desktop VM or farm VM for the purpose of setting up a connected session between each end-user client and the agent running in that VM. This noun — broker — is used because one general definition of the noun broker in the English language is one who negotiates a transaction.

In desktop virtualization software's use cases, the connection broker receives the end-user's client request to make a connection with a virtual desktop VM or farm VM. The connection broker then routes the request appropriately and negotiates a connected session between the agent running in one of the VMs and that end-user client. The negotiation takes into consideration what types of pod-provisioned resources the end user is entitled to make connections with.

The Horizon Cloud control plane provides two distinct connection brokering technologies: Universal Broker and Single-Pod Broker (available for Horizon Cloud pods in Microsoft Azure only). Universal Broker is a multi-tenant, cloud-based service that enables the brokering of resources that span multiple pods and makes brokering decisions based on the geographic sites of users and pods. Single-Pod Broker enables the brokering of resources from a single Horizon Cloud pod in Microsoft Azure.
The Horizon Connection Server within a Horizon pod on VMware SDDC, or the pod manager VM within a Horizon Cloud pod in Microsoft Azure, facilitates the routing of the end-user client to a resource in the pod that meets the client’s connection request. (Remember that a Horizon pod on Azure VMware Solution actually has the Horizon Connection Server and not the pod manager.)

**About the Screenshots**

The screenshots typically:

- Show only that portion of the overall user interface screen that corresponds to the text at which point the screenshot appears, and not necessarily the full user interface.
- Have blurred areas where appropriate to maintain data anonymity.
- In the PDF format, screenshot images that are wider than 6 inches are automatically resized. As a result, such images might appear blurry in the PDF format. In the parallel HTML pages, you can click on such wide screenshot images to see the image at its full-size.

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

**VMware Technical Publications Glossary**

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, visit [http://www.vmware.com/support/pubs](http://www.vmware.com/support/pubs).
Things to Know Before and During Your Use of Horizon Cloud

Use the following information and the linked-to subtopics when preparing to use Horizon Cloud and during your use. Refer back to this information throughout your journey using Horizon Cloud.

Set-Up Prerequisites, Software Downloads, User Settings Persistence, Product Documentation, and Additional Helpful Resources

Set-up prerequisites

For Microsoft Azure deployments, review the set-up prerequisites before you start deploying.

- VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist
- Preparing to Deploy a Horizon Cloud Pod on Microsoft Azure

For connections to your Horizon pods, review the set-up prerequisites before you start. See the following documents:

- Release Notes and Installation guide for the VMware Horizon software you are using in those pods, linked from either VMware Horizon 7 Documentation page or VMware Horizon Documentation page.
- VMware Horizon on VMware Cloud on AWS Deployment Guide (for manually installing a pod in your VMware Cloud on AWS SDDC)
- When Onboarding a Horizon Pod to Use Horizon Subscription Licenses or Cloud-Hosted Services with That Pod (for onboarding the pods to Horizon Cloud)

Software downloads

Review the software downloads you might want for your environment from My VMware®. Even though these downloads might be optional to have before you get started with your particular deployment, depending on your use case scenario, you might want to review them prior to deploying. See the VMware Horizon Cloud Service download page and navigate the downloads link for this specific January 2021 release. Within that same page, you will see the Horizon Cloud Connector row and can click on its Go to Downloads to obtain the latest versions of both the Horizon Cloud Connector and VMware Universal Broker Plugin installer. For a table of which version of VMware Universal Broker Plugin Installer goes with which
Horizon Connection Server, see the table in the topic Horizon Pods - Install the Universal Broker Plugin on the Connection Server.

User settings persistence

For all Microsoft Azure deployments, you can provide persistence of user profiles using VMware Dynamic Environment Manager™ with folder redirection. You can download the Dynamic Environment Manager software that is supported for use with this release from the VMware Horizon Cloud Service download page and navigate the downloads link for this specific release.

Product documentation and additional helpful resources

To access all of the product documentation for the various deployment models of Horizon Cloud, see the VMware Horizon Cloud Service documentation landing page.

Visit the community site for helpful tips and to ask any questions. Technical papers are also available in the Resources section of the Horizon Cloud product page.

Useful Facts to Know Before Using Horizon Cloud

Before doing any deployment type

- When your Horizon Cloud environment is not integrated with your Workspace ONE environment, login authentication into the cloud-based 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 console during that time period. If you encounter issues logging in to the console's first login screen, check the Horizon Cloud System Status page at https://status.horizon.vmware.com to see the latest system status. On that page, you can also subscribe to receive updates.

- When deploying a pod using the console's pod deployer wizard and when connecting a Horizon pod using Horizon Cloud Connector, specific DNS names must be reachable and specific ports and protocols must be allowed. See DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod, DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features, and Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later for the connectivity requirements.

- Each of the pods paired with the Horizon Cloud control plane and associated with the same customer account must have line of sight to the Active Directory domains connected to those pods and have one-way or two-way trust configured along with that...
line of sight. For example, when you have three pods where one pod is in Microsoft Azure, one pod is on-premises, and one pod in VMware Cloud on AWS, each of those pods must have line of sight and one-way or two-way trust configured to the same set of Active Directory domains.

**Before doing Microsoft Azure deployments**

- **Subscriptions and Number of Pods:** Be mindful about the number of pods you deploy into a single Microsoft Azure 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 many 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 can, and often prefer, this approach because it provides some benefits for ongoing management of the subscriptions. Using this approach, you would deploy a single pod per subscription, roll up those subscriptions in a single "primary account", and avoid the chances of hitting the Microsoft Azure limits that are imposed on a single subscription.

- **Outbound Internet access is required on the Microsoft Azure Virtual Network (VNet) that is connected to the node's temporary jump box VM and pod manager VM (or plural VMs for the case where high availability is enabled on the pod).** Proxy-based authentication is supported in this release. You must provide your proxy details in the pod deployment wizard. For pod deployment, specific DNS names must be reachable and specific ports and protocols must be allowed. See [DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features](#) for the connectivity requirements.

- **Subnet sizing:** Expanding the size of the pod's subnets after the pod is deployed is not currently supported. As a result, for production environments, you should use subnet sizes that are large enough to accommodate the following requirements:
  - **Management subnet:** When deploying a pod, as of March 2019, the pod's management subnet is required to have a minimum of CIDR /27, where in previous releases a lower minimum CIDR of /28 was allowed. This change was made to reduce the occurrence of issues that can happen during pod updates due to lack of available IP addresses in the subnet. A CIDR of /27 provides for 32 IP addresses.
  - **VM subnet - primary:** Use a CIDR in a range that is large enough to accommodate attaching the VMs for your anticipated VDI desktops, the RDS images, and every VM in the pod's RDS farms. The pod manager VMs and the Unified Access Gateway VMs...
also need some IP addresses from this subnet (12 addresses total to accommodate the blue-green update of an HA-enabled pod with both types of gateways). Generally speaking, the range of /24 to /21 would provide for typical use cases. Note: At times, this VM subnet is referred to as the desktop subnet or the tenant subnet.

- Starting with service release July 2020 and pod manifest 2298.0, a new feature provides for using additional tenant subnets for your VDI desktops and RDS farm VMs. Those additional subnets can be in the same VNet as the pod or in peered VNets. For a pod at manifest 2298.0 or later, you can edit the pod’s configuration to include those additional subnets. Then you can specify use of those additional tenant subnets in the definitions of your farms and VDI desktop assignments instead of them using the primary VM subnet. Use of these secondary subnets for your farm VMs and VDI desktop VMs provides for simplified administration, because you can specify which farms and VDI desktop assignments are on which tenant subnet and VNet.

- To leverage the feature to deploy the external gateway into its own VNet, the VNets must be peered. As a result, you must create the subnets manually in advance of running the deployment wizard. For the external gateway’s VNet, its management subnet and back-end subnet must each adhere to the same minimum CIDR /27.

**Before connecting pods using Horizon Cloud Connector**

- If your Horizon Cloud tenant account was created on or after March 17, 2020 in one of the following regions: US-2, Europe-2, Australia-2 (also formerly known as PROD1_NORTHCENTRALUS2_CI1, PROD1_NORTHEUROPE_CI1, PROD1_AUSTRALIAEAST_CI1), you must use Horizon Cloud Connector version 1.6 or later to connect those pods to Horizon Cloud. The date on your Welcome to Horizon Cloud Service email is the date to use to determine if your tenant account was created after March 17, 2020. The email also states the region in which your account is created. Earlier versions of the Cloud Connector will have compatibility issues when used with tenant accounts created on or after March 17, 2020 in those regions.

- Outbound Internet access is required for the Horizon Cloud Connector to communicate with the service’s cloud plane, especially to receive the licensing details. Specific DNS names must be reachable and specific ports and protocols must be allowed. See [DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod](#) for the connectivity requirements.

- Before connecting a second Horizon pod to Horizon Cloud, you should log in to the Horizon Cloud administrative console and complete the Active Directory domain registration process after connecting your first Horizon pod using the Horizon Cloud Connector’s onboarding process. If you pair multiple Horizon pods with Horizon Cloud before completing that Active Directory domain registration, unexpected results might occur when you eventually log in to the console to attempt the domain registration process.

- Due to a known issue, when you are using an on-premises Active Directory domain to service a pod in VMware Cloud on AWS, slow access times might occur due to network
latency or network congestion between that on-premises Active Directory domain and
the pod in VMware Cloud on AWS which results in calls to the domain timing out.
Symptoms of this latency typically include the Active Directory login screen failing to
complete the login before timing out. If you experience such symptoms, configuring a
writable domain controller in each in-cloud software-defined data center (SDDC) might
help.

This chapter includes the following topics:

- Horizon Cloud — Environments, Operating Systems, and Compatibility
- For Current Customers with Existing Cloud-Connected Pods — About Horizon Cloud Service
  Releases
- Horizon Cloud — Known Limitations
- Horizon Cloud — Known Issues

**Horizon Cloud — Environments, Operating Systems, and Compatibility**

This documentation topic provides information about the environments and operating systems
that are relevant when using Horizon Cloud. This topic also provides pointers to where to find
information about compatibility of the current service level with other VMware products.

**Compatibility with other VMware Products**

For the most recent information about compatibility between this product and other VMware
products, see the [VMware Product Interoperability Matrices](#).

**Browser Experience**

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

**Microsoft Azure Cloud Support**

For Microsoft Azure deployments, the service is currently available in the following Microsoft
Azure cloud environments.

- Microsoft Azure (Commercial)
- Microsoft Azure in China
- Microsoft Azure Germany (Public)

**Note**  Currently, the High Availability (HA) capable architecture for pods in Microsoft Azure is not provided for pods in Microsoft Azure in China.

### Supported Microsoft Windows Operating Systems

In the service's Microsoft Azure deployments, the following Microsoft Windows operating system editions and versions in the Azure Marketplace are the ones supported for use in this release, regardless of whether you use the automated or manual method of deploying an image in this release.

- For the supported non-Windows 10 operating systems, see [VMware Knowledge Base Article 78170](#).
- For the supported Windows 10 operating systems, see [VMware Knowledge Base Article 70965](#).

The service also provides Tech Preview support for Windows 7 virtual desktops with Extended Security Updates. If your Welcome to Horizon Service email indicates that your Horizon Cloud tenant account was created in one of the following regions, you have access to this Tech Preview operating system using your Horizon Cloud tenant: US-2, Europe-2, Australia-2 (previous names appeared as PROD1_NORHCENTRALUS2_CP1, PROD1_NORTHEUROPE_CP1, PROD1_AUSTRALIAEAST_CP1). With virtual desktops based on this operating system, you can use the Horizon Windows client, RDP 8.x protocol, and the Horizon remote experience features USB redirection and Help Desk. Use of GPU with NV-series VMs is not supported.

### Supported Horizon Client Versions for Microsoft Azure Deployments

To see the specific versions of Horizon Clients that are compatible with the desktops and remote applications brokered by your pods in Microsoft Azure, see the [VMware Product Interoperability Matrices](#) and select Horizon Cloud Service on Microsoft Azure and VMware Horizon Clients in the drop-down menus. You can obtain the Release Notes for the Horizon Client versions from the VMware Horizon Client Documentation page at [docs.vmware.com/en/VMware-Horizon-Client/](docs.vmware.com/en/VMware-Horizon-Client/)

**Note**  The VMware Horizon HTML Access client does not support certain features when used in mobile browsers. Also, even though the Horizon Client supports copying and pasting text between a client's local system and a VM out of the box, for HTML Access, you must configure this feature before your end users can use it. For more information, see the [VMware Horizon HTML Access documentation page](#) and search for the information in the most recent [User Guide](#) and [Installation and Setup Guide](#).
Supported NSX Cloud Versions with Microsoft Azure Deployments

For pods at this release's manifest version (new pods or upgraded pods), using NSX-T Data Center 2.5 or later is recommended. For pods at the prior release's manifest version, the NSX-T Data Center patch release (patch release 2.3.0.1.0, build 10539383) will continue to work. Note: When using NSX-T Data Center 2.4 or 2.5, additional configuration steps are needed on the forwarding policies for the NSX-managed VMs. For details, see the Administration Guide.

Versions for Cloud-Connected Horizon Pods

See the VMware Product Interoperability Matrices tool for the matrix of supported versions of Horizon pod software with Horizon Cloud Connector. To get the benefits of advanced features that are only available for cloud-connected Horizon pods, you must have more recent versions of the Horizon Cloud Connector and Horizon pod software. You can download the latest Horizon Cloud Connector appliance and VMware Universal Broker plugin installer by navigating to the Horizon Cloud Connector section located within the VMware Horizon Cloud Service download page.

Important You must use the version 1.6 or later of Horizon Cloud Connector if your Horizon Cloud customer account was created in one of the following regions: US-2, Europe-2, Australia-2 (previous names appeared as PROD1_NORThCENTRALUS2_CP1, PROD1_NORTHEUROPE_CP1, PROD1_AUSTRALIAEAST_CP1). Only version 1.6 and later versions is compatible with those regions. Your Welcome to Horizon Service email states in which region your account was created.

When you plan to upgrade both Horizon Cloud Connector and Connection Server for a cloud-connected Horizon pod, make sure to monitor and verify the health of the pod during the upgrade process. Monitoring the Horizon pod’s health can help with troubleshooting any issues that might arise. Upgrading the Connection Server on a cloud-connected Horizon pod can sometimes result in problems with the health of that Horizon pod. If you then subsequently try to upgrade the Horizon Cloud Connector paired with that unhealthy Horizon pod, the upgrade of Horizon Cloud Connector might fail. Follow this best practice:

1 After upgrading the cloud-connected Horizon pod's Connection Server, verify that the pod is in good health.

2 To view the pod's health status, first log in to the Horizon Cloud administrative console and perform an Active Directory domain bind. That step allows you to access the console's Capacity page where you can verify that the pod shows a health status of Online or Ready.

3 If the pod shows an unhealthy status, contact VMware Support to get help with resolving any connectivity issues involving the pod before you attempt the Horizon Cloud Connector upgrade.

About Use of IPv6

Horizon Cloud does not support use of IPv6.
For Current Customers with Existing Cloud-Connected Pods — About Horizon Cloud Service Releases

Use the information in this page in tandem with the What’s New in the Release Notes. Along with the items listed in the Release Notes document, this page is for those of you who already have existing cloud-connected pods onboarded in your environment prior to the January 2021 service refresh date, or you have previous experience with Horizon Cloud features and workflows. This page describes the significance the newly debuted features and changes might mean to you and those pods. Only significant changes to the features and workflows are described. Minor changes, such as new layouts and color schemes in the administrative console that do not significantly change the workflows are not detailed here.

To see the up-to-date information about the various workflows that you perform in your Horizon Cloud tenant environment, read the documentation topics found in the individual guides linked from the Horizon Cloud Service documentation page.

Important For information that is key to understanding terms used in this page, see the information in the Release Notes document prior to reading the information in this page. The Release Notes document has key relevant pieces of information such as the latest pod manifest number for pods that deploy into Microsoft Azure. Also keep in mind that the key facts described in the following section are true in every Horizon Cloud release.

The following sections go back to September 2019. Similar information for earlier releases is not available for publication.

Six Key Facts About Every Horizon Cloud Release

- All new cloud-plane-based features that are agnostic to pod manifest version level or Horizon Cloud Connector version level or Horizon pod version level or control-plane regional differences are automatically provided to both existing customers and new customers. As an example, a new feature that does not depend on new APIs for API calls between the cloud plane to the pods or related to Horizon Cloud Connector will be visible and exploitable by existing customers unless otherwise noted below or noted in the product guides. To illustrate this point, one such feature is the console's enhanced feedback submission. Even though this feedback icon debuted in July 9, 2020, the icon and flow is available for use by tenant environments that existed prior to July 9, 2020 even prior to updating the pods or Horizon Cloud Connector to their latest versions.

- The VMware Horizon Cloud Service team debuts new cloud-plane-based features that are agnostic to pod manifest version level or Horizon Cloud Connector version level or Horizon pod version level on an ongoing, regular basis and on any week of the calendar year. The Release Notes document contains the debut dates of those features.

- Starting on the day on which that manifest version debuts in the cloud control plane, the pod deployer for deploying pods into Microsoft Azure always deploys pods at the latest pod manifest version.
Already deployed pods that exist in your service tenant prior to the day on which a new pod manifest version debuts in the cloud plane will continue running at their existing manifest version until they are updated to the manifest that is brand new for the release. The following facts apply:

- New service features which have zero dependencies on APIs that require the latest manifest level will be available for those existing pods.
- New service features which rely on APIs at the latest manifest level will not be available for those existing pods until those pods are updated.
- Some new service features might depend on the cloud plane region in which your tenant account is located. Such features are noted in the documentation where applicable. Your control-plane region is stated in the Welcome to Horizon Service email sent when the customer account is created, as described in *Deployments and Onboarding to Horizon Cloud for Microsoft Azure and Horizon Pods*.

The console’s Import VM from Marketplace wizard uses the Horizon Agents Installer (HAI) that is built into the pod manifest. As a result, pods deployed at the latest manifest version will have the latest HAI built into them, and running the Import VM wizard and selecting a pod at the latest level will install the agents from that latest HAI. For pods that are not yet updated to the latest manifest level, the Import VM from Marketplace wizard uses the HAI version that was available when their respective pod manifests were built.

Horizon pods are onboarded to Horizon Cloud for two primary use cases: to activate use of a subscription license with those pods and to enable use of cloud-hosted services that Horizon Cloud provides for Horizon pods. Each pod is onboarded using the Horizon Cloud Connector. The origin of onboarding Horizon pods to Horizon Cloud started with Horizon 7 version 7.6 environments and Horizon Cloud Connector 1.0 for activating subscription licenses on Horizon pods. Then with each new version of Horizon combined with a new version of Horizon Cloud Connector, additional cloud-hosted services become available for cloud-connected Horizon pods running the latest Horizon version paired with the latest Horizon Cloud Connector version. We recommend customers having earlier versions of Horizon Cloud Connector to update to this latest version to take advantage of new features as well as security and resiliency fixes. Also, see the [VMware Product Interoperability Matrices tool](https://www.vmware.com/products/product-interoperability-matrix.html) for the matrix of currently supported versions of Horizon pod software with Horizon Cloud Connector. If you are running a combination of Horizon Connection Server and Horizon Cloud Connector version that no longer matches that matrix, please update as soon as possible to a supported combination.

**January 2021 - v2101**

Use the following information when you are an existing customer with cloud-connected pods dating from before January 2021 and you want to understand any effects on your experience from the features described in the [Release Notes What’s New January 2021](https://www.vmware.com/support/pubs/horizon_2_webapp_release_notes.html).
New versions of the following key binaries have debuted in January 2021: a new pod manifest version for service-deployed pods, new versions of Horizon Cloud Connector, Universal Broker Plugin Installer, and the Horizon Agents Installer (HAI).

This list is based on the items listed in the What's New January 2021 section of the Release Notes page.

**New items related to Horizon Cloud Connector and its use with Horizon pods**

- With Horizon Cloud Connector 1.9, the automatic update feature now has a simpler configuration for the network details. You only need to provide an unassigned static IP address for the new appliance for upgrade.
- Horizon Cloud Connector 1.9 enables more secure access methods when troubleshooting the Horizon Cloud Connector appliance. SSH access for the appliance's root user is disabled and a new custom user (ccadmin) is now available for SSH access, including support for using an SSH public key instead of password credentials.

**New items related to service-deployed pods in Microsoft Azure**

The pods now support the ability to rollback the dedicated desktop to a previous usable state in the event that the agent update fails and a configurable failure threshold that provides a fail-fast mechanism that will stop the update process and skip any remaining desktops. For this feature to be used with a previously existing pod, that pod must first be updated to manifest 2632.0 or later.

**Additional items of note for current customers**

As documented in the Release Notes document, some cloud-plane-based features debuted in the weeks prior to the v2101 release. See that document for those details.

For pod manifests of 2474.0 and later, the set of Active Directory permissions for the domain join accounts is reduced to provide more flexibility for tenants. However, because the system will use the same domain join accounts in domain-join-related operations with all of the pods in your tenant's fleet, when your fleet includes pods of manifests prior to 2474.0, you must ensure your domain join accounts have the prior set of permissions that those pods require. When all of your Horizon pods in Microsoft Azure are updated to pod manifest 2474.0 or later, then you can adopt the newer reduced set of Active Directory permissions for your domain join accounts. See Service Accounts That Horizon Cloud Requires for Its Operations and the updated section about the permissions for the domain join account.

The console is enhanced to reflect some new terminology. Previously, the console displayed labels such as On-Premises and VMware Cloud on AWS when referring to cloud-connected Horizon pods that are installed in on-premises vSphere installations or in a VMware Cloud on AWS SDDC (software-defined data center). These are the pods that are based on the Horizon Connection Server software. With the availability of Horizon pod deployments on additional cloud-hosted VMware SDDCs such as Horizon pod on Azure VMware Solution (AVS) and Horizon pod on Google Cloud VMware Engine (GCVE), the console is enhanced to use the label VMware SDDC when referring to those members of your tenant's pod fleet.
Support is added for running the Enrollment Server on Microsoft Windows Server 2019. The Enrollment Server is used for the True SSO feature. Installation of Enrollment Server on Microsoft Windows Server 2008 is no longer supported.

October 2020 - v2010

Use the following information when you are an existing customer with cloud-connected pods dating from before October 2020 and you want to understand any effects on your experience from the features described in the Release Notes What’s New October 2020.

New versions of the following key binaries have debuted in October 2020: a new pod manifest version for service-deployed pods, new versions of Horizon Cloud Connector, Universal Broker Plugin Installer, and the Horizon Agents Installer (HAI).

This list is based on the items listed in the What’s New October 2020 section of the Release Notes page.

**New items related to Horizon Cloud Connector and its use with Horizon pods**

- Horizon Cloud Connector version 1.8 is released in both OVA and VHD forms.
- Horizon Cloud Connector 1.8 provides the ability to select a deployment profile to either enable with subscription license support only or with Horizon Cloud features. This selection is made during the deployment of the appliance.
- Horizon Cloud Connector now supports Horizon pods that are deployed on Azure VMware Solution (AVS). Currently, this support is for use of your subscription license with those deployments. The full set of cloud-hosted services are not yet provided for these deployment types.

**New items related to service-deployed pods in Microsoft Azure**

Horizon Cloud on Microsoft Azure pods now support the ability to specify custom Azure Resource Tags during a pod deployment or gateway deployment. The pod deployer applies the specified tags on the resource groups that the pod deployer creates. For a description of the resource groups that the pod deployer creates, see Resource Groups Created for a Pod Deployed in Microsoft Azure. This new feature is not dependent on the pod manifest version.

July 2020 - v3.1

Use the following information when you have cloud-connected pods dating from before July 2020 and you want to understand any effects on your experience from the features described in the Release Notes What’s New July 2020.

**Specifically about existing cloud-connected Horizon pods**

Debut of Horizon Cloud Connector 1.7. For its features, see the July 2020 What’s New in the Release Notes.

**Specifically about existing pods in Microsoft Azure**
For the following new features described in the Release Notes document's July 2020 What's New section to be used with a previously existing pod, that pod must first be updated to manifest 2298.0 or later to take advantage of the feature.

- Multiple tenant subnets for use with farms and VDI desktop assignments. This feature is not yet available for use with multi-cloud desktop assignments, which are used in a tenant configured with Universal Broker.
- Use of the advanced session load balancing for RDSH farms.
- Ability to cancel both desktop and farm expansion tasks that are in a queued or running state, with support for automatic desktop assignment and farm resizing. This feature is not yet available for use with multi-cloud desktop assignments, which are used in a tenant configured with Universal Broker.
- To provide for improved end-user login times, the time it takes for a VM to get to agent-ready state for pod-provisioned desktop VMs that are powered off and need to power on to fulfill an end user's request for a desktop has been reduced.
- Use of the App Volumes features — the pods must be updated to this release's manifest version and your customer account must be located in one of the following Horizon Cloud control-plane regions: USA-2 (PROD1_NORTHCENTRALUS2_CP1), Europe-2 (PROD1_NORTHEUROPE_CP1), or Australia-2 (PROD1 AUSTRALIAEAST CP1). Your control-plane region is stated in your Welcome to Horizon Cloud Service email.

When deploying a gateway configuration on your pod, in addition to the Standard_A4_v2 VM size in previous releases, you now have the option to use the Standard_F8s_v2 VM size, which provides more vCPUs for each Unified Access Gateway instance. For existing pods, this new feature is available when editing the pod to add a new gateway configuration to that pod.

**Additional items of note for current customers**

An enhancement to submitting product feedback is now available in the console's header bar, for all existing customers.

Pods that can have the high availability (HA) feature are now supported for Microsoft Azure Government (US Gov Virginia, US Gov Arizona, US Gov Texas). If you have an existing pod in Microsoft Azure Government for which you want this feature, please contact your VMware representative for that enablement.

**March 2020 - v3**

Use the following information when you have cloud-connected pods dating from before March 2020 and you want to understand any effects on your experience from the features described in the Release Notes What's New March 2020.

**Specifically about existing cloud-connected Horizon pods**

The debut of Horizon Cloud Connector 1.6.x provides a command-line diagnostic tool for you to check the health of required Horizon pod's system components and services that are needed for Horizon Cloud Connector to successfully pair the pod with Horizon Cloud. Before
you log in to the web-based configuration portal and run the pod configuration wizard, you can run this diagnostic tool to check for things that might prevent a successful outcome. If there are issues discovered, the tool will report the component name, details, and recommended remediation steps.

**Specifically about existing pods in Microsoft Azure**

For the following new features described in the Release Notes document's March 2020 What's New section to be used with a previously existing pod, that pod must first be updated to manifest 1976.0 or later to take advantage of the feature, unless otherwise noted.

- To support advanced deployment configurations, when using a separate subscription for the external Unified Access Gateway configuration, you can choose to deploy the Unified Access Gateway resources into an existing customer-created resource group, instead of the default one created by the pod deployer. For an existing pod to take advantage of this new feature, the pod must first be updated to at least manifest version 1763 or later (the December 2019 manifest). Then you need to meet all the documented requirements for using a separate subscription, VNet, and custom resource group for the external gateway configuration, including peering that VNet with the pod's VNet and creating the resource group in that subscription. Then you must delete the pod's existing external Unified Access Gateway configuration, using the console's workflow to delete that existing external gateway. When the deletion is completed successfully, then you can run the **Edit Pod** workflow to add back an external gateway using the new option to place the externalUnified Access Gateway in your existing resource group.

- Support for administrators to specify that the names of the dedicated VDI desktop assignments are displayed in the end-user clients after a VDI desktop VM gets assigned to the end user, instead of displaying the desktop VM name. Previously, after an end user claimed a specific VDI desktop VM, their client displayed the name of the desktop VM by default and that behavior was not configurable. This option does not change what is displayed for those end-user connections that are going through Workspace ONE Access. Workspace ONE Access always displays the dedicated VDI desktop assignment name, and when the end user launches the desktop VM from Workspace ONE Access, the desktop name is displayed in their end-user client. Even though you will see this feature's option in the General Settings page, a pod must be running manifest 1976.0 or later for it to be able to take advantage of this feature.

- Pod manifest 1976.0 or later supports administrators to put an individual farm VM into a maintenance mode, so that the administrator can perform maintenance actions on the VM. Before you can exploit this feature to set a per-VM maintenance mode, the pod must be running this release's manifest version. Also, due to a known issue in the console, even though this feature's options are displayed in the farm's Servers tab in the console, those user-interface options will not set the mode until the agents in the farm's VMs are running version 20.1.0 or later.

**Additional items of note for current customers**
Enhancements in the reports available in the console's Reports page and Dashboard page. The data in these reports is provided by the Cloud Monitoring Service. Existing pods can take advantage of this feature.

December 2019 - v2.2

Use the following information when you have cloud-connected pods dating from before December 2019 and you want to understand any effects on your experience from the features described in the Release Notes What's New December 2019.

Specifically about existing cloud-connected Horizon pods

Starting in this release:

- Some things that are within your control can prevent a successful automatic update of the Cloud Connector, such as insufficient datastore space in your vCenter environment to accommodate the update. Starting in this release, if automated update is enabled for your Horizon Cloud tenant account, such items are identified in the console, so that you can address and clear those items.

- Automated updates of Horizon Cloud Connector are now supported for Horizon pods deployed in VMware Cloud on AWS.

- Enhancements to the Horizon Cloud Connector onboarding success screen include a health status display for the connector's components and an option for activating and deactivating SSH on the Horizon Cloud Connector appliance.

Specifically about existing pods in Microsoft Azure

For the following new features described in the Release Notes document's December 2019 What's New section to be used with a previously existing pod, that pod must first be updated to manifest 1763.0 or later to take advantage of the feature, unless otherwise noted.

- To support advanced deployment configurations, the pod deployer provides options for:
  - Using a separate VNet for the external gateway configuration's Unified Access Gateway instances, separate from the pod's VNet and the core pod elements. The VNets must be peered.
  - Using a separate subscription for the external Unified Access Gateway configuration, separate from the subscription used for the core pod elements. Because a VNet is scoped to a subscription, the separate subscription deployment scenario is also the separate VNet scenario. The VNets must be peered.
  - For an existing pod to take advantage of this feature, the pod must first be updated to manifest 1763.0 or later. Then you need to meet all the documented requirements for using a separate VNet for the external gateway configuration, including peering that VNet with the pod's VNet. Then you must delete the pod's existing external Unified Access Gateway configuration, using the console's workflow to delete that existing external gateway. When the deletion is completed successfully, then you can run the Edit Pod workflow to add back an external gateway using the new options.
Starting with this release's manifest, you can use SSD disk types for VDI desktop assignments and RDSH farms.

Starting with this release's manifest, you can customize the OS disk sizes for VDI desktop assignments and RDSH farms. At earlier pod manifests, their OS disk sizes were set to be the same as the published base image, which was 127 GB by default and could not be changed.

New in this release, in the Import VM from Marketplace wizard, you will see a toggle that provides the ability to omit joining the resulting VM to an Active Directory domain. Previously, this workflow joined the VM to the domain by default and you could not change that behavior. This new toggle is available for existing pods prior to this release's manifest version.

With the redesign of the Capacity page in this release, the Type view is removed. With the removal of the Capacity page's Type view, there are two changes to note about items that were previously accessed from that view: the action to view the pod's current usage of its subscription's Microsoft Azure limits has moved to the pod's details page and the \textbf{Remove Subscription} action that had been present in that view is removed completely.

\textbf{Additional items of note for current customers}

- Enhancements in the reports available in the Administration Console's Reports page. The data in these reports is provided by the Cloud Monitoring Service.

- Enhancements to the Horizon Cloud Administration Console's Capacity page. Instead of having to drill-down into a pod's details page to modify the pod's configurable details or to delete a pod from your tenant environment, you can now initiate the edit pod and remove pod workflows from the Capacity page itself. As a result of this redesign, the workflows for modifying location information that were previously done using the Capacity page's Location view are now options within the Edit Pod workflows. As an example, to specify a new location name, use the \textbf{Edit} action on a pod and you can specify a new location name as an option of that Edit Pod workflow. Please note that the previous Location view's workflow for removing saved Microsoft Azure subscription information when all of that subscription's associated pods have been deleted is no longer available.

- The product name formerly known as VMware Identity Manager is now named VMware Workspace ONE™ Access.

- The Horizon Agents Installer no longer installs a dormant DaaS agent. In the previous release, the HAI installed the DaaS agent's MSI into the guest operating system, but it was dormant and not used. In this release, the MSI is not installed at all.
September 2019 - v2.1

Use the following information when you have cloud-connected pods dating from before September 2019 and you want to understand any effects on your experience from the features described in the Release Notes What's New September 2019.

Specifically about existing cloud-connected Horizon pods

Starting in this release:

- Automatic update is now supported on Cloud Connector versions 1.3 and 1.4. It is recommended that customers on earlier versions of Cloud Connector update to the latest to take advantage of this feature.

- Cloud Monitoring Services (CMS) with session usage details is provided as part of Horizon Cloud Service.

Specifically about existing pods in Microsoft Azure

For the following new features described in the Release Notes document's September 2019 What’s New section to be used with a previously existing pod, that pod must first be updated to manifest 1600.0 or later to take advantage of the feature, unless otherwise noted.

- The pod architecture has changed in this release. All pods at the September 2019 release's manifest version have a pod Microsoft Azure load balancer and a Microsoft Azure Database for PostgreSQL server instance (Gen 5 Memory optimized tier). This means that before you update your existing pods to this release’s manifest version, you must ensure that your existing networking configuration meets the DNS, ports, and protocols required to accommodate the pod Microsoft Azure load balancer and Microsoft Azure Database for PostgreSQL server instance. If you have firewalls or network security groups that block specific ports and protocols, compare your current networking configuration to the information in the following topics and update your networking configuration accordingly.
  - DNS Requirements for a Horizon Cloud Pod in Microsoft Azure
  - Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release’s Manifest Level

- Enhanced alerting for pod update errors that require customer actions to resolve them is provided in this release. Some things that are completely within your control can prevent a successful pod update, such as not having enough cores in the pod’s associated subscription to create the jump box VM which orchestrates the pod update. Starting in this release, such items are identified in the console, so that you can address and clear those items.

- Starting in this release, you can revise the following gateway-related settings on an already deployed pod: add two-factor authentication settings to a gateway that does not have them, edit a gateway's two-factor authentication settings, change the gateway’s session brokering timeout setting. In previous releases, you had to configure RADIUS two-factor authentication when the pod was first deployed, and could not change those
settings afterwards. Also new in this release, you can delete gateways from an already deployed pod and you can deploy a new pod to have an external gateway without a public IP address on its Azure load balancer and instead have a private IP address on that load balancer.

- Support for defining Microsoft Azure resource tags when creating a new dedicated or floating VDI desktop assignment or a new farm for Horizon Cloud on Microsoft Azure.

- High availability is now available. To support high availability for pods in Microsoft Azure, the pod architecture is updated to use the Microsoft Azure Database for PostgreSQL service (Updated Gen 5 Memory optimized tier), a Microsoft Azure load balancer, and an availability set. For a pod that is newly deployed in this release, you have the option to enable high availability for that pod at deployment time, or enable high availability later on. For pods that existed prior to this release, before you can enable those pods for high availability, you must first update them to the 1600.0 manifest or later and also update the agents in the pods' images, farms, and VDI desktop assignments to this release level. When the pod update and agent updates are completed, then you can enable high availability on the pod by editing the pod from its pod details page in the Administration Console. This new feature brings additional requirements for enabling the Microsoft.SQL service endpoint on the pod's management subnet when your pod uses subnets that you create yourself, and for allowing outbound access for port 5432.

At the September 2019 time, this High Availability (HA) feature for pods in Microsoft Azure is only supported for pods deployed in the Microsoft Azure Commercial regions (standard global regions). The pod HA feature is not currently supported for pods deployed in Microsoft Azure China, Microsoft Azure Germany, and Microsoft Azure Government (US Gov Virginia, US Gov Arizona, US Gov Texas). The VMware team is working on adding support for the HA feature for pods in those above listed cloud environments. If you have an existing pod in Microsoft Azure in China, Microsoft Azure Germany, or Microsoft Azure Government that you want to update to this release's manifest version without HA, please contact your VMware representative for assistance.

Before updating an existing pod in one of the standard Microsoft Azure global regions to manifest 1600 or later, because the new pod architecture uses the Microsoft Azure Database for PostgreSQL service, you must ensure the following items are in place:

- If the pod is using a custom management subnet, you must add the Microsoft.SQL service endpoint to that management subnet prior to the pod update process. See the steps in When Using Existing Subnets for a Horizon Cloud Pod in Microsoft Azure.

- You must ensure your firewall rules and network security groups allow pod communication to the Microsoft Azure PostgreSQL database server over the management subnet. See the entry for TCP port 5432 in DNS Requirements for a Horizon Cloud Pod in Microsoft Azure.

- Ensure the pod's associated subscription includes the resource providers that are listed in Step 8 of Create the Required Service Principal by Creating an Application Registration.
To increase resiliency of the Horizon Agent pairing process, this release brings further evolution of moving the DaaS agent functions into the Horizon Agent. The DaaS agent has now been incorporated into the Horizon Agent. Even though both the automated Import Image workflow and manual installation of the Horizon Agents Installer install the DaaS agent's MSI into the guest operating system as they did in previous releases, starting in this release, the DaaS agent is dormant and not used. However, the service for the DaaS agent still appears in the Windows Services list. Do not start that service or unexpected results can occur.

Moving the DaaS agent functions into the Horizon View agent has changed both the automated Image Import from the Azure Marketplace workflow and the steps for manually building a base VM. Previously, the base VM that resulted from the automated workflow was paired to the cloud at the end of the workflow, while for a manually created VM, you had to manually bootstrap and pair the VM. Now, for base VMs in a pod that is new or updated to this release version, the resulting base VM is listed on the Imported VMs page with an agent status of Not Paired. To pair the VM, you can either:

- Run the **Reset Agent Pairing** action on the VM listed on the Imported VMs page, if you want to pair it with the cloud before customizing it.
- Run the **New Image** action on the VM directly, if the VM has all of the customizations you want and you are ready to publish it. In this case, the New Image workflow will first run the pairing process to make the agent active, and then you can complete the rest of the fields and click **Publish** to publish the image.

With the move of the DaaS agent functions into the Horizon View agent, the Reset Agent Pairing workflow is now available to use on imported VMs, farm server VMs, and desktop VMs in dedicated VDI desktop assignments. In a farm's details or dedicated VDI desktop assignment's details, if you see an error state in the Agent Status column for a farm server VM or desktop VM, you can use the **Reset Agent Pairing** action in the console to repair the pairing state of that VM. (The action is not available for floating VDI desktop assignments.) In the Imported VMs page, you can use the **Reset Agent Pairing** action to initially pair a VM that has not yet been paired, or repair the pairing state for a VM that was previously paired.

The disk encryption feature now uses the newer AzureDiskEncryption v2.2. This newer version enables support of disk encryption for VMs with in-guest proxy set up to talk to the Internet. To take advantage of this new support, update your VMs' agents to version 19.3.0 or later.

Updated guidance to use VM models that have a minimum of two (2) CPUs for your farms and VDI desktop assignments. VMware scale testing has shown that for production environments, using a minimum of 2 CPUs avoids unexpected end-user connection issues. Even though the system does not prevent you from choosing a VM model with a single CPU, you should use such VM models for tests or proof-of-concepts only.
- Usability enhancements to the VM Types and Sizes page.

**Additional items of note for current customers**

- Improved usability and optimization of the Unified Dashboard interactive map view, including more accurate reflection of the pod location and zoom functionality.
- Enhancements in the reports available in the Administration Console’s Reports page. The data in these reports is provided by the Cloud Monitoring Service.
- For cloud-connected Horizon 7 pods, additional details are displayed in a pod’s details page. The pod and Cloud Connector must be at the latest version to see this feature.
- The product name formerly known as VMware User Environment Manager™ is now named VMware Dynamic Environment Manager™.

**Horizon Cloud — Known Limitations**

So that you can have the best success throughout your journey using Horizon Cloud, keep these known limitations in mind.

**Limitations that Apply to All Deployment Types**

- The Web-based administrative console is not supported in the Apple Safari browser. Some user interface features might not work correctly. In a Mac OS, instead of Apple Safari, you can use Chrome or Firefox browsers.
- Every pod associated with your Horizon Cloud customer account and connected to Horizon Cloud must have line of sight to the same set of Active Directory domains and have one-way or two-way trust configured along with that line of sight.
- Your authenticated (logged in) session into the Web-based administrative console will time out after the time setting that is configured in the console’s General Settings page. The default is 30 minutes. If you have at least one cloud-connected pod, you can change the default to a value ranging from 30 minutes to 180 minutes. In most cases, when the configured time is up, the system will automatically explicitly log you out and present a message that you must log back in. However, sometimes the system ends your authenticated session and does not explicitly log you out. When that happens, when performing certain tasks in the console, error messages might be displayed which do not accurately reflect the current state, such as the node deployment wizard fails to validate your subscription entries, values are not displayed in drop-down lists, and the Farms page reports no node is available in which to create a farm and error messages stating "No service_sessions of type identity_node were provided". If you start to see such behavior and you have been using the console for 30 minutes or more, manually log out and then log back in.
- The system retrieves the data for the Utilization, Concurrency, Session History, and Top Applications reports once a day, at a specific UTC time. The data for the Utilization and Concurrency reports is retrieved at 2 AM UTC, the data for the Session History report is retrieved at 2:10 AM UTC, and the data for the Top Applications report is retrieved at 2:30
AM UTC. As a result, the reported information that is displayed in the administrative console might not reflect the data collected between the last retrieval time and the time at which you are viewing the reports in the console. As an example, because the logic for the Users and Peak Concurrency data in the Concurrency report is calculated on the daily basis for which the data is retrieved, the data from user activity on April 23 is calculated at the 2 AM UTC time point on April 24 (the following day). After that time point is passed and the system retrieves the collected data, the data from April 23 gets displayed in the report. If one of your end users starts a session after the 2 AM UTC time point on April 23, data for that user’s session will not be reflected in the on-screen report until after 2 AM UTC on April 24.

Limitations Related to Deployments of Horizon Cloud Pods in Microsoft Azure

- Due to limitations with how Microsoft Azure V Nets handle concurrent subnet creation and deletion operations, running concurrent pod-related operations that require modifying the same V Net at the same time can result in failure to complete those operations. To avoid running into this issue, avoid running pod deployment, pod deletion, or pod edit operations that involve subnets at the same time when those pods are using the same V Net. Here are some examples of concurrent pod-related operations involving modifying the V Net where the chances of experiencing concurrent subnet actions on the V Net can occur, resulting in failures to complete the operations:
  - When you do not create your subnets ahead of time and are having the pod deployer create the subnets using CIDRs, and you initiate creation of two pods concurrently on the same V Net. The subnets are being added to the V Net for both pod creations simultaneously.
  - When one pod is deploying and you initiate deletion of another pod on the same V Net. The subnets are added to the V Net for the deploying pod at the same time the other pod’s subnets are being deleted from the same V Net.
  - When you edit a pod to add an external gateway configuration in the pod’s V Net using CIDR blocks while another pod is in progress of being deleted. The subnets are added to the V Net for the gateway configuration at the same time the other pod’s subnets are being deleted from the V Net.
  - Expanding the size of the pod’s subnets after the pod is deployed is not currently supported. Before you deploy a pod, you must ensure the address spaces for the subnets you specify in the deployment wizard are large enough to accommodate your expected usage. Note:

  **Note** To workaround this limitation, a new feature made available in pods of manifest 2298.0 and later provides for adding tenant subnets for use by your farms and VDI desktops assignments after the pod is deployed. This feature provides for flexibility to add tenant subnets located in the pod’s same V Net or in a peered V Net for use by your farm and desktop VMs after the pod is deployed. For more details, see the Administration Guide.
Multiple pods cannot share the same fully qualified domain name that is set on their Unified Access Gateway configurations. Each pod configured with Unified Access Gateway instances needs its own unique fully qualified domain name (FQDN). The FQDN cannot contain underscores.

**Note** As of the December 15, 2020 cloud plane refresh, having different FQDNs for the pod's external gateway and internal gateway configurations is supported. Prior to December 15, 2020, the system enforced having the same FQDN for a pod of manifest 2298 and later. Now it is your choice if you want the pod's gateways to use different FQDNs or the same FQDN. If you want to use the same FQDN on both gateways, after pod deployment, you would configure Split DNS (Split Domain Name System) to resolve the gateway address either to the external gateway or internal gateway depending on the origin network of the end-user client's DNS query. Then the same FQDN used in the end-user client can route to the external gateway when the client is on the Internet and route to the internal gateway when the client is on your internal network.

The NSX Cloud capabilities in this release are not supported for Microsoft Windows Server 2019.

When you deploy a Horizon Cloud pod in Microsoft Azure after you have already configured True SSO for previously deployed pods, the system does not automatically pair the new pod with the Enrollment servers. You must manually repeat the steps to export the pairing bundle and import it into the Enrollment servers. For the steps, see the topic [Configure True SSO for Use with Your Horizon Cloud Environment](#) and its subtopics.

In workflows that result in the system creating VMs, such as creating farms, images, and assignments, if you try to enter a name that is longer than length supported by the system for the to-be-created item, the system prevents you from typing in more than the supported number of characters. The number of characters supported for an item's name depends on the workflow.

In a Microsoft Azure multi-pod environment, you cannot reuse names that you used in one pod when creating items in another pod. The reason for this limitation is that pods in the multiple-pod environment share the same Active Directory domain and the same VNet. As a result, if names are shared within such multiple-pod environments, unexpected behavior can occur. This limitation applies to names for image, farms, and VDI desktop assignments. Ensure that unique names are used for your images, farms, and VDI desktop assignments.

Follow these rules when entering characters in the administrative console:

- Use only standard ASCII characters in user names and passwords, and for the password when downloading the DaaS SSL bootstrap file. If you use non-ASCII characters for these items, unexpected results might occur.
- When entering names for imported images, farms, assignments, and other assets that result in creating a VM in Microsoft Azure, do not enter more than 12 characters for the name.
- Do not use commas in user passwords.
When using the Import VM wizard to create a base image VM from the Microsoft Azure Marketplace:

- Enter a username and password that adheres to the Microsoft Azure requirements for VM admin usernames and passwords. See the Microsoft Azure FAQ page for details.
- Do not enter a name for the image that ends with a hyphen (-).
- Do not include an underscore character (_) in the image name.

Limitations Related to Updates of Horizon Cloud Pods in Microsoft Azure

- During the process of updating a pod from an earlier software level to the latest one, end users who have connected sessions to the updating node will have those active sessions disconnected. No data loss will occur – except for the case where the RDSH farm or VDI desktop assignment serving the sessions has the Logoff Disconnected Sessions set to Immediately. For such farms and VDI desktop assignments, the disconnected sessions are also logged off immediately and in-progress user work is lost in those conditions. After the update process is complete, those users can reconnect. The pod update process typically takes less than a half hour. However, some pod updates might take longer than that.

- When pods on manifests prior to manifest 2299 are then updated to 2299 or later, if you used the Microsoft Azure Portal to manually add tags directly on resources or resource groups created by Horizon Cloud in your subscription — such as creating custom tags on the farm or VDI desktop assignments’ resource groups — when those pods are then updated to manifest 2299 or later, the pod update process does not preserve those custom tags that you had directly added using the Microsoft Azure Portal. After the pod update on such pods, you must subsequently use the Horizon Cloud Administration Console features to edit the farm and VDI desktop assignment to have the system apply those tags on the resource groups for those farms and VDI desktop assignments. Using the console’s Azure Resource Tags feature is the supported method of adding resource tags on the pod-created resource groups for farms and VDI desktop assignments. In each of the following documentation topics, read the descriptions of Azure Resource Tags fields located in them. The same fields are used when editing a farm or VDI desktop assignment.

- Create a Farm
- Create a Dedicated VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure
- Create a Floating VDI Desktop Assignment Provisioned by a Single Pod in Microsoft Azure
- Horizon Cloud Pods in Microsoft Azure - Create a VDI Multi-Cloud Assignment in Your Horizon Cloud Tenant Environment
Limitations Related to Imported VMs, Golden Images, Farms, or VDI Desktop Assignments in Horizon Cloud Pods in Microsoft Azure

- Use of True SSO with session desktops, remote apps, or VDI desktops based on images running Windows 2004 requires installation of a Microsoft patch on the Windows 2004 operating system to fix a Microsoft issue that was blocking True SSO from authenticating with the Windows 2004 system. For details, see VMware KB 79644 which references Microsoft Update KB4598291.

- Use of the disk encryption feature for farms and VDI desktop assignments is not currently supported for pods in Microsoft Azure Government clouds.

- Currently, use of the following Horizon Agent features is not supported: VMware Logon Monitor service. By default, the Horizon Agents Installer deactivates the VMware Logon Monitor service in all installations that the installer performs.

- The USB redirection capability is not supported when using the VMware Horizon Client for Android to access virtual desktops and remote applications served by your Horizon Cloud environment.

- For GPU-enabled golden images based on server-type operating systems, Microsoft Windows Server versions 2016 and 2019 are recommended to avoid limiting the number of end user sessions. Due to an NVIDIA driver limitation on Windows Server 2012 R2, the maximum number of sessions for each RDS desktop server is 20.

- If you have an image using Microsoft Windows 10 1709 (RS3) and you want to update it to Windows 10 1803 (RS4) or Windows 10 1809 (RS5), first upgrade that Windows 10 1709 to the latest Horizon Agent version 19.4 before proceeding with upgrading the Windows operating system.

- By default, when you use the automated Import Virtual Machine from Marketplace wizard to create an image with a Windows 2012 server operating system, the resulting image does not have the Desktop Experience enabled. If you want the resulting image to have the Desktop Experience, you must manually enable the Desktop Experience in the resulting image.

- If you initiate converting a desktop to an image but cancel before the task finishes, a second attempt to convert the desktop to an image may fail. To avoid this issue, you should power off the desktop and power it on again before attempting to convert it to an image a second time.

- In a URL redirection customization, URL patterns are treated as case sensitive when they are intercepted by the Horizon Client. For example, URL redirection does not occur for URL patterns specified as *GOOGLE.com and *Google.com, even though the pattern *google.com is redirected. Redirection for the end users does not occur if the specified pattern does not match the actual character case used in the target file systems.
Horizon Cloud — Known Issues

This topic lists known issues that you might encounter when using the service and known workarounds, if any.

This documentation topic includes the known issues for Horizon Cloud Connector. However, even though you use the Horizon Cloud Connector to connect Horizon pods to Horizon Cloud, the known issues for the software running inside those Horizon pods are provide elsewhere. The known issues for the software versions of Horizon pods are located in the release notes for the Horizon software product itself. Horizon software version 7.x documents are linked from the VMware Horizon 7 Documentation page. Horizon software version 2006 and later documents are linked from this VMware Horizon Documentation page (sometimes referred to as Horizon 8 in addition to Horizon 2006).

For Image Management Service (IMS) known issues involving IMS features that are available in production for all Horizon Cloud customers, see the known issues page in Management Horizon Images from the Cloud.

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

Login Related Known Issues

Even though you successfully created a password for your My VMware account that contains a backslash (\), logging in to Horizon Cloud using those credentials fails (2595757)

When you use My VMware credentials to login to Horizon Cloud, passwords which contain a backslash are not supported. To see the list of supported special characters, log in to my.vmware.com and navigate to your profile's Change Password section. That page will display the supported special characters. Workaround: Reset your My VMware account password to a new one and ensure the new one does not contain a backslash (\).

Active Directory Related Known Issues

Primary bind account lockout is not detected until you perform an action involving Active Directory in the administrative console. (2010669)

Due to this issue, an administrator logged into the Web-based administrative console will not see a primary bind account lockout notification until an action involving Active Directory is performed in the user interface, such as when searching Active Directory to add users to assignments. The underlying services only detect a locked-out service account when they make a request to talk to Active Directory for either authenticating or searching (user or group). Workaround: None.

It takes up to 15 minutes for the Web-based administrative console to reflect a lockout or unlocked state of the primary bind domain account. (2009434)

The system's connection object to Active Directory is cached for 15 minutes. As a result, it might take 15 minutes from the time point when the primary bind account goes to locked
state and the system raises the notification to the administrator. Conversely, after the administrator clears the locked-out condition of the account, it might take up to 15 minutes for the system to stop notifying about the now-cleared account. Workaround: None.

For farms in a pod in Microsoft Azure, reusing the same farm name with a different domain in the same Active Directory forest can lead to domain join failures due to duplicate service provider names (SPNs). (1969172)

Due to a new feature for domain controllers in Microsoft Windows Server 2012 R2 and higher, a duplicate SPN check on the domain controller causes domain join failures. See the Microsoft KB article 3070083. Workarounds:
- Avoid reusing farm names.
- As described in that Microsoft KB article, turn off duplicate SPN checks in the Active Directory domain.

When using Azure AD Domain Services, the Active Directory registration workflow fails at the domain join step with an error that the Reset Password permission is lacking. (2218180)

The Horizon Cloud team has verified that adding the required domain join account permissions works the same when using Azure Active Directory (AD) Domain Services with your pod as for other Active Directory domain deployments. See the Microsoft documentation topic Create an Organizational Unit (OU) on an Azure AD Domain Services managed domain that describes the built-in container AADDC Computers and see also the Important note at the beginning of that topic about enabling password hash synchronization to Azure AD Domain Services. Before setting the permissions on the domain join service account, it is important that you follow the Microsoft documentation about enabling password hash synchronization to Azure AD Domain Services for the domain join service accounts. If you continue to experience a domain join permissions error in the Register Active Directory workflow after following the Microsoft documentation, please contact VMware support and reference problem report number 2218180.

Cloud Connector Related Known Issues

The no-proxy host configuration specified in the No Proxy For field when deploying the OVF template is not saved to the deployed appliance (2454245, 2466306, 2467017, DPM-5388)

This issue is resolved in Horizon Cloud Connector Version 1.6 or later. When running the Deploy OVF Template workflow in your vSphere environment, you have the option to specify a no-proxy host configuration in the No Proxy For field. However, due to this known issue, the entered settings do not get captured in the deployed appliance's configuration files. As a result, the deployed appliance does not honor the specified no-proxy host setting.

Universal Broker Related Known Issues

The Horizon Universal Broker client on the Horizon Cloud Connector does not consume proxy-related updates that you make in the connector appliance after the appliance is initially deployed (HD-35551)
This issue is resolved in Horizon Cloud Connector Version 1.6 or later. The Horizon Universal Broker client in the connector appliance picks up proxy details during the first-time boot of the appliance. Because the first-time boot runs only during the very first time the appliance is powered on after deploying the OVF template, any subsequent changes to the appliance's proxy configuration settings are not consumed by the Horizon Universal Broker client. Taking this known issue together with the above known issue about the no-proxy configuration during OVF template deployment means that any hosts related to the Horizon Universal Broker cannot be set as non-proxy hosts.

Error message 'Failed to connect to the Connection Server' is displayed when your Horizon Client or Horizon HTML Access in the browser starts to connect to the Universal Broker (2714266)

This issue might occur intermittently for Horizon Cloud pods in Microsoft Azure that are running manifest 2632.x if the pod manager instance was rebooted. Sometimes when the pod manager instance has been rebooted (a rare, atypical situation), after the pod manager instance is powered up and the Universal Broker attempts a connection to the pod, it cannot make an authenticated connection. Workaround: None. If you encounter this situation, open a service request for assistance.

Images, Farms, Assignments Related Known Issues

The known issues listed here apply to pods deployed in Microsoft Azure.

For pods deployed into Microsoft Azure Government cloud subscriptions, using the disk encryption feature in farms and desktop assignments fails. (2572579)

When your pod is located in Microsoft Azure Government clouds and you try to create a farm or VDI assignment with the disk encryption feature selected, the creation process fails with error Azure error encrypting the VM. Workaround: None.

In the Servers tab for an existing farm, all of the User Login Mode choices give an error message that the Horizon Agent must be updated. (2528295)

Use of the administrative console to set the User Login Mode depends on detecting agent version 20.1.0 running in the farm VM. However, that version of the agent might not yet be available in the cloud control plane for you to use to update the agents in your existing farm VMs. Workaround: None. When the 20.1.0 version of the agent is available in the cloud plane and your pods are updated to the manifest version that can consume that agent version, then you can update the farm VMs to that agent to use the User Login mode choices.

Sometimes some desktop VMs out of a large floating VDI desktop assignment report unknown agent status. (DPM-3201)

In floating VDI desktop assignments with large numbers of desktop VMs, due to a known issue, a small number of those desktop VMs can go into an unknown agent state because some Windows services, like the Horizon Agent's Blast service or the Microsoft Azure service, do not start or are slow to start. As a result, in the administrative console, the Agent Status
column for those desktop VMs shows "Unknown" state, with reported agent errors. Workaround: In the console, use the Restart action to restart those VMs.

The Import VM from Marketplace wizard creates Windows Server 2012 images without the Desktop Experience enabled. (2101856)

Due to a known issue, when you use the automated Import VM from Marketplace wizard to create an image with a Windows Server 2012 operating system, the resulting image does not have the Desktop Experience enabled. Workaround: If you want the resulting image to have the Desktop Experience, you must manually enable the Desktop Experience in the resulting image. Note also that for the Windows Server 2012 operating system, to install the Horizon Agent with the Scanner Redirection option requires the Desktop Experience be enabled in the operating system.

When publishing (also known as sealing) an imported VM, the process might result in a timeout or other failures to publish due to sysprep failures. (2036082, 2080101, 2120508, 2118047)

After you click Convert to Desktop on an imported VM and Publish to make it a published (sealed) image, a number of operations are performed on the VM. These operations include running the Windows System Preparation (sysprep) process, shutting down the VM and powering it off, and so on. Due to industry-known issues with the Windows sysprep process and customizing virtual machines, sometimes the publishing process fails for various reasons. On the Activity page, you see messages like "Timeout Error Waited 20 minutes for virtual machine to power off.", and other sysprep failure message.

Generally speaking, you can avoid such sysprep issues when you create the VM using the Import Virtual Machine from Marketplace wizard and select Yes for the wizard's Optimize Windows Image toggle. If you are seeing this error for an imported VM in which you did not use that option, or if you manually created that VM, refer to VMware KB 2079196, Microsoft KB 2769827, Microsoft MVP article 615 for best practices in configuring your image VM to minimize likelihood of having sysprep issues when you go to publish the image. If you continue to get sysprep issues, see the information in the articles Deciding to Optimize the Windows Image When Using the Import Virtual Machine from Marketplace Wizard and Using the Remove Windows Store Apps Option When Using the Import Desktop Wizard for ways that the automated Import VM from Marketplace wizard uses to reduce the changes of sysprep issues. If you see the timeout errors in the Activity page, you can try this workaround: on the Images page, use the Convert Image to Desktop action on the image.

During farm creation, sometimes the server VMs are stuck at the customization step. (2010914, 2041909)

Sometimes during the sysprep process on the farm's server VMs, a Windows service named tiledatamodelsvc prevents sysprep from accessing Windows files that it needs to complete
the sysprep customization process. As a result, the farm’s server VMs do not move past the customization step. The sysprep error log contains the line "Error SYSPRP setupdigetclassdevs failed with error 0". Workaround: If you encounter this issue and see that error message in the sysprep error log file, try stopping and deactivating the tiledatamodelsvcs service in the image. Then create the farm.

Agent status might display as 'undefined' on the Imported VMs page after duplicating an image or manually creating an image in Microsoft Azure. (2002798)

When you use the Duplicate button on the Images page to clone a published image or when you manually create an image VM in Microsoft Azure, the resulting VM is listed on the Imported VMs page. Due to this issue, even when the VM is fully powered-on, the agent status might be displayed as 'undefined'. However, when you select the VM and choose Convert to Image to publish it, the user interface reports the agent in 'Active' state. Workaround: None. If the Reset Agent Pairing or New Image or Convert to Image workflows report the agent as 'Active', you can ignore the 'undefined' status on the Imported VMs page.

App Volumes on Pods in Microsoft Azure Related Known Issues

The known issues listed here apply to pods deployed in Microsoft Azure.

When your environment has multiple pods in Microsoft Azure, the Capture process can sometimes go into an unknown state after the process has completed. (2600573)

When your environment has multiple pods with which you are using App Volumes, sometimes after running the capturing process, the console indicates the capture is in an unknown state even though the capture process on the VM has completed. To work around this issue, re-import the application package using Inventory > Applications > New > Import. As a result, the application package is successfully imported as a separate application and the subsequent assignment and application launch works.

Agent Update Related Known Issues

The known issues listed here apply to pods deployed in Microsoft Azure.

When you attempt an agent update on an image that has a Windows update pending, the update process might fail. (2234964)

If the image needs an update to the Windows OS, as opposed to a minor non-OS update, this can cause OS resources to be offline and not available for the agent update. Workaround: Wait until the Windows update is complete and retry the agent update. To confirm that all Windows updates are complete, you can take the image offline, perform all pending updates, and re-publish the image before initiating the agent update.

Reports and Monitoring Related Known Issues

The known issues listed here apply to pods deployed in Microsoft Azure.

In the User Activity report, the displayed weekly average (hrs) is not intuitive. (1817065)
Due to this issue, the weekly statistics fluctuate along the time because the calculation logic is dividing the current week's duration by seven (7) and not rounding up to a whole week. For example, when you select the last 30 days, the data for completed weeks is unchanged but the data for the current week is divided by seven (7). The current logic is weekly average (hrs) = daily average (hrs) * 7 days, resulting in the last 30 days weekly average = (total duration / 30 days) * 7 days. Workaround: None

The Desktop Health report does not reflect a newly updated farm or VDI desktop assignment name until an hour after the name change. (1756889)

If you change a farm's name or VDI desktop assignment's name, it takes an hour for the Desktop Health report's Assignment drop-down menu and Assignment column to reflect the new name. Workaround: Wait an hour before expecting the new name to appear in the report.

The formatting in some of the CSV files that you can export from the Reports user-interface screens do not match the on-screen tables. (2015500)

Some of the Reports page's subscreens provide an export feature to export the displayed data in CSV format. Due to this issue, the formatting in the CSV files exported from the Desktop Health, Concurrency, and Session History reports do not precisely match the ones you see displayed on the screen. For example, the column headings might be different and the CSV files might have more columns of data than in the on-screen tables. Workaround: None.

Identity Management, Workspace ONE Access, True SSO Related Known Issues

The known issues listed here apply to pods deployed in Microsoft Azure.

When a pod of manifest versions prior to 1763 is updated to manifest 1763 or later, and that pod has two-factor RADIUS configured on its Unified Access Gateway instances and is also integrated with Workspace ONE Access, you see that launching a desktop from Workspace ONE Access using the browser will display the RADIUS login form with the user name field prefilled with the user's UPN. (2248160)

This symptom occurs because of a change that was released in VMware Horizon HTML Access 4.10. When your pod in Microsoft Azure from a previous Horizon Cloud release is configured with Unified Access Gateway instances and two-factor RADIUS authentication and you configure that pod to use Workspace ONE Access, previously when launching a desktop from Workspace ONE Access using the browser, the RADIUS login form prompts for the user name and passcode. The end user would type the user name and passcode in the form. However, due to this issue, after upgrading that pod to this release, using the same desktop launch steps, the RADIUS login form has the user name field prefilled with the domain user's UPN. This behavior only occurs when using the browser to launch the desktop. It does not occur when using Horizon Client. Workaround: If this situation is encountered, the end user can clear the prefilled user name field and enter their information. Generally, for most
environments that are integrated with Workspace ONE Access, the two-factor authentication would be configured in Workspace ONE Access and not on the underlying Unified Access Gateway instances, in which case this issue would not be encountered.

**Launching a second desktop from Workspace ONE Access using the Horizon Client can fail with the error ‘You are not entitled to that desktop or application’. (1813881, 2201599)**

This symptom occurs in the following situation. The user has entitlements to two dedicated VDI assignments through a group entitlement. Both dedicated VDI desktop assignments are listed in Workspace ONE Access when the user logs in. The user launches the first desktop using Horizon Client. That desktop connects. Then the user tries to launch the other desktop from the other assignment, also using the Horizon Client. The launch of that other desktop fails with an error indicating the user is not entitled. However, this issue is seen only for the first attempt on the second desktop. If the user launches the second desktop using the browser, subsequent attempts to launch the second desktop using Horizon Client succeed. Workaround: If you encounter this situation, try launching the second desktop using the browser.

**Workspace ONE Access does not display the remote applications' display names that you set in the Horizon Cloud Administration Console. (2131583)**

This issue is resolved by using Workspace ONE Access Connector version 19.03. Due to a known issue in versions of Workspace ONE Access Connector prior to 19.03, when Workspace ONE Access displays the remote applications that you sync from Horizon Cloud, Workspace ONE Access does not display the display names that you set for those remote applications in Horizon Cloud. Even though Horizon Cloud sends the display names to Workspace ONE Access, Workspace ONE Access uses the remote applications' launchIDs instead. As a result, Workspace ONE Access displays the basic names for the remote applications.

**User Interface Related Known Issues**

Unless otherwise noted in the known issue text, the known issues listed here apply to pods deployed in Microsoft Azure.

**Contents of the Administration Console's Help > About window is not accurate.**

When you click Help > About in the console, the information in the window is not accurate. Due to this issue, the text is hard-coded to always display Version 2.2 instead of stating something accurate and relevant about the tenant environment or about the cloud control plane environment in which you are working. Workaround: None.

**Even though a pod at manifest 2298.0 or later must have at least one gateway configuration for supported operations, the Administration Console does not prevent you from deleting the only gateway configuration from the pod and leaving it in that unsupported state.**

The Administration Console provides a workflow in which you can delete a pod's existing gateway configuration for the purposes of redeploying the gateway with a new deployment configuration. This workflow is provided because at this time, the console does not provide a
way to use the Edit Pod workflow to update the gateway's deployment configuration, even though the Edit Pod workflow can be used to update the gateway's software configuration at any point in time.

Now, a pod at manifest 2298 or later must have at least one gateway configuration to have supported operations. When you delete such a pod's sole gateway configuration for the purposes of updating the gateway's deployment configuration, as described in the previous paragraph, the console displays a warning message. However, the console does not prevent the deletion of the pod's sole deployed gateway, because it is providing for the use case as described in the previous paragraph. The expectation is that you will redeploy the gateway configuration shortly afterwards with new choices for the gateway deployment that the deleted configuration did not have. The issue is that the console currently allows for deleting the sole gateway configuration from a pod on which at least one gateway is required for supported operations, while at the same time the console does not require the redeployment of a new gateway on the pod shortly afterwards. If you leave the pod without a gateway configuration, that pod is in an unsupported configuration.

Workaround: To be in a supported configuration, you must ensure that each pod of manifest 2298.0 or later has at least one gateway configuration. One of the following configurations must be deployed on the pod:

- An external gateway
- An internal gateway
- Both external and internal gateways

If you delete the sole gateway configuration from a pod of manifest 2298.0 or later for the purposes of changing a gateway setting that can only be changed by deleting and redeploying the gateway, you must redeploy a new gateway on the pod to remain in a supported configuration. The VMware Horizon Service Team is working on enhancements that will no longer require the console to provide a workflow to delete a deployed gateway for the use case of changing the gateway deployment configuration. At that time, the ability to delete the sole gateway configuration from the pod using the console will be prevented.

**In the User Card, when you click Reset on a VDI desktop session from a pod in Microsoft Azure, an error message is displayed even though the VM is successfully reset. (2567272)**

Due to this issue, even though the reset operation is initiated successfully and the VM eventually is reset, the Administration Console displays an error message box. The message implies the system was unable to complete your request even though the VM actually gets reset. This issue might be seen for a desktop session from a floating VDI desktop assignment.

Workaround: None. The reset operation is initiated successfully and the VM eventually is reset. Close the error message box that is displayed.

**The Logon Segments chart displayed in the session dashboard has no data.**

This issue applies to all types of pods. The VMware Logon Monitor service provides the data for the Logon Segments chart that appears in the session dashboard. However, this release does not support use of the VMware Logon Monitor service and by default, the Horizon
Agents Installer deactivates the VMware Logon Monitor service in all installations that the installer performs. As a result, even though no data is reported that the Logon Segments chart can display, you see the Logon Segments chart is still visible in the session dashboard. Workaround: None.

When using the administrative console in one browser tab, if you try to launch a disconnected desktop that you have in another browser tab in the same browser, the HTML Access portal is also logged off and you must log back in to the HTML Access portal itself. (2118293)

Usually when you launch a desktop and disconnect from it without logging out of the desktop, you stay logged in to the HTML Access portal itself and you can reconnect to the disconnected desktop without having to enter credentials to the HTML Access portal. Due to this issue, if you are in a browser window where you are logged in to the console in one browser tab and use another browser tab to log in to the HTML Access portal and launch a desktop, when you disconnect from that desktop and try to reconnect to it, the HTML Access portal logs off. Then you must re-enter credentials to the HTML Access portal before you can reconnect to that desktop. Workaround: To avoid this issue, log in to the administrative console using a separate browser window from where you have the HTML Access portal. This behavior only occurs if you are also logged in to the console in a browser tab in the same browser window in which you are also using the HTML Access portal.

In the User Card screen for a specific user, VDI dedicated desktop assignments are removed from the Assignments tab after the user's first launch of the dedicated desktop from that assignment. (1958046)

When a user is specified in a VDI dedicated desktop assignment as an individual user, not through an Active Directory group, that VDI dedicated desktop assignment appears in the Assignments tab in the User Card screen for that user only until the user's first launch of a dedicated desktop from that assignment. After the user's first launch of a VDI dedicated desktop from that assignment, the user card's Assignments tab no longer displays that VDI dedicated desktop assignment for that user. The user's first launch results in that user claiming a specific dedicated desktop from the underlying pool defined by that assignment and the system maps that specific dedicated desktop to that particular user. When that mapping is made, that specific dedicated desktop gets the Assigned state, and it is listed on the user card's Desktops tab for that user.

Workaround: Instead of relying on the user card's Assignments tab in this case, to see the already launched VDI dedicated desktops assigned to a specific user, you can use the Desktops tab. If you need to locate the specific VDI dedicated desktop assignment in which that user-desktop mapping is made, obtain the desktop name from the user card's Desktop tab and use the search by VMs feature of the top banner search to list that specific desktop VM. In the results from the search by VMs, click the name to open the specific assignment page that has that particular dedicated desktop. Then you can locate the user in the assignment's details.

The What's New screen appears even though you previously selected the option not to continue showing it. (2075825)
This issue applies to environments with any pod type. Due to this issue, if you clear your browser cache or you use a different browser than the one in which you previously selected the option to not show the What's New screen, the screen might appear when you log in to the administrative console. The flag for whether to show the What's New screen is stored in the browser's local cache, instead of per user. Workaround: None.

Even though the image creation process has not fully completed, the Getting Started screen displays Completed for the Create Image step. (2100467)

Due to this issue, the Create Image step is marked as completed prematurely. Workaround: Use the Activity page to verify that the image creation process has completed.

When using the administrative console, you might see placeholders instead of the actual text strings or you click a button on a page and nothing happens. (2045967)

This issue applies to environments with any pod type. VMware periodically updates the in-cloud management environment that hosts the Web-based console. This issue can occur when static content has been cached in the browser prior to the latest in-cloud update. It is a temporary issue that will clear when the browser cache is cleared. Workaround: Try logging out of the console, clearing the browser cache, restarting the browser, and then logging back in to the console.

Application names are displayed in lowercase characters when end users access them using Workspace ONE Access. (1967245)

When your Horizon Cloud environment is integrated with Workspace ONE Access, your end users access their assigned desktops and applications using Workspace ONE Access. Due to this know issue, the users see the application names displayed with lowercase characters, regardless of the actual case used in the application names. This limitation is due to the way Workspace ONE Access creates launch IDs from Horizon Cloud by using older Horizon Cloud REST APIs. Workaround: None.

The memory usage percentages reported for desktop health reports and used for the desktop health alerts are based on percentage of committed memory, which equals physical memory plus pagefile size, and not on percentage of only physical memory. (2015772)

Committed memory for a desktop VM is calculated as physical memory plus pagefile size. When calculating the percentage of memory usage in a desktop, the system takes the percentage used of that total (physical memory plus pagefile size). Both the desktop health alerts and the memory usage report in the desktop health reports use that percentage calculation. However, when you log into a desktop VM and open the Windows Task Manager to view the memory usage in the desktop’s Windows operating system, the Windows Task Manager displays percentage based on physical memory only. As a result, the memory usage percentage that the desktop’s Windows Task Manager displays does not match the memory usage percentage displayed in the Desktop Health reports or in the desktop health alert. Workaround: Keep in mind this difference if you decide to make a comparison between the memory usage percentage reported by a desktop’s Windows Task Manager and the memory
usage percentage reported in the console’s Desktop Health report and desktop health alerts
for that desktop.

If a desktop VM’s CPU usage is at or close to 100%, the desktop alert is not triggered.
(1446496)

If an application or something in the desktop VM causes the VM’s CPU usage to reach 100%,
the desktop agent fails to send as many data samples as it usually sends to Horizon Cloud
because the CPU is very busy. As a result of the low sample count returned, the calculation
the system uses to trigger the desktop alert is affected. Workaround: None.

End User, Horizon Agent, Horizon Client Related Known Issues

The known issues listed here apply to pods deployed in Microsoft Azure.

For a VM running Microsoft Windows 10 Enterprise multi-session 2004 or later, the DPI
Synchronization and Display Scaling features have issues (2587685, DPM-6352)

Due to an inability to query the current DPI in VMs running Microsoft Windows 10 Enterprise
multi-session 2004 or later, these features with those VMs do not work as documented in the
Horizon Client documentation. The DPI Synchronization and Display Scaling features do not
work for PCoIP session reconnections. The DPI Scaling feature does not work for Blast
session reconnections. Workaround: Log out of the session and log back in again.

For a VM running Microsoft Windows 10 Enterprise operating system 1903 or later, the DPI
Synchronization and Display Scaling features have issues (2589129)

Due to an inability to query the current DPI in VMs running Microsoft Windows 10 Enterprise
client operating system 1903 or later, when reconnecting a PCoIP or Blast session, the
features do not work as documented in the Horizon Client documentation. Workaround: Log
out of the session and log back in again.

Sometimes when launching a VDI desktop using VMware HTML Access, an error message
about being disconnected appears, and then subsequently the launch is successful. (2243471)

VDI desktop virtual machines have a default session connection timeout, and when that
timeout is reached, the session is disconnected. Sometimes, when launching a desktop, if the
end user's HTML Access session has timed out at the time the desktop's default session
connection timeout is reached, the desktop will initially throw that error, and then continue
launching the desktop. Workaround: None.

When a VDI desktop assignment has disk encryption selected and a one- or two-core VM
model, and a desktop's underlying VM is powered off, the Horizon Client's automatic retry
option might fail to make a connection. (2167432)

When a VDI desktop VM is powered off due to the VDI desktop assignment's power
management settings, the VM has to power on and get ready before an end user connection
can be made to that desktop. When an end user's client tries to connect to a VDI desktop
assignment's VM and the VM is powered off, the system starts powering on that VM. For
non-encrypted VMs, the VM is typically ready to accept a client connection in under 10
minutes. However, an encrypted VM with one or two cores usually takes longer than 10 minutes to get ready to accept a connection. The Horizon Client’s **Client Retry** option has an upper limit of 12 minutes. Because of this upper limit of the **Client Retry** option, when the end user has the client automatically retry the connection while the desktop's underlying VM is getting powered on and ready but the connection is not made within 12 minutes, the client’s automatic retry gives up. Because an encrypted VM usually takes longer than 12 minutes until it is ready to take the client connection, the end user might see that Horizon Client's automatic retry fails to complete the connection to their encrypted desktop VM.

Workaround: When you want to have disk encryption for a VDI desktop assignment, select a VM model that has more than two cores. Otherwise, if your VDI desktop assignment has disk encryption and has a VM model with one or two cores, inform your end users that they might experience this issue with using the **Client Retry** option with these encrypted desktop VMs.

**For a virtual desktop from a dedicated VDI desktop assignment, the shortcut link on the Horizon client's Recent page might not launch the desktop.** (1813881, HD-3686, DPM-1140)

The iOS and Android versions of the Horizon clients have a Recent page which displays links to recently launched desktops. When the user does the initial launch of a dedicated pool virtual desktop, the desktop launches as usual, and the client creates a launch icon on the Recent page. However, when the user disconnects from the desktop and then tries later to launch the desktop from the Recent page, the desktop fails to launch because the launch icon is using a shortened version of the desktop name. Workaround: Launch the desktop from the client’s main page, and not the Recent page.

**Pods at 1976.0 manifest version and farm VMs running agent level 19.4: Users get disconnected after one hour from their desktops or remote application sessions when using HTML Access (Blast) and PCoIP protocols.** (2519400)

This issue is due to an issue in Microsoft terminal services in Microsoft Windows 10 Enterprise multi-session systems. For session-based desktops and remote applications provisioned from RDSH farms based on the Microsoft Windows 10 Enterprise multi-session operating system, when an end user reconnects to an existing desktop or remote application session using either HTML Access (Blast) or PCoIP protocol, after an hour has passed, the user’s session is forcefully disconnected. There is no data loss. Even though the user can reconnect again and the session is in the same state it was at the disconnect time, this behavior repeats and the reconnected session is again forcefully disconnected after an hour.

This issue is resolved using Horizon Agents Installer (HAI) 20.1 or later. When your 1976.0 pod is updated to manifest 1976.1 or later, the Import Virtual Machine from Marketplace wizard will automatically install the agent software that has this fix. If your pod is still at 1976.0 manifest level, running the wizard will still install the agent software with the issue. However, when you seal the VM, the Images page will show the blue dot, signifying that you can use the Update Agent feature to update the agent to the level with the fix.

**Pods at manifest versions earlier than 2298: When switching protocols in the client, if you choose the Connect choice instead of Log Out and Reconnect, the client might become unresponsive.** (2528014)
This issue is resolved in pods that are updated to manifest 2298 or later. This issue happens when switching protocols in the client after establishing a session to an RDSH farm using one protocol. When you launch the desktop or application using one protocol, disconnect that session, use the client’s menu to switch to a different protocol, launch the same desktop or application, the client presents a dialog box saying "This desktop is open on the server but is running a different protocol." and presents a choice to connect or to log out and reconnect. If you select the Connect button, the dialog appears a second time, and if you select Connect again, the client becomes unresponsive.

**When using the Update Agent feature to update images that have an agent version earlier than 18.2.2, the update process might fail (2200962)**

Images that you created on nodes at manifest level earlier than 965 might experience this issue. Sometimes the image has RunOnce registry values that block completion of the agent update process. Workaround: Perform the agent update again, adding the following command line argument on the Command Line tab of the Agent Update wizard:

```
VDM_SUPPRESS_RUNONCE_CHECK=1
```
Introduction to Horizon Cloud and Onboarding Pods to Become Cloud-Connected Pods

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

Horizon Cloud

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

cloud-connected pod

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

- Horizon Cloud pod deployed into your Microsoft Azure subscription by the Horizon Cloud automated pod deployment wizard. This type of pod is called a Horizon Cloud pod because this type's underlying software consists of the pod-manager technology from Horizon Cloud. That software runs in a pod manager instance deployed in your Microsoft Azure subscription.

- Horizon pod installed and running in a VMware software-defined data center (SDDC) that is supported for use with VMware Horizon software. This type of pod is called a Horizon pod because this type's underlying software consists of the Horizon Connection Server software. Types of VMware SDDCs include on-premises vSphere environments and cloud environments such as VMware Cloud on AWS. For the details about the types of VMware SDDCs that are supported for use with the VMware Horizon software used for Horizon pods, see the VMware Horizon documentation that is applicable for the version of the Horizon Connection Server software — Horizon 7 version 7.x, Horizon (2006 and later).
Depending on the type of capacity environment you are using, you can use the cloud-based console for an automated pod deployment and connection to Horizon Cloud. For some of those pod types, even though they cannot be automatically deployed and configured, you can still onboard those pods to Horizon Cloud.

For a high-level overview of the pod-onboarding concept, see Horizon Cloud Deployments and Onboarding Pods — Horizon Pods on VMware SDDCs and Horizon Cloud Pods on Microsoft Azure.

**Control Plane**

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

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

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

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

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

This Horizon Cloud release provides for the following deployment types.

**Note** To connect a pod to Horizon Cloud or use the administrative console for an automated deployment, your customer account must have the appropriate licensing. For licensing information, contact your VMware account representative.
Table 2-1. Pod Deployment Types

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Horizon pod that you have installed and configured in a VMware SDDC</td>
<td>Connect that pod to Horizon Cloud by deploying the Horizon Cloud Connector into the supported VMware SDDC and using the Horizon Cloud Connector configuration portal to configure the pod as a cloud-connected pod.</td>
</tr>
<tr>
<td>(software-defined data center) supported for such use. Such a VMware SDDC</td>
<td></td>
</tr>
<tr>
<td>might be your on-premises vSphere infrastructure or a cloud environment the</td>
<td></td>
</tr>
<tr>
<td>likes of VMware Cloud on AWS, Azure VMware Solution (AVS), and similar</td>
<td></td>
</tr>
<tr>
<td>VMware SDDCs that support VMware Horizon pods.</td>
<td></td>
</tr>
<tr>
<td>Horizon Cloud pod deployed into your Microsoft Azure cloud capacity using the</td>
<td>Deploy the pod using the automated deployment wizard within the Horizon Cloud Administration Console. The automated deployment process both deploys and configures the pod as a cloud-connected pod.</td>
</tr>
<tr>
<td>Horizon Cloud pod deployment wizard.</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

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

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

This chapter includes the following topics:
VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist For New Pod Deployments - Updated As Appropriate for Pods That Deploy Starting From the January 2021 Service Release

VMware Horizon Pods with Horizon Cloud - Requirements Checklist - Updated as Appropriate for Connecting Pods Starting from the January 2021 Service Release

VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist For New Pod Deployments - Updated As Appropriate for Pods That Deploy Starting From the January 2021 Service Release

This checklist will guide you to prepare your Microsoft Azure subscriptions and networks for the deployment of a pod from Horizon Cloud into Microsoft Azure. Ensuring that these requirements are fulfilled as described below will provide both for completing a successful new pod deployment and successfully completing those key tasks that are required to complete after a pod is deployed.

This checklist is primarily for Horizon Cloud customer accounts that have never had a pod deployed from or cloud-connected to their tenant environment prior to the January 2021 service release date. Such environments might be referred to as clean-slate environments or greenfield environments. New pod deployments that happen after the cloud plane binaries and new pod manifest versions are pushed into the cloud plane on the January 2021 quarterly service release date will deploy using the new pod manifest version. The requirements for a successful pod deployment are primarily determined by the pod manifest version. The cloud plane binaries that are in the production cloud plane might also determine requirements for a successful deployment.

Some of the requirements listed below are the ones needed for pod deployment itself. Some requirements are those needed for the key tasks that are performed after pod deployment to get a productive tenant environment, able to provide pod-provisioned desktops and applications to your end users.

Requirements for pod deployment itself

- Horizon Cloud Control Plane Requirements
- Microsoft Azure Subscription Requirements
- Network Requirements
- Ports and Protocols Requirements
- Pod Deployment Workflow

Requirements for a productive environment after pod deployment

- Active Directory Requirements
- Universal Broker Requirements
### DNS Record Requirements

### Horizon Cloud Golden Images, Desktops, and Farms

### Licensing for the Microsoft Windows Operating Systems

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

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

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

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

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

- All cloud-connected pods must have line-of-sight to the same set of Active Directory domains at the time you deploy those pods.
## Horizon Cloud Control Plane Requirements

- Active My VMware account to log in to the Horizon Cloud control plane.

## Microsoft Azure Subscription Requirements

- Valid Microsoft Azure subscription in a supported Microsoft Azure environment (Azure Commercial, Azure China, or Azure Government). If you will be deploying the external Unified Access Gateway in a separate VNet using its own subscription, then you need an additional valid Microsoft Azure subscription in the same Microsoft Azure environment.  

  **Note** Horizon Cloud supports the majority of the Microsoft Azure regions. For the list of Microsoft Azure regions that are not currently supported, see VMware Knowledge Base article Microsoft Azure Regions with Horizon Cloud Service on Microsoft Azure (77121).

- Valid Microsoft Azure administrative privileges in that Microsoft Azure subscription. For additional information, see Get Started with Role-Based Access Control in the Azure portal in the Microsoft documentation.
Minimum Microsoft Azure capacity available for Horizon Cloud infrastructure in addition to the expected desktop and app workload. Note that as long as this capacity is made available, Horizon Cloud will automatically deploy these VMs and no manual installation is required.

- Pod Deployment Engine, also known as the Jump Box (transient) — 1 x Standard_F2
- Pod/Pod Manager with High Availability enabled — 2 x Standard_D4_v3 (if no Standard_D4_v3 in the region, 2 x Standard_D3_v2)
- Pod/Pod Manager without High Availability enabled — 1 x Standard_D4_v3 (if no Standard_D4_v3 in the region, 1 x Standard_D3_v2)
- Microsoft Azure Database for PostgreSQL Service — Generation 5, Memory Optimized, 2 vCores, 10 GB Storage
- External Unified Access Gateway (optional, unless no internal gateway is specified) — 2 x Standard_A4_v2 or 2 x Standard_F8s_v2
- Internal Unified Access Gateway (optional, unless no external gateway is specified) — 2 x Standard_A4_v2 or 2 x Standard_F8s_v2

**Note**

- Starting with the July 2020 service release, in clean-slate environments, new pods are required to deploy with at least one gateway configuration. If your customer account was created prior to the July 2020 release, but you have not yet deployed your first pod, deployment of that first pod will require configuring at least one gateway configuration at the time of pod deployment. As a result, your minimum Microsoft Azure capacity available must accommodate the VMs for one of the gateway configurations, as described in the preceding list.
- If your subscription's region does not provide for the Standard_F8s_v2 VM sizes, the pod deployer wizard does not display that choice in the selector in the Specify Gateways wizard step.
- After pod deployment is finished, your capacity in Microsoft Azure cloud will have to also accommodate the imported VMs, golden images, virtual desktops, and RDSH farms that you create in that pod. When your account is enabled to use the App Volumes features and you use the console's applications capturing workflow, your capacity will have to also accommodate the VMs in the system-generated desktop assignment used for that capturing process. See the **Horizon Cloud Golden Images, Desktops, and Farms** section below.
- When your tenant account is enabled to use the Horizon Infrastructure Monitoring feature and you are planning to enable that feature on the pod after the pod is deployed, your capacity will have to also accommodate at that time the deployment of the Horizon Edge Virtual Appliance. See the **Horizon Infrastructure Monitoring Requirements** section below.

The external Unified Access Gateway can be optionally deployed into its own Microsoft Azure Virtual Network (VNet), either using the same subscription as the pod or using a different subscription. When deploying the external Unified Access Gateway into its own VNet, the following capacity is needed in the subscription into which the external Unified Access Gateway is deployed:

- External Unified Access Gateway Deployment Engine, also known as the Gateway Jump Box (transient) — 1 x Standard_F2
- External Gateway Connector — 1 x Standard_A1_v2
- External Unified Access Gateway — 2 x Standard_A4_v2 or 2 x Standard_F8s_v2.

Service principal and authentication key created for each subscription. For additional details, see **Use a portal to create an Azure Active Directory application and service principal that can access resources.** See also **Create the Required Service Principal Needed by the Horizon Cloud Pod Deployer by Creating an Application Registration.**
Each service principal must be assigned the appropriate role that allows for the actions that Horizon Cloud must perform in the subscription. This role can be the Contributor role or a custom role with the required permitted actions at the subscription level. When you are deploying the external gateway configuration in an existing resource group in a separate subscription, more granular permissions can be set for that subscription's service principal. For additional details about the required role actions, see Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions.

**Important** The role must be assigned directly to the service principal used for Horizon Cloud. The use of a group-based assignment of a role to the service principal — in which the role is assigned to a group and the service principal is a member in that group — is unsupported.

Required resource providers registered in each Microsoft Azure subscription. See step 8.b in Create the Required Service Principal Needed by the Horizon Cloud Pod Deployer by Creating an Application Registration.

Microsoft Azure subscription ID, directory ID, application ID and key identified.

If you will be deploying the external Unified Access Gateway in a separate VNet using its own subscription, and your organization requires use of a resource group controlled by you and not created by the pod deployer, you would use the feature to deploy the external Unified Access Gateway into your own named resource group. Use of that feature requires you to create that resource group in that subscription before you run the pod deployer. You also need to ensure the necessary permissions are in place for the pod deployer to deploy the Unified Access Gateway configuration into that resource group, manage the configuration, and update the Unified Access Gateway software in the standard pod update process. For details about the necessary permissions, see Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions.

### Network Requirements

- Microsoft Azure Virtual Network (VNet) created in desired Microsoft Azure region with applicable address space to cover required subnets. For additional details, see Azure Virtual Network.
  
  When deploying the external Unified Access Gateway into its own VNet separate from the pod's VNet, create that Unified Access Gateway VNet in the same Microsoft Azure region as the pod's VNet with applicable address space to cover required subnets, and peer the two VNets.

- 3 non-overlapping address ranges in CIDR format in the pod's VNet, reserved for subnets.
  - Management subnet — /27 minimum
  - VM subnet - Primary (tenant) — /27 minimum with /24 - /22 preferred, based on the number of desktops and RDS servers
  - DMZ subnet — /28 minimum when Unified Access Gateway is deployed in the pod's VNet (optional)

  Subnets can either be created manually on the VNet or by Horizon Cloud during deployment. If using manually created subnets, no other resources can be attached.

  **Note** For pods deployed new at manifest 2298.0 or later, after the pod is deployed, you can edit the pod to add additional tenant subnets for use with the VMs in your farms and desktop assignments. The additional tenant subnets can be in the same VNet into which the pod is deployed or in a peered VNet. For details, see the Administration Guide.
When deploying the external Unified Access Gateway into its own VNet separate from the pod’s VNet, 3 non-overlapping address ranges in CIDR format in the Unified Access Gateway’s VNet, reserved for subnets.

- Management subnet — /27 minimum
- Back end subnet — /27 minimum with /24 - /22 preferred, based on the number of desktops and RDS servers
- DMZ (front end) subnet — /28 minimum

Subnets can either be created manually on the VNet or by Horizon Cloud during deployment. If using manually created subnets, no other resources can be attached. For this use case, usually the subnets are created manually. In this use case, the back end subnet’s purpose is similar to the purpose of the VM subnet (Primary) described in the preceding table row.

- NTP server or servers available and accessible from the Horizon Cloud pod and Unified Access Gateway instances.

- Configure the VNet (Virtual Network) DNS server, pointing to a valid DNS server that can resolve both internal machine names and external names.

- Outbound Internet access on the VNets you are using for the pod and gateway deployment must resolve and reach specific DNS names using specific ports and protocols. This is required for deployment and ongoing operations. For the list of DNS names and ports, see DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features and Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release’s Manifest or Later.

- Proxy server information if required for outbound internet access on the VNet that is used during deployment and ongoing operations of the Horizon Cloud environment (optional)

- Microsoft Azure VPN/Express Route configured (optional)

- FQDN for external user access, internal user access, or both (Required when deploying a pod with Unified Access Gateway).

**Note** As of the December 15, 2020 cloud plane refresh, having different FQDNs for the pod’s external gateway and internal gateway configurations is supported. Prior to December 15, 2020, the system enforced having the same FQDN for a pod of manifest 2298 and later. Now it is your choice if you want the pod’s gateways to use different FQDNs or the same FQDN. If you want to use the same FQDN on both gateways, after pod deployment, you would configure Split DNS (Split Domain Name System) to resolve the gateway address either to the external gateway or internal gateway depending on the origin network of the end-user client’s DNS query. Then the same FQDN used in the end-user client can route to the external gateway when the client is on the Internet and route to the internal gateway when the client is on your internal network.
Certificate or certificates for Unified Access Gateway in PEM format matching the FQDN (required when deploying a pod with Unified Access Gateway).

**Note** If the certificate or certificates that you supply for this purpose use CRLs (Certificate Revocation Lists) or OCSP (Online Certificate Status Protocol) settings that refer to specific DNS names, then you must ensure outbound Internet access on the VNet to those DNS names is resolvable and reachable. During configuration of your supplied certificate in the Unified Access Gateway gateway configuration, the Unified Access Gateway software will reach out to those DNS names to check the certificate's revocation status. If those DNS names are not reachable, pod deployment will fail during its Connecting phase. These names are highly dependent on the CA that you used to obtain the certificates, and therefore are not in VMware's control.

Two-factor authentication to an on-premises RADIUS authentication server (optional)

- DNS Addresses for Unified Access Gateway to resolve the name of the authentication server
- Routes for Unified Access Gateway to resolve network routing to the authentication server

**Note** After the pod is deployed, when you plan to set the environment to use Universal Broker to broker the desktops to your end users, some additional configuration is needed when you want to skip two-factor authentication for end users on your internal network. The pod’s internal Unified Access Gateway instances route the connection requests to virtual desktops and apps for such internal end users. When you will have an internal gateway configuration on the pod, you plan to set the environment to use Universal Broker, and you want two-factor authentication for your external end users but skip two-factor authentication for your internal end users, then after the pod is deployed, you will want to enter IP ranges for the Universal Broker to use to identify the internal end users from the external end users for the purposes of skipping the two-factor authentication. For details, see the documentation topic Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment and its subtopics.

Ports and Protocols Requirements

- Specific ports and protocols are required for onboarding pods and ongoing operations of your Horizon Cloud environment. See Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release’s Manifest or Later.

Pod Deployment Workflow

The preceding items are the ones needed before you start the pod deployment wizard. After you ensure you have the preceding items, follow the pod deployment steps through step 4 in High-Level Workflow for Adding a Horizon Pod on Microsoft Azure as Your First Pod to Your Horizon Cloud Tenant Environment to deploy your pod.

Then after the pod is successfully deployed, ensure you have the items described in the following section, so that you can complete the remaining key steps in that high-level workflow.

Active Directory Requirements

The following items are needed for the Active Directory registration workflow. For understanding of that workflow, see Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment.
One of the following supported Active Directory configurations:
- On-premises Active Directory Server connected via VPN/Express Route
- Active Directory Server located in Microsoft Azure
- Microsoft Azure Active Directory Domain Services

Supported Microsoft Windows Active Directory Domain Services (AD DS) domain functional levels:
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

All cloud-connected pods in the same Horizon Cloud customer account must have line-of-sight to the same set of Active Directory domains at the time you deploy those pods. This requirement applies not only to additional pods that you subsequently deploy into Microsoft Azure after the first pod, but also to any Horizon pods that are cloud-connected to the same customer account using the Horizon Cloud Connector. You can see the checklist for such Horizon pods at VMware Horizon Pods with Horizon Cloud - Requirements Checklist - Updated as Appropriate for Connecting Pods Starting from the January 2021 Service Release.

Domain bind account

- Active Directory domain bind account (a standard user with read access) that has the following permissions:
  - List Contents
  - Read All Properties
  - Read Permissions
  - Read tokenGroupsGlobalAndUniversal (implied by Read All Properties)

**Note**
- If you are familiar with the VMware Horizon on-premises offering, the above permissions are the same set that are required for the Horizon on-premises offering’s secondary credential accounts, stated in this Horizon on-premises documentation topic.
- Generally speaking, the domain bind accounts should be granted the default out-of-the-box read-access-related permissions typically granted to Authenticated Users in a Microsoft Active Directory deployment. However, if your organization’s AD administrators have chosen to lock down read-access-related permissions for regular users, you must request those AD administrators preserve the Authenticated Users standard defaults for the domain bind accounts you will use for Horizon Cloud.

You should also set the account password to Never Expire to ensure continued access to log in to your Horizon Cloud environment.

For additional details and requirements, see Service Accounts That Horizon Cloud Requires for Its Operations
Auxiliary domain bind account — cannot use the same account as above
- Active Directory domain bind account (a standard user with read access) that has the following permissions:
  - List Contents
  - Read All Properties
  - Read Permissions
  - Read tokenGroupsGlobalAndUniversal (implied by Read All Properties)

**Note**
- If you are familiar with the VMware Horizon on-premises offering, the above permissions are the same set that are required for the Horizon on-premises offering's secondary credential accounts, stated in [this Horizon on-premises documentation topic](#).
- Generally speaking, the domain bind accounts should be granted the default out-of-the-box read-access-related permissions typically granted to Authenticated Users in a Microsoft Active Directory deployment. However, if your organization’s AD administrators have chosen to lock down read-access-related permissions for regular users, you must request those AD administrators preserve the Authenticated Users standard defaults for the domain bind accounts you will use for Horizon Cloud.

You should also set the account password to Never Expire to ensure continued access to log in to your Horizon Cloud environment.

For additional details and requirements, see [Service Accounts That Horizon Cloud Requires for Its Operations](#)
Domain join account

- Active Directory domain join account which can be used by the system to perform Sysprep operations and join computers to the domain, typically a new account (domain join user account)
- Set account password to Never Expire
- This account requires the following Active Directory permissions: Read All Properties, Reset Password, Create Computer Objects, Delete Computer Objects, Write All Properties

**Note** As of pod manifest 2474.0, the required permissions for the domain join account are reduced from the previous set used for manifests prior to 2474 and now include Write All Properties on Descendent Computer objects. Pods running prior manifests still require the previous set of permissions. See [Service Accounts That Horizon Cloud Requires for Its Operations](#) for details.

- This account also requires the Active Directory permission named Write All Properties on all descendant objects of the target Organizational Unit (OU) that you plan to use for farms and VDI desktop assignments.
- For additional details and requirements, see [Service Accounts That Horizon Cloud Requires for Its Operations](#)

**Note**

- The use of white spaces in the account's user name is currently not supported. If name contains a white space, unexpected results will occur in the system operations that rely on that account.
- In Microsoft Active Directory, when you create a new OU, the system might automatically set the Prevent Accidental Deletion attribute which applies a Deny to the Delete All Child Objects permission for the newly created OU and all descendant objects. As a result, if you explicitly assigned the Delete Computer Objects permission to the domain join account, in the case of a newly created OU, Active Directory might have applied an override to that explicitly assigned Delete Computer Objects permission. Because clearing the Prevent Accidental Deletion flag might not automatically clear the Deny that Active Directory applied to the Delete All Child Objects permission, in the case of a newly added OU, you might have to verify and manually clear the Deny permission set for Delete All Child Objects in the OU and all child OUs before using the domain join account in the Horizon Cloud console.
- Prior to manifest 1600.0, this account required the permissions of the system's Super Administrator role. If your tenant environment has any Horizon Cloud pods in Microsoft Azure running manifests older than manifest 1600.0, the domain join account must be in the described Horizon Cloud Administrators group. The system uses this domain join account with all of your tenant's Horizon Cloud pods in Microsoft Azure. When your tenant has existing pods of manifests older than 1600.0, the domain join account must meet this requirement. For details, see [Service Accounts That Horizon Cloud Requires for Its Operations](#).
Auxiliary domain join account (Optional, cannot use the same account as above)
- Active Directory domain join account which can be used by the system to perform Sysprep operations and join computers to the domain, typically a new account (domain join user account)
- Set account password to Never Expire
- This account requires the following Active Directory permissions: Read All Properties, Reset Password, Create Computer Objects, Delete Computer Objects, Write All Properties

**Note** As of pod manifest 2474.0, the required permissions for the domain join account are reduced from the previous set used for manifests prior to 2474 and now include Write All Properties on Descendent Computer objects. Pods running prior manifests still require the previous set of permissions. See Service Accounts That Horizon Cloud Requires for Its Operations for details.

- This account also requires the Active Directory permission named Write All Properties on the all descendant objects of the target Organizational Unit (OU) that you plan to use for farms and VDI virtual desktops.
- For additional details and requirements, see Service Accounts That Horizon Cloud Requires for Its Operations

**Note**
- The use of white spaces in the account's user name is currently not supported. If name contains a white space, unexpected results will occur in the system operations that rely on that account.
- In Microsoft Active Directory, when you create a new OU, the system might automatically set the Prevent Accidental Deletion attribute which applies a Deny to the Delete All Child Objects permission for the newly created OU and all descendant objects. As a result, if you explicitly assigned the Delete Computer Objects permission to the domain join account, in the case of a newly created OU, Active Directory might have applied an override to that explicitly assigned Delete Computer Objects permission. Because clearing the Prevent Accidental Deletion flag might not automatically clear the Deny that Active Directory applied to the Delete All Child Objects permission, in the case of a newly added OU, you might have to verify and manually clear the Deny permission set for Delete All Child Objects in the OU and all child OUs before using the domain join account in the Horizon Cloud console.
- Prior to manifest 1600.0, this account required the permissions of the system's Super Administrator role. If your tenant environment has any Horizon Cloud pods in Microsoft Azure running manifests older than manifest 1600.0, the domain join account must be in the described Horizon Cloud Administrators group. The system uses this domain join account with all of your tenant's Horizon Cloud pods in Microsoft Azure. When your tenant has existing pods of manifests older than 1600.0, the domain join account must meet this requirement. For details, see Service Accounts That Horizon Cloud Requires for Its Operations.
Active Directory groups

- **Horizon Cloud Administrators** — Active Directory security group for Horizon Cloud administrators. Contains the Horizon Cloud administrative users. This group is granted the Super Administrator role in Horizon Cloud.
- **Horizon Cloud Users** — Active Directory security group for the users which will have access to virtual desktops and RDS session-based desktops and published applications in Horizon Cloud.

**Note** If your tenant environment has any Horizon Cloud pods in Microsoft Azure running manifests older than manifest 1600.0, the domain join account and any auxiliary domain join accounts must also be in Horizon Cloud Administrators group — or in an Active Directory group which is granted the Super Administrator role in Horizon Cloud.

Active Directory organizational unit (OU) or units (OUs) for virtual desktops and RDS session-based desktops or published applications or both.

**Note** In Microsoft Active Directory, when you create a new OU, the system might automatically set the Prevent Accidental Deletion attribute which applies a Deny to the Delete All Child Objects permission for the newly created OU and all descendant objects. As a result, if you explicitly assigned the Delete Computer Objects permission to the domain join account, in the case of a newly created OU, Active Directory might have applied an override to that explicitly assigned Delete Computer Objects permission. Because clearing the Prevent Accidental Deletion flag might not automatically clear the Deny that Active Directory applied to the Delete All Child Objects permission, in the case of a newly added OU, you might have to verify and manually clear the Deny permission set for Delete All Child Objects in the OU and all child OUs before using the domain join account in the Horizon Cloud console.

### Universal Broker Requirements

Starting with the July 2020 release, when your Horizon Cloud tenant environment is a brand new account starting from that date and you have just completed deploying your first pod into Microsoft Azure, you can choose to use Universal Broker as the brokering method for your environment. When you choose to configure Universal Broker for your environment, the following items are needed. See Configure Universal Broker.

- Outbound Internet access on the VNets you are using for the pod must resolve and reach specific DNS names using specific ports and protocols. This is required for Universal Broker configuration and ongoing operations. For the list of DNS names and ports, see DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features and Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later.

- Optional: Configure your pod’s gateways for two-factor authentication to a RADIUS authentication server, if you want Universal Broker to use two-factor authentication for the pod.
  - DNS Addresses for Unified Access Gateway to resolve the name of the authentication server
  - Routes for Unified Access Gateway to resolve network routing to the authentication server

- Optional: A custom FQDN that your end users will use to access the Universal Broker service and the certificate based on that FQDN (optional).
DNS Record Requirements

After the pod is deployed into the Microsoft Azure cloud and depending on your business situation and the features you want to leverage, it is important to set up records in your DNS server that map fully qualified domain names (FQDNs) to pod-related IP addresses.

**Note**  If you deployed the pod with the external and internal gateway configurations having the same FQDN, then after pod deployment, configure Split DNS (Split Domain Name System) to resolve the gateway address either to the external gateway or internal gateway depending on the origin network of the end-user client’s DNS query.

- ☐ If you configured Universal Broker with a custom FQDN, create a public DNS record that maps your custom FQDN to the VMware-provided brokering FQDN in your Universal Broker configuration. See Configure Universal Broker.

- ☐ Public DNS record created for external end-user access that matches the FQDN on the external gateway configuration, pointing to the Microsoft Azure external load balancer in the pod’s external Unified Access Gateway configuration (required when the deployed pod has that configuration). For additional details, see Configuring a custom domain name for an Azure cloud service.

- ☐ Internal DNS record created for internal end-user access that matches the FQDN on the internal gateway configuration, pointing to the Microsoft Azure internal load balancer in the pod’s internal Unified Access Gateway configuration (required when the deployed pod has that configuration).

- ☐ Internal DNS record created when you plan to choose single-pod brokering for your deployment and you will be integrating the deployment with VMware Workspace ONE Access. In this scenario, this internal DNS record supports the VMware Workspace ONE Access connections to the pod, in which the VMware Workspace ONE Access Connector synchs the information about user assignments from the pod. This internal DNS record matches the FQDN in the certificate that you will upload to the pod itself and points to the pod manager’s Microsoft Azure internal load balancer. Required when you want to use VMware Workspace ONE Access with a pod in an environment configured for single-pod brokering.

  **Note** This internal DNS record and a certificate that matches and is uploaded to the pod itself are also used in the rare, atypical use case when you would tell internal end users to directly connect to the pod, instead of telling them to connect to an internal Unified Access Gateway configuration on the pod. Such direct connections are an unusual use case. Typically, an internal Unified Access Gateway is used instead.

- ☐ Certificate chain (CA certificate, SSL certificate, SSL key file) that matches the above internal DNS record created for VMware Workspace ONE Access connections to the pod. For additional details, see Upload SSL Certificates to a Horizon Cloud Pod for Direct Connections. (Also required if you are using the atypical use case of having internal end users connect directly to the pod. Direct connections are a rare, unusual usage. Typically an internal Unified Access Gateway is used instead.)
Horizon Cloud Golden Images, Desktops, and Farms

Your Microsoft Azure subscription must accommodate the following requirements depending on the types of golden images, VDI desktops, and RDS farms you want to provision from the deployed pod.

**Note** When your account is enabled to use the App Volumes features and you use the console's **Capture** action to add App Volumes applications to your inventory, the system generates a desktop assignment of two desktop VMs to support that capturing workflow. Your capacity will have to also accommodate creating those desktops while you are performing the capturing workflow. You can delete that desktop assignment when you are finished capturing applications for your environment.

☐ **Base for the golden image** — one of the supported Microsoft Azure VM configurations.
  - Standard_D3_v2, Standard_D4_v3
  - Standard_D2_v2, Standard_D2_v3
  - Standard_NV6

**Note** When using the automated Import VM from Marketplace wizard to create a base VM, the system automatically uses one of the above VM sizes by default. The system’s default choice is based on internal algorithms that including checking what sizes are available in the pod’s Microsoft Azure region. When using the wizard to create a GPU-enabled VM, the Standard_NV6 size VM is created by default. When using the wizard to create a server OS-based VM, a VM of either Standard_D2_v2 or Standard_D2_v3 is created. When creating a client OS-based VM or a Windows 10 multi-session VM, a VM of either Standard_D3_v2 or Standard_D4_v3 is created.

☐ **Model selection for the desktop VMs in VDI desktop assignments** — any of the Microsoft Azure VM configurations available in the Microsoft Azure region, except for those not compatible with Horizon Cloud desktop operations.

For production environments, VMware scale testing recommends using models that have a minimum of 2 CPUs or larger.

☐ **Model selection for the RDSH VMs in farms** — any of the Microsoft Azure VM configurations available in the Microsoft Azure region, except for those not compatible with Horizon Cloud RDS farm operations.

This requirement also applies to a VM running Microsoft Windows 10 Enterprise multi-session when that VM is used with Horizon Cloud. As described in the [Microsoft Windows 10 Enterprise multi-session FAQ](https://kb.vmware.com/kb/70965) in the Microsoft Azure Windows Virtual Desktop documentation, Microsoft Windows 10 Enterprise multi-session is a Remote Desktop Session Host (RDSH) type that allows multiple concurrent interactive sessions, which previously only Microsoft Windows Server operating systems could provide. The Horizon Cloud workflows that apply to RDS servers are applicable to Microsoft Windows 10 Enterprise multi-session.

For production environments, VMware scale testing recommends using models that have a minimum of 2 CPUs or larger.

---

**Licensing for the Microsoft Windows Operating Systems**

The items are related to the Microsoft Windows operating systems in your imported VMs, golden images, RDSH-capable farm VMs, and virtual desktop VMs. For the list of Microsoft Windows operating systems that Horizon Cloud supports, see [VMware Knowledge Base article 78170](https://kb.vmware.com/kb/78170) and [VMware Knowledge Base article 70965](https://kb.vmware.com/kb/70965).
Horizon Cloud does not provide any guest operating system licensing required for use of Microsoft Windows operating systems that you use in the course of using the Horizon Cloud workflows. You, the customer, have the responsibility to have valid and eligible Microsoft licenses that entitle you to create, perform workflows on, and operate the Windows-based desktop VMs and RDSH VMs that you choose to use in your Horizon Cloud tenant environment. The required licensing depends on your intended use.

**Tip**  For information about Microsoft Windows Virtual Desktop licensing for Windows 10 Enterprise multi-session and Windows 7 Enterprise, see the Microsoft Azure documentation topic [Windows Virtual Desktop pricing](#).

| ☐ | Licensing for one or more of the following types: Microsoft Windows 7 Enterprise, Microsoft Windows 10 (client types) |
| ☐ | Licensing for Microsoft Windows 10 Enterprise multi-session |
| ☐ | Licensing for one or more of the following types: Microsoft Windows Server 2012 R2, Microsoft Server 2016, Microsoft Server 2019 |
| ☐ | Microsoft Windows RDS Licensing Servers — for high availability, redundant licensing servers are recommended |
| ☐ | Microsoft RDS User or Device CALs or both |

**Horizon Infrastructure Monitoring Requirements**

If your Horizon Cloud tenant is enabled to use Horizon Infrastructure Monitoring, you can use the Horizon Cloud Administration Console to activate that feature on your choice of pods. When you choose to activate that feature on a pod, the system automatically builds a virtual appliance into the same Microsoft Azure subscription where that pod resides, and configures that appliance to collect the infrastructure data. Before you can activate this monitoring feature, your tenant must be onboarded to VMware Cloud Services. See [Onboard Your Horizon Cloud Tenant to VMware Cloud Services](#) and [Horizon Infrastructure Monitoring and the Pods in Your Horizon Cloud Environment](#).

| ☐ | Onboard your tenant to VMware Cloud Services. |
| ☐ | For each pod on which you will activate the Horizon Infrastructure Monitoring feature, the pod’s Microsoft Azure subscription must accommodate these additional requirements. |
|   | Horizon Edge Virtual Appliance — 1 x Standard_D4_v3 |

**Reference Architecture**

Use the architecture diagrams below for reference.
Figure 2-1. Illustration of the Horizon Cloud Pod Architecture for a Pod with High Availability Enabled and Configured with Both External and Internal Gateway Configurations, the External Gateway Deployed into the Same VNet as the Pod, Three NICs on the External Gateway VMs, Two NICs on the Internal Gateway VMs, and a Public IP Enabled for the External Gateway’s Load Balancer.
Figure 2-2. Illustration of the External Gateway’s Architecture Elements When the External Gateway is Deployed into Its Own VNet, Separate from the Pod’s VNet, with Three NICS, and into a Resource Group Created by the Pod Deployer

Resources

See the following resources for additional information.

- VMware Horizon Cloud Service documentation page, for links to the product guides and release notes
- VMware Unified Access Gateway documentation page
- Quick Start Tutorial for VMware Horizon Cloud on Microsoft Azure
- Microsoft Azure Resource Manager overview (5 minutes)
- Create Microsoft Azure Service Principal using the portal (6 minutes)
- Microsoft Azure Virtual Network (VNet) (5 minutes)
- Microsoft Azure Virtual Network peering (6 minutes)
VMware Horizon Pods with Horizon Cloud - Requirements Checklist - Updated as Appropriate for Connecting Pods Starting from the January 2021 Service Release

Complete the following tasks to prepare your Horizon pod's components for connecting with Horizon Cloud. Ensure that every step is completed as described below to complete a successful deployment.

The sections in this documentation topic are:

- Horizon Cloud Control Plane Requirements
- Active Directory Requirements
- Horizon Pod and Horizon Cloud Connector Requirements
- DNS, Ports, and Protocols Requirements
- Universal Broker Requirements
- Licensing for the Microsoft Windows Operating Systems

This checklist is primarily for Horizon Cloud customer accounts that have never had a pod deployed from or cloud-connected to their tenant environment prior to the January 2021 service release date. Such environments might be referred to as clean-slate environments or greenfield environments.

Some of the requirements listed below are the ones needed for successfully onboarding a Horizon pod to Horizon Cloud. Some requirements are those needed for the key tasks that are performed after onboarding the Horizon pod to get a productive tenant environment, able to provide multi-cloud assignments to your end users.

**Horizon Cloud Control Plane Requirements**

| ☐ | Active My VMware account to log in to the Horizon Cloud control plane. |
| ☐ | Valid Horizon Universal License. For more information, see the [Horizon Universal License page](Link). |

**Active Directory Requirements**

| ☒ | Supported Microsoft Windows Active Directory Domain Services (AD DS) domain functional levels: |
| ☒ | - Microsoft Windows Server 2008 R2 |
| ☒ | - Microsoft Windows Server 2012 R2 |
| ☒ | - Microsoft Windows Server 2016 |

| ☐ | All cloud-connected pods in the same Horizon Cloud customer account must have line-of-sight to the same set of Active Directory domains at the time you deploy those pods. This requirement applies not only to additional Horizon pods that you subsequently cloud connect using the Horizon Cloud Connector after the first pod, but also to pods deployed into Microsoft Azure using the same customer account. You can see the checklist for Microsoft Azure pods at [VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist For New Pod Deployments - Updated As Appropriate for Pods That Deploy Starting From the January 2021 Service Release](Link). |
Domain bind account
- Active Directory domain bind account (a standard user with read access) that has the following permissions:
  - List Contents
  - Read All Properties
  - Read Permissions
  - Read tokenGroupsGlobalAndUniversal (implied by Read All Properties)

Note
- If you are familiar with the VMware Horizon on-premises offering, the above permissions are the same set that is required for the Horizon on-premises offering’s secondary credential accounts, stated in this Horizon on-premises documentation topic.
- Generally speaking, the domain bind accounts should be granted the default out-of-the-box read-access-related permissions typically granted to Authenticated Users in a Microsoft Active Directory deployment. However, if your organization’s AD administrators have chosen to lock down read-access-related permissions for regular users, you must request that those AD administrators preserve the Authenticated Users standard defaults for the domain bind accounts you will use for Horizon Cloud.

You should also set the account password to Never Expire to ensure continued access to log in to your Horizon Cloud environment.
For additional details and requirements, see Service Accounts That Horizon Cloud Requires for Its Operations

Auxiliary domain bind account — cannot use the same account as above
- Active Directory domain bind account (a standard user with read access) that has the following permissions:
  - List Contents
  - Read All Properties
  - Read Permissions
  - Read tokenGroupsGlobalAndUniversal (implied by Read All Properties)

Note
- If you are familiar with the VMware Horizon on-premises offering, the above permissions are the same set that is required for the Horizon on-premises offering’s secondary credential accounts, stated in this Horizon on-premises documentation topic.
- Generally speaking, the domain bind accounts should be granted the default out-of-the-box read-access-related permissions typically granted to Authenticated Users in a Microsoft Active Directory deployment. However, if your organization’s AD administrators have chosen to lock down read-access-related permissions for regular users, you must request that those AD administrators preserve the Authenticated Users standard defaults for the domain bind accounts you will use for Horizon Cloud.

You should also set the account password to Never Expire to ensure continued access to log in to your Horizon Cloud environment.
For additional details and requirements, see Service Accounts That Horizon Cloud Requires for Its Operations
Domain join account

- Active Directory domain join account which can be used by the system to perform Sysprep operations and join computers to the domain, typically a new account (domain join user account)
- Set account password to Never Expire
- This account requires the following Active Directory permissions: List Contents, Read All Properties, Read Permissions, Reset Password, Create Computer Objects, Delete Computer Objects.
- This account also requires the Active Directory permission named Write All Properties on the OU descendant objects of the target Organizational Unit (OU) that you plan to use for farms and VDI desktop assignments which you create using the Horizon Cloud Administration Console.
- For additional details and requirements, see Service Accounts That Horizon Cloud Requires for Its Operations

Note

- The use of white spaces in the domain join account’s logon name is not supported. If the domain join account’s logon name contains a white space, unexpected results will occur in the system operations that rely on that account.
- In Microsoft Active Directory, when you create a new OU, the system might automatically set the Prevent Accidental Deletion attribute which applies a Deny to the Delete All Child Objects permission for the newly created OU and all descendant objects. As a result, if you explicitly assigned the Delete Computer Objects permission to the domain join account, in the case of a newly created OU, Active Directory might have applied an override to that explicitly assigned Delete Computer Objects permission. Because clearing the Prevent Accidental Deletion flag might not automatically clear the Deny that Active Directory applied to the Delete All Child Objects permission, in the case of a newly added OU, you might have to verify and manually clear the Deny permission set for Delete All Child Objects in the OU and all child OUs before using the domain join account in the Horizon Cloud console.
- Prior to manifest 1600.0, this account required the permissions of the system’s Super Administrator role. If your tenant environment has any Horizon Cloud pods in Microsoft Azure running manifests older than manifest 1600.0, the domain join account must be in the described Horizon Cloud Administrators group. The system uses this domain join account with all of your tenant’s Horizon Cloud pods in Microsoft Azure. When your tenant has existing pods of manifests older than 1600.0, the domain join account must meet this requirement. For details, see Service Accounts That Horizon Cloud Requires for Its Operations.
Auxiliary domain join account (Optional, cannot use the same account as above)
- Active Directory domain join account which can be used by the system to perform Sysprep operations and join computers to the domain, typically a new account (domain join user account)
- Set account password to Never Expire
- This account requires the following Active Directory permissions: List Contents, Read All Properties, Read Permissions, Reset Password, Create Computer Objects, Delete Computer Objects.
- This account also requires the Active Directory permission named Write All Properties on the OU descendant objects of the target Organizational Unit (OU) that you plan to use for farms and VDI desktop assignments which you create using the Horizon Cloud Administration Console.
- For additional details and requirements, see Service Accounts That Horizon Cloud Requires for Its Operations

Note
- The use of white spaces in the domain join account's logon name is not supported. If the domain join account's logon name contains a white space, unexpected results will occur in the system operations that rely on that account.
- In Microsoft Active Directory, when you create a new OU, the system might automatically set the Prevent Accidental Deletion attribute which applies a Deny to the Delete All Child Objects permission for the newly created OU and all descendant objects. As a result, if you explicitly assigned the Delete Computer Objects permission to the domain join account, in the case of a newly created OU, Active Directory might have applied an override to that explicitly assigned Delete Computer Objects permission. Because clearing the Prevent Accidental Deletion flag might not automatically clear the Deny that Active Directory applied to the Delete All Child Objects permission, in the case of a newly added OU, you might have to verify and manually clear the Deny permission set for Delete All Child Objects in the OU and all child OUs before using the domain join account in the Horizon Cloud console.
- Prior to manifest 1600.0, this account required the permissions of the system's Super Administrator role. If your tenant environment has any Horizon Cloud pods in Microsoft Azure running manifests older than manifest 1600.0, the domain join account must be in the described Horizon Cloud Administrators group. The system uses this domain join account with all of your tenant's Horizon Cloud pods in Microsoft Azure. When your tenant has existing pods of manifests older than 1600.0, the domain join account must meet this requirement. For details, see Service Accounts That Horizon Cloud Requires for Its Operations.

Active Directory groups
- Horizon Cloud Administrators — Active Directory security group for Horizon Cloud administrators. Contains the Horizon Cloud administrative users and domain join account. This group is granted the Super Administrator role in Horizon Cloud.
- Horizon Cloud Users — Active Directory security group for the users which will have access to virtual desktops and RDS session-based desktops and published applications in Horizon Cloud.

Note If your tenant environment has any Horizon Cloud pods in Microsoft Azure running manifests older than manifest 1600.0, the domain join account and any auxiliary domain join accounts must also be in Horizon Cloud Administrators group — or in an Active Directory group which is granted the Super Administrator role in Horizon Cloud.
Horizon Pod and Horizon Cloud Connector Requirements

☐ Horizon pod running a minimum of version 7.10 or later. To obtain use of the latest cloud services and features with the cloud-connected pod, it must be running the most currently available version of the Horizon pod software.

☐ Horizon Cloud Connector virtual appliance, a minimum of version 1.7 or later. To obtain use of the latest cloud services and features with the cloud-connected pod, it must be running the most current version, Horizon Cloud Connector version 1.9.
- Static IP
- DNS forward and reverse lookup records

☐ Resource requirements for the Horizon Cloud Connector virtual appliance:
- For version 1.7: 8 vCPUs, 8 GB memory (RAM), 40 GB datastore
- For version 1.8:
  - Full Feature profile: 8 vCPUs, 8 GB memory (RAM), 40 GB datastore
  - Basic Feature profile: 4 vCPUs, 6 GB memory (RAM), 40 GB datastore
- For version 1.9:
  - Full Feature profile: 8 vCPUs, 8 GB memory (RAM), 40 GB datastore
  - Basic Feature profile: 4 vCPUs, 6 GB memory (RAM), 40 GB datastore

**Important** Along with reserving capacity for the Horizon management components such as the Connection Server VMs, Unified Access Gateway VMs, and other components, you should plan on reserving capacity for the Horizon Cloud Connector component. The Horizon Cloud Connector is an infrastructure component that is deployed into your Horizon pod environment to connect a Horizon pod to Horizon Cloud for the use cases of using Horizon subscription licenses and cloud-hosted services with that pod.

☐ Active Directory user used in the pod-onboarding process, when pairing the Horizon Cloud Connector with the pod's Connection Server. This Active Directory user must have the pod's predefined Administrators role on the root access group, as displayed in the pod's Horizon Console in Global Administrators View > Role Permissions > Administrators. In other words, the Active Directory user specified for the pod-onboarding process is a super user for that pod, as described in the Horizon documentation's Horizon Administration guide or Horizon Console Administration guide that is applicable for your pod's software version.

DNS, Ports, and Protocols Requirements

☐ Specific ports and protocols are required both for onboarding a Horizon pod to Horizon Cloud and for ongoing operations of the pod, the Horizon Cloud Connector paired with that pod, and your Horizon Cloud tenant environment. See DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod.

Universal Broker Requirements

After you complete onboarding your first pod, you can set up use of Universal Broker as the brokering method for your Horizon Cloud environment. When you choose to configure Universal Broker for your environment, at a high-level, the following items are needed. For additional specifics, Configure Universal Broker and System Requirements for Universal Broker.
To use Universal Broker with a cloud-connected Horizon pod, the pod must have Unified Access Gateway configured.

Universal Broker has specific DNS, port, and protocol requirements to work with participating Horizon pods. See [Horizon Pods - Port and Protocol Requirements for Universal Broker](#).

Optional: Configure your pod’s gateways for two-factor authentication to a RADIUS authentication server, if you want Universal Broker to use two-factor authentication for the pod.
- DNS Addresses for Unified Access Gateway to resolve the name of the authentication server
- Routes for Unified Access Gateway to resolve network routing to the authentication server

Optional: A custom FQDN that your end users will use to access the Universal Broker service and the certificate based on that FQDN (optional)

---

## Licensing for the Microsoft Windows Operating Systems

Horizon Cloud does not provide any guest operating system licensing required for use of Microsoft Windows operating systems that you use in the course of using the Horizon Cloud workflows. You, the customer, have the responsibility to have valid and eligible Microsoft licenses that entitle you to create, perform workflows on, and operate the Windows-based desktop VMs and RDSH VMs that you choose to use in your Horizon Cloud tenant environment. The required licensing depends on your intended use.

- Licensing for one or more of the following types: Microsoft Windows 7, Microsoft Windows 10
- Licensing for one or more of the following types: Microsoft Windows Server 2012 R2, Microsoft Server 2016, Microsoft Server 2019
- Microsoft Windows RDS Licensing Servers — for high availability, redundant licensing servers are recommended
- Microsoft RDS User or Device CALs or both
Onboarding Your Very First Cloud-Connected Pod to Your Horizon Cloud Tenant Environment

You use the topics in this guide when you are starting your journey with VMware Horizon® Cloud Service™ from the very beginning. At the start of this journey, your Horizon Cloud tenant environment starts fresh, without any cloud-connected pods. The first step is to onboard a pod into that fresh environment. That pod will be your very first cloud-connected pod. The topics that follow this one describe how you get that first cloud-connected pod of any one of the pod types currently supported for Horizon Cloud.

For a high-level description of the process of obtaining a Horizon Cloud tenant environment and how it relates to onboarding a pod, see Horizon Cloud Deployments and Onboarding Pods — Horizon Pods on VMware SDDCs and Horizon Cloud Pods on Microsoft Azure.

The following screenshot is a representative example of what a brand new fresh Horizon Cloud environment looks like when you log in to your account for the first time.
That first-time screen is oriented around the following concepts:

- Connecting a Horizon pod on VMware SDDC to your Horizon Cloud tenant environment. As described in Deployments and Onboarding to Horizon Cloud, this pod type is constructed based on VMware Horizon product software, and which includes Horizon Connection Server software components. Such Horizon pods are those located in your VMware-supported SDDC, whether in an on-premises vSphere infrastructure or in a cloud-based VMware SDDC (software defined data center) environment.

- Automated pod deployment of a Horizon Cloud pod on Microsoft Azure. As described in Deployments and Onboarding to Horizon Cloud and When Adding a Horizon Pod on Microsoft Azure as Your Very First Pod in Your Horizon Cloud Pod Fleet, this pod type is based on pod-manager technology. Such pods are deployed into your Microsoft Azure subscription using an automated pod deployment wizard.

<table>
<thead>
<tr>
<th>On-screen paths</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware SDDC &gt; Add &gt; Download</td>
<td>Use this choice when you want your first cloud-connected pod to be an existing Horizon pod that is deployed in a supported VMware SDDC. Clicking Add &gt; Download in the user interface will take you to the my.vmware.com download page where you download the Horizon Cloud Connector component. Follow the steps in High-Level Workflow When You are Onboarding an Existing Horizon Pod That is Deployed in a VMware SDDC as Your First Pod to Your Horizon Cloud Tenant Environment.</td>
</tr>
<tr>
<td>Microsoft Azure &gt; Manage &gt; Add Pod</td>
<td>Use this choice when you want your first cloud-connected pod to be the type that is based on the pod-manager technology and which is created by the wizard-driven, automatic deployment of a pod into Microsoft Azure. When that process is completed, that pod is your first cloud-connected pod. If you are interested in this type for your first cloud-connected pod, learn how to proceed from the topic When Adding a Horizon Pod on Microsoft Azure as Your Very First Pod in Your Horizon Cloud Pod Fleet and its subtopics.</td>
</tr>
</tbody>
</table>
After your first pod is onboarded to your tenant environment, you then use the companion *Horizon Cloud Administration Guide* to read about how to complete the Active Directory domain registration workflow with that first cloud-connected pod. After the domain registration is completed, you continue using that companion *Horizon Cloud Administration Guide* to learn about all of the workflows you can do with Horizon Cloud, including adding additional pods. In that guide, begin with the Introduction to Horizon Cloud topic, the Getting Started Using Your Horizon Cloud Environment, and their subtopics.

**Note**

- To connect a Horizon pod on VMware SDDC to Horizon Cloud, you use the **VMware SDDC > Add > Download** workflow. If that is the first pod workflow you complete, then that pod would become your first cloud-connected pod. Before starting the steps described in this document, read the VMware Horizon Pods with Horizon Cloud - Requirements Checklist - Updated as Appropriate for Connecting Pods Starting from the January 2021 Service Release. That checklist gives a nice overview of the various prerequisite elements needed to have success with that pod type.

- To deploy a pod-manager-based pod, you use the **Microsoft Azure > Manage > Add Pod** workflow. Before starting that workflow, read the VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist For New Pod Deployments - Updated As Appropriate for Pods That Deploy Starting From the January 2021 Service Release. That checklist gives a nice overview of the various prerequisite elements needed to have success with that pod type.

This chapter includes the following topics:

- **When Onboarding a Horizon Pod to Use Horizon Subscription Licenses or Cloud-Hosted Services with That Pod**

- **When Adding a Horizon Pod on Microsoft Azure as Your Very First Pod in Your Horizon Cloud Pod Fleet**

**When Onboarding a Horizon Pod to Use Horizon Subscription Licenses or Cloud-Hosted Services with That Pod**

You onboard Horizon pods to your Horizon Cloud tenant environment for two primary use cases: to apply a subscription license with your Horizon pod and to use cloud-hosted services with it. Such cloud-hosted services include features and workflows for your cloud-connected pods. Both use cases require use of the VMware Horizon® Cloud Connector™, the component that connects your Horizon deployment with the Horizon Cloud cloud-based management plane. That connection provides both for applying the subscription license to your Horizon deployment and for enabling cloud-hosted services, such as the Cloud Monitoring Service (CMS).
For a high-level description of the process of first-time onboarding any of the supported pod types to the cloud control plane, see *Horizon Cloud Deployments and Onboarding Pods — Horizon Pods on VMware SDDCs and Horizon Cloud Pods on Microsoft Azure*.

**Important**  Your Horizon Cloud environment can consist of pods in Microsoft Azure and Horizon pods. As a result, all those cloud-connected pods must have line of sight to the same set of Active Directory domains. If your environment already has pods in Microsoft Azure and you are connecting your first Horizon pod, you must ensure that the Horizon pod will be able to have line of sight to the Active Directory domains that are already registered with your Horizon Cloud environment at the time you connect the Horizon pod. For details about the Active Directory domain registration workflow, see *Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment*.

### Activating Subscription Licenses and Enabling Cloud-Hosted Services for Horizon Pods Using the Horizon Cloud Connector

The Horizon Cloud Connector is a virtual appliance that bridges a Horizon pod with Horizon Cloud. Horizon Cloud Connector is required for using cloud-hosted services with your Horizon pod including Horizon subscription licenses, health status dashboard, and Horizon Help Desk Tool.

**Horizon subscription licenses**  Horizon subscription licenses are available with the standalone Horizon package and as part of the Workspace ONE Enterprise bundle. The Horizon subscription license provides the same product with more flexible deployment options. Horizon subscription licenses enable Horizon deployment in the data center, private cloud, and supported public clouds such as VMware Cloud on AWS. When you have completed the steps using the Horizon Cloud
Connector to onboard your pod to Horizon Cloud, VMware activates your subscription license. Within 48 hours, the License Service applies the license to that cloud-connected pod, and a message is displayed in the Horizon administration’s licensing screen:

![License Key](image)

You must have an active My VMware account to purchase a Horizon license from [https://my.vmware.com](https://my.vmware.com). You then receive a Welcome email with the link to download the Horizon Cloud Connector as an OVA file.

When you deploy the Horizon Cloud Connector virtual appliance from vSphere Web Client, you pair the Cloud Connector with the Connection Server of the pod you want to connect to Horizon Cloud to use subscription licenses or cloud-hosted services. As part of the pairing process, the Horizon Cloud Connector virtual appliance connects the Connection Server to Horizon Cloud to manage the Horizon subscription license and other services. With a Horizon subscription license, you do not need to manually enter a Horizon license key for the VMware Horizon product activation. However, you do need to use the license keys to activate supporting components such as vSphere, App Volumes, and others.

**Cloud-hosted services for Horizon pods**

If you select the default **Full Feature** option when deploying the Horizon Cloud Connector, you can leverage those cloud-hosted services, features, and workflows that Horizon Cloud provides, such as the Cloud Monitoring Service (CMS). See [Introducing the Cloud Monitoring Service’s Unified Visibility, Health Monitoring, and Help Desk Features Provided in Horizon Cloud](https://your-link-here).

**High-Level Workflow When You are Onboarding an Existing Horizon Pod That is Deployed in a VMware SDDC as Your First Pod to Your Horizon Cloud Tenant Environment**

This list is a high level of the steps when you are onboarding your very first pod to your Horizon Cloud tenant environment and that pod is an existing Horizon pod that you have already stood up in a supported VMware SDDC (software-defined data center) environment. Such a manually deployed pod is one that you manually installed and configured in the VMware SDDC. After these onboarding steps are completed for your very first cloud-connected pod, the subscription license is applied to that onboarded pod. Additionally, if you selected the **Full Feature** option when deploying Horizon Cloud Connector, you can start using the cloud-hosted services that Horizon Cloud provides for that pod type, which include the Cloud Monitoring Service (CMS). At that point, you can also onboard additional pods.
The following diagram illustrates the overall flow.

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

- See the VMware Horizon software installation information according to the software edition that is running on the pod that you are going to connect to the cloud plane — Horizon 7 Documentation page or Horizon Documentation page.
- When manually installing Horizon pods using VMware Cloud on AWS capacity, start with the best practices guide for deploying Horizon pods on VMware Cloud on AWS, available from the Horizon on VMware Cloud on AWS product page.
- For installing Horizon pods on Azure VMware Solution (AVS), start with Tech Zone’s Horizon on Azure VMware Solution Architecture and Horizon on Azure VMware Solution Configuration.

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

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

1. Fulfill the prerequisites, which include obtaining a Horizon subscription license, such as the Horizon universal license. See VMware Horizon Pods with Horizon Cloud - Requirements Checklist - Updated as Appropriate for Connecting Pods Starting from the January 2021 Service Release as well as the prerequisites section in Connect Horizon Cloud Service with an Existing Horizon Pod to Use Horizon Subscription Licenses or Cloud-Hosted Services or Both.

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

3. If your environment requires use of a proxy server for the Horizon Cloud Connector virtual appliance to reach the Internet, obtain the required proxy settings so that you can specify them when you deploy the appliance into your pod's environment.

4. Optionally log in to the Horizon Cloud tenant portal and configure additional administrators for your tenant environment.

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

6. After the virtual appliance is powered up, enable SSH access to the virtual appliance to remotely run commands in the appliance's operating system. Follow the steps in **Enable SSH Access to the Horizon Cloud Connector Before Pairing It with Your Horizon Connection Server**.

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

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

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

9. Verify the health of the pod's system components and services by opening an SSH session to the Horizon Cloud Connector virtual appliance and running the `precheck.sh` diagnostics script. See **Verify the Horizon Pod and Virtual Appliance Are Ready to Be Paired** for more details.

10. Using either a mapped FQDN or the virtual appliance's IP address, log in to the browser-based Horizon Cloud Connector configuration portal and complete the onboarding steps that pair the connector with the pod's Connection Server. Follow the steps described in **Complete Pairing the Horizon Pod with Horizon Cloud Using the Horizon Cloud Connector Configuration Portal**.

**Tip** When the connector and Connection Server are successfully paired, the Horizon Cloud Connector configuration portal will display a Congratulations message. At this point, VMware will activate your subscription license. The activation is typically completed after 30 minutes but can take up to 4 hours in some cases. When the license is activated, you will see the message **Connected to License Service** in your pod's web-based console's **Product Licensing & Usage** screen.
Depending on your team standard practices and environment, optionally configure the Horizon Cloud Connector virtual appliance in areas such as configuring a CA-signed certificate and setting a password expiry for the appliance's root user. See the topic.

Register your Active Directory domain with the deployed pod, which includes providing the names of service accounts. Ensure these service accounts meet the requirements described in Service Accounts That Horizon Cloud Requires for its Operations.

Tip: Completing the Active Directory domain registration workflow enables you to take advantage of all the cloud-hosted services, such as the Cloud Monitoring Service (CMS). Until the pod's Active directory domain is registered with your tenant environment, the areas of the console involving those features are inaccessible.

In the rare, atypical situation where your tenant environment already has Horizon Cloud pods in Microsoft Azure that are running manifests older than manifest 1600.0, you must give the Horizon Cloud Super Administrators role to an Active Directory group that includes the domain join account as a member. See the topic Assign Horizon Cloud Administrative Roles to Active Directory Groups in the Administration Guide.

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 Administration Guide.

DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod

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

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

Connectivity and DNS Requirements

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

**Important** Keep in mind the following important points:

- For all tenant accounts, reachability to DNS name cloud.horizon.vmware.com is required. Reachability to cloud.horizon.vmware.com is required in addition to reachability to the regional control plane DNS name for the region specified in your tenant account.
- Horizon Cloud Connector uses SSL certificates signed by DigiCert, an industry-trusted certificate authority (CA). These certificates use CRL (Certificate Revocation Lists) and OCSP (Online Certificate Status Protocol) queries that refer to specific DNS names on the DigiCert domain. To ensure Horizon Cloud Connector connectivity, you must configure these DNS names to be resolvable and reachable by the virtual appliance. If these DNS names are not reachable, you will not be able to access the Horizon Cloud Connector configuration portal. The specific names are determined by DigiCert, and therefore are not in VMware's control.
- When you are going to enable use of Universal Broker with the pod, there are connectivity requirements in addition to the DNS names. For details, see System Requirements for Universal Broker and its related topics.

Your Welcome to Horizon Service email will indicate which regional control plane instance your tenant account was created in. Due to a known issue that existed when the welcome email was sent to you, the email you received might display the system string names used for the regions instead of human-friendly names. If you see a system string name in your welcome email, you can use the following table to relate what is shown in your email with the regional control plane DNS names.

Table 3-1. Regions in Your Welcome Email Mapped to Regional Control Plane DNS Names

<table>
<thead>
<tr>
<th>Your welcome email says</th>
<th>Regional DNS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>cloud.horizon.vmware.com</td>
</tr>
<tr>
<td>EU_CENTRAL_1 Or Europe</td>
<td>cloud-eu-central-1.horizon.vmware.com</td>
</tr>
<tr>
<td>AP_SOUTHEAST_2 Or Australia</td>
<td>cloud-ap-southeast-2.horizon.vmware.com</td>
</tr>
<tr>
<td>PROD1_NORTHCENTRALUS2_CPI Or USA-2</td>
<td>cloud-us-2.horizon.vmware.com</td>
</tr>
<tr>
<td>PROD1_NORTHEUROPE_CPI Or Europe-2</td>
<td>cloud-eu-2.horizon.vmware.com</td>
</tr>
<tr>
<td>PROD1_AUSTRALIAEAST_CPI Or Australia-2</td>
<td>cloud-ap-2.horizon.vmware.com</td>
</tr>
<tr>
<td>Japan</td>
<td>cloud-jp.horizon.vmware.com</td>
</tr>
<tr>
<td>UK</td>
<td>cloud-uk.horizon.vmware.com</td>
</tr>
<tr>
<td>Source</td>
<td>Destination (DNS name)</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Horizon Cloud Connector</td>
<td>cloud.horizon.vmware.com plus one of the following names, depending on which</td>
</tr>
<tr>
<td></td>
<td>regional control plane instance is specified in your Horizon Cloud tenant account.</td>
</tr>
<tr>
<td></td>
<td>The regional instance is set when the account is created, as described in Deployments</td>
</tr>
<tr>
<td></td>
<td>and Onboarding to Horizon Cloud for Microsoft Azure and Horizon Pods.</td>
</tr>
<tr>
<td></td>
<td>- cloud-us-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-eu-central-1.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-eu-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-ap-southeast-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-ap-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-jp.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-uk.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> In addition to the regional instance as stated below, reachability to</td>
</tr>
<tr>
<td></td>
<td>cloud.horizon.vmware.com is required by Horizon Cloud Connector for all tenant</td>
</tr>
<tr>
<td></td>
<td>accounts.</td>
</tr>
<tr>
<td></td>
<td>- United States: cloud.horizon.vmware.com, cloud-us-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- Europe: cloud-eu-central-1.horizon.vmware.com, cloud-eu-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- Asia Pacific: cloud-ap-southeast-2.horizon.vmware.com, cloud-ap-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- Japan: cloud-jp.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- United Kingdom: cloud-uk.horizon.vmware.com</td>
</tr>
<tr>
<td>Horizon Cloud Connector</td>
<td>Depending on which regional control plane is specified in your Horizon Cloud account:</td>
</tr>
<tr>
<td></td>
<td>North America:</td>
</tr>
<tr>
<td></td>
<td>- kinesis.us-east-1.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>- query-prod-us-east-1.cms.vmware.com</td>
</tr>
<tr>
<td></td>
<td>Europe:</td>
</tr>
<tr>
<td></td>
<td>- kinesis.eu-central-1.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>- query-prod-eu-central-1.cms.vmware.com</td>
</tr>
<tr>
<td>Source</td>
<td>Destination (DNS name)</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Australia:</td>
<td>kinesis.ap-southeast-2.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>query-prod-ap-southeast-2.cms.vmware.com</td>
</tr>
<tr>
<td>Japan:</td>
<td>kinesis.ap-northeast-1.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>query-prod-ap-northeast-1.cms.vmware.com</td>
</tr>
<tr>
<td>United Kingdom:</td>
<td>kinesis.eu-west-2.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>query-prod-eu-west-2.cms.vmware.com</td>
</tr>
<tr>
<td>Source</td>
<td>Destination (DNS name)</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Horizon Cloud Connector</td>
<td>*.digicert.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>If your organization discourages the use of wildcards in allowable DNS names, you can allow specific names instead. For example, at the time of this writing, the specific DNS names required for certificate validation are:</td>
</tr>
<tr>
<td></td>
<td>ocsp.digicert.com</td>
</tr>
<tr>
<td></td>
<td>crl3.digicert.com</td>
</tr>
<tr>
<td></td>
<td>crl4.digicert.com</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.digicert.com/CPS">www.digicert.com/CPS</a></td>
</tr>
<tr>
<td></td>
<td>These DNS names are determined by DigiCert and subject to change. For instructions on how to obtain the specific names required by your certificates, refer to VMware Knowledge Base (KB) article 79859.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Horizon Cloud Connector</td>
<td>One of the following names, depending on which regional control plane instance is specified in your Horizon Cloud tenant account. The regional instance is set when the account is created, as described in Deployments and Onboarding to Horizon Cloud for Microsoft Azure and Horizon Pods.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>connector-azure-us.vmwarehorizon.com</td>
</tr>
<tr>
<td></td>
<td>connector-azure-eu.vmwarehorizon.com</td>
</tr>
<tr>
<td></td>
<td>connector-azure-aus.vmwarehorizon.com</td>
</tr>
<tr>
<td></td>
<td>connector-azure-jp.vmwarehorizon.com</td>
</tr>
<tr>
<td></td>
<td>connector-azure-uk.vmwarehorizon.com</td>
</tr>
</tbody>
</table>
Ports and Protocols Required by the Horizon Cloud Connector Virtual Appliance

For ongoing operations between Horizon Cloud Connector and Horizon Cloud, the ports and protocols in the following table are required.

Table 3-2. Horizon Cloud Connector Ports

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Cloud Connector</td>
<td>Horizon Cloud</td>
<td>443</td>
<td>HTTPS</td>
<td>Used to pair the Horizon Cloud Connector with Horizon Cloud and transfer data.</td>
</tr>
<tr>
<td>Horizon Cloud Connector</td>
<td>Connection Server</td>
<td>443</td>
<td>HTTPS</td>
<td>API calls to Connection Server.</td>
</tr>
<tr>
<td>Horizon Cloud Connector</td>
<td>Connection Server</td>
<td>4002</td>
<td>TCP</td>
<td>Java Message Service (JMS) communication between the Cloud Connector and the Connection Server</td>
</tr>
<tr>
<td>New version of the Horizon Cloud Connector appliance</td>
<td>Existing version of the Horizon Cloud Connector appliance</td>
<td>22</td>
<td>SSH</td>
<td>Listen for requests to start the update process.</td>
</tr>
<tr>
<td>Web browser</td>
<td>Horizon Cloud Connector</td>
<td>443</td>
<td>HTTPS</td>
<td>Listen for the initiation of the pairing process.</td>
</tr>
<tr>
<td>Cloud Monitoring Service agent in the desktop or server VMs that are from the cloud-connected Horizon pod on your network</td>
<td>Horizon Cloud Connector appliance</td>
<td>11002</td>
<td>TCP</td>
<td>For the Cloud Monitoring Service agent on a server or desktop VM to send data to the Horizon Cloud Connector</td>
</tr>
</tbody>
</table>

Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector

To connect an existing Horizon pod with the current service release level for the purposes of using Horizon subscription licenses or cloud-hosted services with that pod, ensure you have the following items in place before you deploy the Horizon Cloud Connector appliance and running the onboarding wizard.

- Verify you have met the prerequisites described in [VMware Horizon Pods with Horizon Cloud - Requirements Checklist - Updated as Appropriate for Connecting Pods Starting from the January 2021 Service Release](#).
- You have determined which of the pod’s Connection Server instances you will pair with the Horizon Cloud Connector virtual appliance and you have the FQDN of that Connection Server instance. You can pair the Horizon Cloud Connector virtual appliance with only one of the pod's installed Connection Server instances at any given time.
You have determined which of the pod's administrator accounts you will specify when pairing the Connection Server with the Horizon Cloud Connector and that administrator account meets the requirements needed for pairing. This Active Directory user must have the Horizon predefined Administrators role on the root access group, as displayed in your pod's web-based console in **Global Administrators View > Role Permissions > Administrators**. In other words, the Active Directory user specified for the pod-onboarding process is a super user for that pod, as described in the Horizon documentation's Horizon Console Administration guide.

You have a valid My VMware account at [https://my.vmware.com](https://my.vmware.com). This account is required to purchase a Horizon subscription license, for running the Horizon Cloud Connector onboarding workflow to pair the pod with the cloud service, and for logging in to the cloud-based administrative console to use the cloud-hosted services with that pod.

A Horizon subscription license is associated with that My VMware account.

You have the information from the welcome email that was sent to that My VMware account's associated email address, including the link for downloading the Horizon Cloud Connector OVA. If you do not have the email information, you can download the OVA by logging in to my.vmware.com using that My VMware account and navigating to the product downloads that are listed for that account.

If you are using the Microsoft Internet Explorer Web browser, verify that the compatibility mode is off. This setting enables viewing the Horizon Cloud Connector appliance onboarding user interface in that web browser.

Verify that you have met the **DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod**.

Determine the static IP address that you will use for the Horizon Cloud Connector virtual appliance. You will need this IP address when you deploy the Horizon Cloud Connector appliance.

**Note** Do not use IPv6 with the Horizon Cloud Connector virtual appliance. IPv6 is not supported.

Verify you have the typical networking information that is appropriate for your environment to use when you deploy the Horizon Cloud Connector appliance in your pod's environment, such as your DNS search domain, DNS server IP address, default gateway address, and subnet mask.

**Note** Proxy SSL configuration is not supported for the self-signed certificate for the Horizon Cloud Connector virtual appliance.
(Horizon pods on premises or in VMware Cloud on AWS) Verify you have a strong root password for the Horizon Cloud Connector virtual appliance containing a minimum of eight characters with one capital, one numeric, and one special character.

**Important** When deploying the OVF template, you must specify a root password that meets the security standards of a strong password. However, due to a known limitation, the OVF deployment wizard continues to deploy the virtual appliance even if you specify a root password that does not contain a special character. In this case, the deployment succeeds but you will be blocked from logging in to the virtual appliance’s operating system after deployment.

To ensure your access to the virtual appliance after it is deployed, always specify a strong root password containing at least one special character as prompted by the OVF deployment wizard.

For the minimum use case of using Horizon subscription licenses with the Horizon pod, verify that you meet these prerequisites, in addition to the ones listed above:

- The Connection Server instance with which you will be pairing the Horizon Cloud Connector must be running version 7.10 or later. Version 7.10 is the minimum version that can be paired with the cloud service.

**Tip** Even though technically you can pair a Horizon pod that is running versions older than the latest version, to obtain the most up-to-date cloud-hosted features with that pod, the pod’s Connection Servers would best be running the most current software version. Only by using the most current combination of the Connection Server version and Horizon Cloud Connector version will you get access to the most up-to-date features of the cloud-hosted features beyond simply using a subscription license with that pod.

**Horizon Cloud Connector Known Considerations**

Keep these considerations in mind when you are using Horizon Cloud Connector.

- You must deploy the Horizon Cloud Connector virtual appliance into your pod’s vSphere environment using vSphere Client or vSphere Web Client. Do not deploy the appliance directly into the ESXi host.
- Use of IPv6 with the Horizon Cloud Connector virtual appliance is not supported.
- Proxy SSL configuration is not supported during the deployment of the Horizon Cloud Connector virtual appliance.
- Due to a known limitation, any no-proxy host configuration that you specify when deploying the OVF template is not honored by Horizon Cloud Connector 1.5 or earlier. To configure a no-proxy host configuration, you must change a configuration file in the appliance after it is deployed. For details, see VMware Knowledge Base article 76663. This limitation does not apply to Horizon Cloud Connector 1.6 or later.
- If you plan to use the pod with Universal Broker and Horizon Cloud Connector 1.5, and your environment requires using proxy settings, you must configure those proxy settings when
you deploy the OVF template. Due to a known limitation, Universal Broker will not honor any modifications made to proxy settings after deployment. Since you can only configure no-proxy hosts after deployment, this limitation means that the use of no-proxy hosts with Universal Broker is not supported by Horizon Cloud Connector 1.5. This limitation does not apply when you use Universal Broker with Horizon Cloud Connector 1.6 or later.

- Information about the static IP and proxy settings for the deployed Horizon Cloud Connector virtual appliance is saved in certain container files. When you want to change those settings on the virtual appliance, you must connect to the virtual appliance and edit those container files. If you change the static IP address for the deployed virtual appliance in your vSphere environment, you must edit the appropriate container file in the virtual appliance's operating system and run a command to ensure that the new IP address is shared with all the pod's components that depend upon the virtual appliance. See Update the Static IP for the Horizon Cloud Connector Virtual Appliance.

- Before deleting the Horizon Cloud Connector virtual appliance from your vCenter environment, point your browser to the Horizon Cloud Connector appliance’s IP address and use the Unplug action to remove the connection between the pod and Horizon Cloud.

- Using a separate vdmadmin account for the Horizon Cloud Connector paired with the Horizon pod is a best practice. Using a separate vdmadmin account avoids configurations being overridden between cloud and on-premises management. Using separate accounts also provides easier auditing for the cloud-based operations.

- The connection between the Horizon Cloud Connector and Horizon Cloud uses outbound Internet port 443. For all the connector’s required DNS, ports, and protocols, see DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod.

- You set the password for the root user of the Horizon Cloud Connector virtual appliance during deployment. By default, this password does not expire. However, based on your organization’s security policy, you might want to periodically update that root password by setting an expiry policy for that root user. For steps, see Set a Password Expiry Policy for the Horizon Cloud Connector Root User.

- If your Connection Server is using self-signed certificates and you then replace those self-signed certificates after pairing the pod with Horizon Cloud, you must log in to the Horizon Cloud Connector interface and use the Reconfigure workflow to perform the certificate validation steps again with the new self-signed certificate. When you log in to the Horizon Cloud Connector interface, you can click Reconfigure and complete the wizard steps to verify communication using the new self-signed certificate from the Connection Server.

Similarly, upgrading your Connection Server might result in changes to self-signed certificates. To ensure validation of the new certificates, perform the Reconfigure workflow for the Horizon Cloud Connector after upgrading your Connection Server.
If you added an entry to the /etc/hosts file to resolve the IP address of the Connection Server, you must restart the hze-core and csms services. Use the following commands:

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

To ensure that the Horizon Cloud Connector virtual appliance authenticates correctly with Horizon Cloud and the required Connection Server instances, you must synchronize the virtual appliance's clock with an NTP server. For more information, see Synchronize the Horizon Cloud Connector Virtual Appliance with an NTP Server.

If you encounter connectivity issues with the Horizon Cloud Connector configuration portal, see the troubleshooting information in VMware Knowledge Base (KB) article VMware Knowledge Base (KB) article 79859.

**Connect Horizon Cloud Service with an Existing Horizon Pod to Use Horizon Subscription Licenses or Cloud-Hosted Services or Both**

Connecting your existing Horizon pod with Horizon Cloud Service is a multi-step process. After you purchase a VMware Horizon subscription license, VMware sends you a license subscription email, which includes the link to download the Horizon Cloud Connector virtual appliance. Then you install the virtual appliance and power it on. After the virtual appliance is powered on and you verify the health of the required pod components and services, you use the connector's onboarding workflow to pair it with a Connection Server in the pod with which you want to use that subscription license. As part of a successful pairing process, the Horizon Cloud Connector virtual appliance bridges the Connection Server to Horizon Cloud Service, so that the cloud management plane can manage the Horizon subscription license and other cloud-hosted services for that now cloud-connected pod.
You use the steps here to connect existing Horizon pods to the cloud management plane. Connecting a pod to Horizon Cloud Service allows you to use Horizon subscription licenses with that pod, even if you do not take advantage of any cloud-hosted services with that pod. With a Horizon subscription license, you do not need to manually enter a license key to activate the license for the pod. After the pairing is complete, VMware activates the subscription license, typically within 4 hours after you paired the pod with the cloud control plane. When VMware has activated the subscription license, a message appears in the pod’s web-based management console that says your Horizon environment is using the subscription license.

As described in the Horizon Cloud Deployments and Onboarding Pods — Horizon Pods on VMware SDDCs and Horizon Cloud Pods on Microsoft Azure, the process to onboard a Horizon pod to Horizon Cloud involves these basic concepts:

- Horizon subscription licenses are managed from the cloud management plane, which is Horizon Cloud.
Therefore, if you want to use subscription licenses with a Horizon pod, you must connect the pod with that cloud management plane. If you wish to avoid connecting that pod with the cloud management plane, you will not be able to use subscription licenses with that pod.

Connecting that existing Horizon pod with the cloud management plane requires a connector, which is named Horizon Cloud Connector. The cloud management plane talks to the connector, which in turn talks to one of the pod's Connection Server instances. The connector is paired with only one of the pod's installed Connection Server instances at any given time.

Because the Horizon Cloud Connector has to reach both the cloud management plane and the pod's Connection Server instance that you are pairing it with, specific DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod must be met to have a successful outcome of pairing the Horizon Cloud Connector with the pod and for ongoing operations. Even the minimal use case of using a subscription license with the pod requires meeting those DNS, ports, and protocols requirements.

A My VMware account is required to obtain a Horizon subscription license and to authenticate with the cloud management plane to set up the connector and establish the connection to use that subscription license with the pod.

You might want to use only subscription licenses with your Horizon pod, or you might want to additionally use cloud-hosted services with that pod. Both of those use cases require a subscription license.

To obtain the most up-to-date features and security and bug fixes, you would best use the combination of running the most current version of the Connection Server software with the most current version of Horizon Cloud Connector. For the supported combinations of VMware Horizon software versions and VMware Horizon Cloud Connector versions, see the VMware Product Interoperability Matrices.

The high-level steps of this process are:

1. Obtain your My VMware account.
2. Use that My VMware account to sign up for a Horizon subscription license.
3. When you sign up for the license, a welcome email is sent to the email address associated with that My VMware account. That welcome email will contain a link to download the Horizon Cloud Connector image from the appropriate my.vmware.com Downloads area.
4. Download the Horizon Cloud Connector image using the link in the welcome email.
5. Deploy that appliance into the pod's environment using a static IP address. When the virtual appliance deployment process is completed, power on the virtual appliance.
6. Obtain the URL address to use to start the pairing workflow to pair the Horizon Cloud Connector with a Connection Server instance in the pod and complete the connection between the Connection Server instance, the Horizon Cloud Connector, and the cloud management plane.
7. Before starting the pairing workflow, run the precheck.sh script to verify the health of the pod's system components and services.
Use the URL address that you obtained earlier to start the pairing workflow. The login screen from Horizon Cloud will display and you log in using the My VMware account credentials. At that point, the workflow’s user interface appears in the browser and you complete the steps as detailed in this topic below.

**Important** If you already have cloud-connected pods in your Horizon Cloud environment to which you are connecting this pod, all those cloud-connected pods must have line of sight to the same set of Active Directory domains. When performing the steps to connect the not-yet-connected pod, you must ensure that the pod will have a line of sight to those Active Directory domains that are already registered with your Horizon Cloud environment.

As an example, if your environment already has pods in Microsoft Azure and you are connecting a Horizon pod, you must ensure:

- The Horizon pod you are connecting using the following steps has a line of sight to the Active Directory domains used by those existing pods in Microsoft Azure, because those domains are already registered with the cloud plane for your environment.

- Your existing cloud-connected pods in Microsoft Azure have line of sight to the Horizon pod’s Active Directory domain, the domain you are using in the following steps to pair the Horizon Cloud Connector virtual appliance with the Horizon pod’s Connection Server.

**Prerequisites**

Verify that you have fulfilled all of the items described in Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector.

Verify that you have met the DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod when using the Horizon Cloud Connector to pair a Horizon pod with Horizon Cloud.

Verify that your DNS configuration in your network topology will provide for the deployed Horizon Cloud Connector to resolve the FQDN of the pod’s Connection Server. If the deployed Horizon Cloud Connector cannot resolve the Connection Server using DNS, the onboarding wizard will encounter an unexpected error at the step where you enter the pod’s domain credentials.

Review Horizon Cloud Connector Known Considerations to ensure you are aware of those items.

The Horizon Cloud Connector virtual appliance must reach the Internet to talk to the Horizon Cloud control plane. If your environment requires use of a proxy server and proxy configuration for virtual appliances to reach the Internet, verify that you have reviewed the proxy-related information, known limitations, and known issues when using proxy settings with the Horizon
Cloud Connector appliance. See the proxy-related information in Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector, Horizon Cloud Connector Known Considerations, and Modifying Proxy Settings for Horizon Cloud Connector 1.6 or Later.

Procedure

1. **Download and Deploy the Horizon Cloud Connector into Your Pod’s Environment**
   To download and deploy the Horizon Cloud Connector, follow the instructions in the subtopic that applies to your VMware SDDC-based environment.

2. **Verify the Horizon Pod and Virtual Appliance Are Ready to Be Paired**
   In this step in the workflow of onboarding a Horizon pod to Horizon Cloud, you run the `precheck.sh` diagnostic tool to validate that the pod and Horizon Cloud Connector are both ready for the pairing process. By first running the diagnostics and remediating any blocking issues found in system components and configurations, you can maximize your chances of success when pairing the pod with Horizon Cloud.

3. **Complete Pairing the Horizon Pod with Horizon Cloud Using the Horizon Cloud Connector Configuration Portal**
   In this step in the workflow of onboarding a Horizon pod to Horizon Cloud, you use the Horizon Cloud Connector configuration portal to specify details that the Horizon Cloud Connector uses to pair with the Horizon pod’s Connection Server. Completing these steps successfully results in that pod connected to your Horizon Cloud tenant environment.

Results

When the Horizon pod is successfully connected with Horizon Cloud, the Horizon Cloud Connector configuration portal displays a Congratulations message. From this point, you use this same configuration portal to perform administrative tasks such as review the health status of the Horizon Cloud Connector components, activate or deactivate SSH access to the Horizon Cloud Connector virtual appliance, and similar tasks. For details, see the topic Typical Administrative and Maintenance Tasks You Perform on the Horizon Cloud Connector After the Horizon Pod is Paired with Horizon Cloud.
What to do next

If your only goal is to use your subscription license with the now cloud-connected pod, there are no additional steps to take, except to ensure that the DNS, ports, and protocols requirements continue to be met to maintain the connection between Horizon Cloud Connector and the cloud control plane. Because the subscription licenses are managed by the cloud control plane, Horizon Cloud Connector must continue to reach the cloud control plane for the pod to receive your subscription license information.

**Important** When the Horizon Cloud Connector is installed, the connection is established to the cloud control plane by outbound Internet port 443. This connection will be open all the time. If this connection between the Cloud Connector and the cloud control plane goes offline, there is a grace period of 10 days by default that can elapse before the pairing between this pod and Horizon Cloud is marked expired. If this happens, contact VMware Support for assistance.

If you want to leverage any of the cloud-hosted services with the cloud-connected pod, you must log in to the administrative console and complete the Active Directory registration workflow that registers the pod's Active Directory domain with Horizon Cloud. For details of that workflow, see *Performing Your First Active Directory Domain Registration in the Horizon Cloud Environment* in the Horizon Cloud Administration Guide.

**Download and Deploy the Horizon Cloud Connector into Your Pod's Environment**

To download and deploy the Horizon Cloud Connector, follow the instructions in the subtopic that applies to your VMware SDDC-based environment.

- For a Horizon pod on premises or in VMware Cloud on AWS, follow the instructions in *Horizon Pods on Premises or in VMware Cloud on AWS: Download and Deploy the Horizon Cloud Connector into the Pod's vSphere Environment*.
- For a Horizon pod in Azure VMware Solution (AVS), follow the instructions in *Horizon Pods in Azure VMware Solution: Download and Deploy the Horizon Cloud Connector into the Pod's Environment*.

**Horizon Pods on Premises or in VMware Cloud on AWS: Download and Deploy the Horizon Cloud Connector into the Pod's vSphere Environment**

In this step in the workflow of onboarding a Horizon pod to Horizon Cloud, you download and deploy the Horizon Cloud Connector in your vSphere environment. The result of these steps is the Horizon Cloud Connector virtual appliance is deployed and running in your vSphere environment.

**Important** You must deploy the Horizon Cloud Connector virtual appliance into your pod's vSphere environment using vSphere Client or vSphere Web Client. Do not deploy the appliance directly into the ESXi host.
Prerequisites

- Verify that you have met the connector-related prerequisites described in *Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector*.

- Verify that you have met the *DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod* for using Horizon Cloud Connector to pair a Horizon pod with Horizon Cloud.

- The Horizon Cloud Connector virtual appliance must reach the Internet to talk to the Horizon Cloud control plane. If your environment requires use of a proxy server and proxy configuration for deployed appliances to reach the Internet, verify that you have reviewed the proxy-related information, known limitations, and known issues when using proxy settings with the Horizon Cloud Connector appliance. See the proxy-related information in *Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector*, *Horizon Cloud Connector Known Considerations*, and *Modifying Proxy Settings for Horizon Cloud Connector 1.6 or Later*.

- (Horizon Cloud Connector 1.9 and later) If you want to enable Secure Shell (SSH) access to the appliance with the recommended level of security before pairing the appliance with the pod, generate an SSH public key. You must register the SSH public key during the deployment of the appliance.

  **Important**  Beginning with Horizon Cloud Connector 1.9, SSH access is no longer supported for the `root` user account. For improved security, SSH access is only supported for the `ccadmin` user account through public-key (strongly recommended) or password authentication.

  You can still use the `root` account to perform non-SSH administrative tasks on the appliance.

Procedure

1. As described in the prerequisites list, download the Horizon Cloud Connector appliance using the link provided in your subscription email.

   The Horizon Cloud Connector appliance is available as an OVA file and has its home location in my.vmware.com after you log in to my.vmware.com using your My VMware account credentials.

   **Important**  Ensure that the downloaded version is the most recent version —version 1.9.0.0 or later — to enable the most up-to-date features. If you previously downloaded a Horizon Cloud Connector OVA with a version prior to 1.9.0.0, log in to my.vmware.com and obtain the most recent version to use to pair your pod.

2. Use vSphere Client or vSphere Web Client to deploy the Horizon Cloud Connector appliance as an OVF template into your Horizon pod.

   For general information about deploying OVF templates, see the *vSphere Virtual Machine Administration* guide on the VMware vSphere Documentation page.
The OVF deployment wizard has several steps, where you make typical OVF deployment choices such as which host, which datastore, which network, and so on.

- (Horizon Cloud Connector 1.8 or later) The **Configuration** step is where you select a feature profile for the Horizon Cloud Connector appliance. The feature profile determines which Horizon Cloud services to activate for the appliance.

  **Note** If you are deploying Horizon Cloud Connector 1.7 or earlier, you do not have the option to select a feature profile. Deploying one of these versions of the appliance always activates the subscription license service and all additional cloud-hosted services, such as the Cloud Monitoring Service (CMS).

- The **Customize template** step is where you provide details that are specific for the Horizon Cloud Connector appliance.

**Important** You might have best results deploying the appliance into your pod when you use the VMware vSphere® Web Client, which is a Flex-based user interface. If you deploy using the VMware vSphere® Client™, which is the newest HTML5-based user interface, you might encounter an error message about an invalid value. That issue is caused by a known issue in the vSphere Client, and is not an issue with the Horizon Cloud Connector appliance package. If you encounter that error, deploy the appliance using the Flex-based user interface instead.
3  (Horizon Cloud Connector 1.8 or later) In the **Configuration** wizard step, select a feature profile to specify the Horizon Cloud services that are activated for the appliance.

**Note** Each feature profile has specific resource requirements. Before you select a profile for the appliance, ensure that you have configured the minimum resource capacity required by that profile, as described in *VMware Horizon Pods with Horizon Cloud - Requirements Checklist - Updated as Appropriate for Connecting Pods Starting from the January 2021 Service Release*.

<table>
<thead>
<tr>
<th>Feature Profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full Feature</strong></td>
<td>Activates all supported Horizon Cloud services for the appliance. These services include:</td>
</tr>
<tr>
<td></td>
<td>- Horizon subscription license service</td>
</tr>
<tr>
<td></td>
<td>- <strong>Cloud Broker Client Service</strong>, which supports Universal Broker and the creation of multi-cloud assignments</td>
</tr>
<tr>
<td></td>
<td>- <strong>Cloud Monitoring Service</strong>, which gives you the ability to monitor capacity, usage, and health within and across your fleet of cloud-connected pods</td>
</tr>
<tr>
<td></td>
<td>- <strong>Image Locality Service</strong>, which supports the Horizon Image Management Service</td>
</tr>
<tr>
<td></td>
<td>This feature profile is selected by default.</td>
</tr>
<tr>
<td><strong>Basic Feature</strong></td>
<td>Activates the subscription license service only. The Cloud Broker Client Service, Cloud Monitoring Service, and Image Locality Service are all deactivated.</td>
</tr>
<tr>
<td></td>
<td>Select this profile if you do not want to use additional Horizon Cloud services with the pod and you want to reduce the resource usage of the Horizon Cloud Connector appliance.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you select this feature profile and are onboarding your first pod into a new tenant account, manually turn off the Cloud Monitoring Service (CMS) setting after pairing the appliance with your pod. Due to a known limitation, the CMS setting does not automatically turn off when you select the Basic Feature profile. Turning off the setting manually ensures that the administration console does not make unnecessary attempts to connect to the CMS service. See the end of the topic <strong>Complete Pairing the Horizon Pod with Horizon Cloud Using the Horizon Cloud Connector Configuration Portal</strong>.</td>
</tr>
<tr>
<td></td>
<td>If you want to use additional Horizon Cloud services after deploying the appliance, you must activate each service manually. See <strong>Manually Activate Horizon Cloud Services for Horizon Cloud Connector 1.8 or Later</strong>.</td>
</tr>
</tbody>
</table>
4 In the **Customize template** wizard step, provide input for the required fields and for those items that are appropriate for your environment.

The input in this step is used to configure the virtual appliance.

a Specify a root password for the appliance.

**Note** Ensure that the new password meets the security standards of a strong password. Verify that the password contains a minimum of eight characters with at least one capital, one numeric, and one special character.

**Important** Due to a known limitation, the OVF deployment wizard continues to deploy the virtual appliance even if you specify a root password that does not contain a special character. In this case, the deployment succeeds but you will be blocked from logging in to the virtual appliance's operating system after deployment. To ensure your access to the virtual appliance after it is deployed, verify that the password contains at least one special character.

b (Horizon Cloud Connector 1.9 and later) To use SSH public key authentication for the ccadmin account, enter the SSH public key that you generated earlier.

**Important** Beginning with Horizon Cloud Connector 1.9, SSH access is no longer supported for the root user account. For improved security, SSH access is only supported for the ccadmin user account through public-key (strongly recommended) or password authentication.

You can still use the root account to perform non-SSH administrative tasks on the appliance.

For more information, see [Enable SSH Access to the Horizon Cloud Connector Before Pairing It with Your Horizon Connection Server](#).

If you do not need SSH access to the appliance before pairing the appliance with the pod, you can skip this step. You can wait to register a public key and enable SSH access until after the appliance is paired with the pod.
c Specify a static IP address for the virtual appliance.

Do not use IPv6 with the Horizon Cloud Connector virtual appliance. IPv6 is not supported.

d If your environment requires use of an HTTP proxy server for your virtual appliances to access the Internet, configure the proxy-related settings.

**Important** Keep the following considerations in mind:

- Proxy SSL configuration is not supported for the self-signed certificate for the Horizon Cloud Connector virtual appliance.

- (Horizon Cloud Connector 1.6 or later) To ensure that only outbound requests to the Internet route through the HTTP proxy, configure no-proxy hosts that bypass the proxy server when receiving internal requests from the appliance. At the minimum, for **No Proxy For**, enter the DNS subdomain of the Connection Server and vCenter Server instances associated with the pod that will be paired with Horizon Cloud Connector. You can also specify no-proxy hosts by entering an IP range, using a comma separator between entries as shown in the following example:

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

If you leave the **No Proxy For** setting blank, the virtual appliance fetches the Connection Server host names provided by the administrator or discovered through querying the pod and configures those hosts as implicit no-proxy hosts.

5 Power on the Horizon Cloud Connector appliance.

6 When the appliance is fully powered on, use the vSphere Client’s option to start the Horizon Cloud Connector appliance’s console.

The Horizon Cloud Connector appliance’s blue console screen appears. That blue console screen displays the URL address to load in your browser for the onboarding workflow. The following screenshot is an example for a deployed appliance that has address https://10.92.245.255/.

7 Complete the steps in **Enable SSH Access to the Horizon Cloud Connector Before Pairing It with Your Horizon Connection Server.**
If you want to use a fully qualified domain name (FQDN) for the Horizon Cloud Connector virtual appliance and resolve the host name, create a forward and reverse lookup record in your DNS server that maps that FQDN to the Horizon Cloud Connector virtual appliance’s static IP.

Continue with the pod onboarding workflow by doing one of the following.

- If you have deployed Horizon Cloud Connector 1.6 or later, proceed to Verify the Horizon Pod and Virtual Appliance Are Ready to Be Paired.
- If you have deployed Horizon Cloud Connector 1.5 or earlier, proceed to Complete Pairing the Horizon Pod with Horizon Cloud Using the Horizon Cloud Connector Configuration Portal.

Horizon Pods in Azure VMware Solution: Download and Deploy the Horizon Cloud Connector into the Pod’s Environment

Follow these steps to download and deploy the Horizon Cloud Connector appliance for a pod that resides in Azure VMware Solution (AVS).

The following is a high-level overview of the steps required to deploy Horizon Cloud Connector into the AVS environment of your Horizon pod:

- Download the Horizon Cloud Connector VHD file.
- Create an Azure storage container and upload the appliance VHD to that storage container.
- Create a virtual machine (VM) image from the uploaded VHD.
- Create the Horizon Cloud Connector VM from the VM image.

**Note** The following features and services are not supported for Horizon pods in AVS:

- Automated updates of Horizon Cloud Connector
- Universal Broker and multi-cloud assignments
- Cloud Monitoring Server (CMS)
- Horizon Image Management Service

**Prerequisites**

- Verify that you have met the connector-related prerequisites described in Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector.
- Verify that you have met the DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod for using Horizon Cloud Connector to pair a Horizon pod with Horizon Cloud.
- The Horizon Cloud Connector virtual appliance must reach the Internet to talk to the Horizon Cloud control plane. If your environment requires use of a proxy server and proxy configuration for deployed appliances to reach the Internet, verify that you have reviewed
the proxy-related information, known limitations, and known issues when using proxy settings with the Horizon Cloud Connector appliance. See the proxy-related information in Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector, Horizon Cloud Connector Known Considerations, and Modifying Proxy Settings for Horizon Cloud Connector 1.6 or Later.

Procedure

1. Download the Horizon Cloud Connector disk image using the link provided in your subscription email.

   The Horizon Cloud Connector disk image is available as a VHD file compressed into a ZIP package after you log in to my.vmware.com using your My VMware account credentials. Download and extract the VHD file to your local system.

   **Important** To enable the most up-to-date features, download version 1.8.0.0 or later of the Horizon Cloud Connector disk image.

   Before uploading the disk image file to your AVS environment, you must first create an Azure storage container and share it using a shared access signature.

2. In the Azure portal, navigate to your storage account and create a storage container for the VHD file. For more information, see https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview.

   During the creation of the shared access signature, a SAS token is generated. You must construct a storage account URL for the disk image file by appending the SAS token to the storage container URL.

   a. Open the storage container by navigating to Storage Account > Properties > URL. Take note of the storage container URL for the next steps.

   b. Create a shared access signature. Navigate to Storage Account > Shared access signature > Select Resource types and Generate SAS and Connection String. Take note of the generated SAS token for the next steps.

   c. Construct the storage account URL using this format:

      `<StorageContainerPath>/HorizonCloudConnectorDiskImageName.vhd<SAS-Token>`

      The following is an example of a storage account URL:

      ```
      https://azurestorage1.blob.core.windows.net/vmware/horizon-cloud-connector-1.8.0.0-16488286.vhd?
sv=2020-01-01&ss=bfqt&srt=sco&sp=rwdlapx&se=2020-01-01T12:00:00Z&st=2020-01-01T06:00:00Z&spr=https&sig=dUPul74l4K0ah%2FdoCpaTTjY4t2Js8kB%3D
      ```
3 Upload the disk image file to the storage account URL that you created.
   a Download and install the AzCopy utility on the local system where you extracted the VHD file containing the Horizon Cloud Connector disk image.

   For more information about the AzCopy utility, see https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10.

   b To upload the VHD file, run the following command in the AzCopy utility:

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

   The following shows an example of an upload command issued from a local Windows computer:

   ```
   azcopy cp c:\horizon-cloud-connector-1.9.0.0-16488286.vhd "https://azurestorage1.blob.core.windows.net/vmware/horizon-cloud-connector-1.8.0.0-16488286.vhd?sv=2020-01-01&ss=bfqt&srt=sco&sp=rwdlapx&se=2020-01-01T12:00:00Z&st=2020-01-01T06:00:00Z&spr=https&sig=dUPul74l4K0ah%2FdoCpaTTjY4t2Js8kB%3D" --blob-type PageBlob
   ```

4 Create a virtual machine (VM) image from the uploaded VHD file.
   a In the Azure portal, navigate to Images and create a new VM image. Enter a name for the image, and specify the target location and resource group.

   b Specify the following options:

   - Set the **OS type** option to **Linux**.
   - Set the **VM generation** option to **Gen1**.

   c For the Storage blob, browse to the storage account and container that you created, and select the VHD file that you uploaded.

   d Click **Create** to create the VM image from the VHD file.

5 Deploy the Horizon Cloud Connector appliance by creating the appliance VM from the VM image.
   a In the Azure portal, open the VM image that you created in the previous step. Click **Create VM**.

   b Specify the following settings:

   - Enter a name for the new VM. This will be the hostname of the Horizon Cloud Connector appliance.

   - For **VM Sizing**, specify a value that is higher than “Standard_D4s - v3.”

   c For the Administrator account, specify **ccadmin** as the user name. You must create this ccadmin user account in order to allow SSH access to the appliance.
d  For SSH Access, specify the **SSH Public Key** authentication method.

**Note**  Both SSH Public Key and Password authentication methods are supported. However, SSH Public Key provides stronger security and is the preferred method.

e  For Firewall settings, configure the following ports:

- Port 443 for HTTPS
- Port 22 for SSH

If you intend to configure a firewall and proxy server for the appliance, you must also configure the appliance to allow certain public URLs. For more information, see [DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod](#).

f  For Network settings, specify a public IP Address allocation if you need to allow access to appliance over a public network. Also, specify the public inbound ports for HTTPS and SSH.

g  Navigate to **VM Properties** and take note of the IP address and FQDN of the appliance VM. You will need this information later to access the browser-based Horizon Cloud Connector configuration portal.

6  If your environment requires use of an HTTP proxy server for your virtual appliances to access the Internet, configure proxy-related settings for the appliance, as described in [Modifying Proxy Settings for Horizon Cloud Connector 1.6 or Later](#).

7  Configure the required certificates, as described in [Configure a CA-Signed Certificate for the Horizon Cloud Connector Virtual Appliance](#).

8  Complete the steps in [Enable SSH Access to the Horizon Cloud Connector Before Pairing It with Your Horizon Connection Server](#).

9  If you want to use a fully qualified domain name (FQDN) for the Horizon Cloud Connector appliance and resolve the host name, create a forward and reverse lookup record in your DNS server that maps that FQDN to the Horizon Cloud Connector virtual appliance's static IP.

10  Continue with the pod onboarding workflow by following the steps in [Verify the Horizon Pod and Virtual Appliance Are Ready to Be Paired](#). Then proceed to [Complete Pairing the Horizon Pod with Horizon Cloud Using the Horizon Cloud Connector Configuration Portal](#).

**Enable SSH Access to the Horizon Cloud Connector Before Pairing It with Your Horizon Connection Server**

Use these steps if you want to use a Secure Shell (SSH) connection with the deployed Horizon Cloud Connector appliance prior to running the onboarding wizard to pair the appliance with the pod.
If you do not require SSH access to Horizon Cloud Connector before pairing the appliance with the pod, you can wait to enable it until after the appliance is paired with the pod. See **Enable or Deactivate SSH on the Horizon Cloud Connector Appliance Using the Configuration Portal** in the *Administration Guide*.

**Prerequisites**

For Horizon pods on premises or in VMware Cloud on AWS, perform the following tasks.

- Verify that the Horizon Cloud Connector appliance is successfully deployed into your pod’s environment as described in the subtopics under *Download and Deploy the Horizon Cloud Connector into Your Pod’s Environment*, but not yet paired with the Connection Server.

- (Horizon Cloud Connector 1.9 and later) To use the recommended public key authentication for SSH access, generate an SSH public key and register the key during the appliance deployment. See *Horizon Pods on Premises or in VMware Cloud on AWS: Download and Deploy the Horizon Cloud Connector into the Pod’s vSphere Environment*.

  Alternatively, if you do not register the public key during deployment, you can copy the public key to the appropriate keys file after enabling SSH access, as described in the steps later in this topic.

**Enable SSH Access With Public-Key Authentication for Horizon Cloud Connector 1.9 and Later for Horizon Pods on Premises or in VMware Cloud on AWS**

**Important**  Beginning with Horizon Cloud Connector 1.9, SSH access is no longer supported for the `root` user account. For improved security, SSH access is only supported for the `ccadmin` user account through public-key (strongly recommended) or password authentication.

You can still use the `root` account to perform non-SSH administrative tasks on the appliance.

Use the following steps to enable SSH access to the Horizon Cloud Connector for the `ccadmin` user. As a security best practice, it is strongly recommended that you configure an SSH public key for authenticating the `ccadmin` user to the appliance.

1. Use vSphere Client to launch the console for the deployed appliance and log in to the appliance using the `root` account and password you set when you deployed the OVA into vSphere.

2. Set the password for the `ccadmin` account.

   ```
   passwd ccadmin
   ```

   **Note**  Ensure that the new password meets the security standards of a strong password. Verify that the password contains a minimum of eight characters with at least one capital, one numeric, and one special character.

3. Enable SSH access by running the following command.

   ```
   /opt/vmware/bin/configure-adapter.py --sshEnable
   ```
Configure public-key authentication using one of the following methods.

- If you registered the SSH public key in the **Customize template** step of the appliance deployment wizard, public-key authentication is already configured and no additional steps are required.
  
  For more information, see [Horizon Pods on Premises or in VMware Cloud on AWS: Download and Deploy the Horizon Cloud Connector into the Pod's vSphere Environment](#).

- If you did not register the SSH public key during the appliance deployment, run the following command from the client system, replacing `<IP_appliance>` with the IP address of the Horizon Cloud Connector appliance. When prompted, enter the `ccadmin` password.

  ```bash
  ssh-copy-id ccadmin@<IP_appliance>
  ```

  The `ssh-copy-id` command copies the public key to the `ccadmin` user's `~/.ssh/authorized_keys` file.

  **Note** If you do not configure public-key authentication, password credentials are used to authenticate the `ccadmin` user for SSH access. For improved security, it is strongly recommended that you use public-key authentication instead of password authentication for SSH access.

  SSH access to the appliance is now enabled.

  **Note** To run commands as a `ccadmin` user with elevated permissions, append the `sudo` prefix to the commands in an SSH session.

**Enable SSH Access to Horizon Cloud Connector 1.8 and Earlier for Horizon Pods on Premises or in VMware Cloud on AWS**

To open an SSH connection to Horizon Cloud Connector 1.8 or earlier, you must enable SSH access and log in as the `root` user.

1. Use vSphere Client to launch the console for the deployed appliance and log in to the appliance using the `root` account and password you set when you deployed the OVA into vSphere.

2. Enable SSH access by running the following command.

   ```bash
   /opt/vmware/bin/configure-adapter.py --sshEnable
   ```

   SSH access to the appliance is now enabled.

**Deactivate SSH Access to Horizon Cloud Connector for Horizon Pods on Premises or in VMware Cloud on AWS**

If you need to deactivate SSH access to the appliance, use the following command:

```bash
/opt/vmware/bin/configure-adapter.py --sshDisable
```
Enable SSH Access to Horizon Cloud Connector for Horizon Pods in Azure VMware Solution (AVS)

1. In the Azure portal, navigate to the Horizon Cloud Connector VM. Start the Run command action and choose RunPowerShellScript.

2. Enable SSH access by running the following command.

```
/opt/vmware/bin/configure-adapter.py --sshEnable
```

SSH access to the appliance is now enabled.

3. If you deployed Horizon Cloud Connector 1.7 and want to use SSH public key authentication, run the following additional command.

```
chmod 744 /home/ccadmin
```

What to do next

Proceed to Verify the Horizon Pod and Virtual Appliance Are Ready to Be Paired. Then continue to Complete Pairing the Horizon Pod with Horizon Cloud Using the Horizon Cloud Connector Configuration Portal. When pairing is successfully completed, the Horizon Cloud Connector web-based configuration portal will provide a toggle that you can use to deactivate SSH access for the appliance, or re-enable SSH if it was previously deactivated.

Modifying Proxy Settings for Horizon Cloud Connector 1.6 or Later

You can configure HTTP proxy settings during deployment of the Horizon Cloud Connector OVF template. If you want to modify these proxy settings after deployment, you must use the configure-webproxy.py command. The configure-webproxy.py command is located in the /opt/vmware/bin directory of the deployed Horizon Cloud Connector appliance.

**Note**  
Observe the following guidelines with respect to proxy settings and appliance updates:

- If you manually update Horizon Cloud Connector 1.6 or later to a newer version, you must reconfigure your proxy settings. Your original proxy configuration does not carry over with the manual appliance update.

- If Horizon Cloud Connector 1.6 or later is automatically updated to a newer version, your proxy settings carry over with the automatic update. You do not need to reconfigure the proxy settings.

- To view the existing proxy settings for the Horizon Cloud Connector virtual appliance, run the following command.

```
cat /opt/container-data/cc-settings/proxy.conf
```

Syntax for Using configure-webproxy.py

Use the following syntax to create a script with configure-webproxy.py:

```
configure-webproxy.py [argument1 [value1]] [argument2 [value2]] ...
```
To display the command usage and list of available arguments, run `configure-webproxy.py -h` or `configure-webproxy.py --help`.

**Arguments for configure-webproxy.py**

All arguments are optional for the `configure-webproxy.py` script.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--proxyHost</td>
<td>Host name or IP address of the HTTP proxy server</td>
</tr>
<tr>
<td>--proxyPort</td>
<td>Port number for the proxy connection</td>
</tr>
<tr>
<td>--noProxyFor</td>
<td>Hosts or network range configured to bypass the HTTP proxy. Use spaces to separate multiple values.</td>
</tr>
<tr>
<td>--proxySsl</td>
<td>Specifies whether to use SSL for the proxy connection. Allowed values are true or false.</td>
</tr>
<tr>
<td>--proxyUsername</td>
<td>User name for the HTTP proxy</td>
</tr>
<tr>
<td>--proxyPassword</td>
<td>Password for the HTTP proxy</td>
</tr>
<tr>
<td>--implicitNonProxyHosts</td>
<td>Specifies whether to add the paired pod's Connection Server and vCenter Server implicitly to the list of hosts that bypass the HTTP proxy. Allowed values are true or false. The default is true. If your environment requires internal requests to the Connection Server and vCenter Server to route through the proxy, set this argument to false. In this case, only the hosts specified explicitly by --noProxyFor bypass the proxy.</td>
</tr>
</tbody>
</table>

**Example Script**

```bash
configure-webproxy.py --proxyHost PROXYEXAMPLE --proxyPort 80 --proxySsl=false --noProxyFor "*.AD-DOMAIN.EXAMPLE.COM 10.109.*"
```

This example script configures the following proxy settings:

- PROXYEXAMPLE is the proxy server.
- The proxy connection uses port 80.
- The proxy connection does not use SSL.
- Hosts that fall under .AD-DOMAIN.EXAMPLE.COM and 10.109.* bypass the proxy.
- Also, the paired pod's Connection Server and vCenter Server implicitly bypass the proxy by default.

**Configure a CA-Signed Certificate for the Horizon Cloud Connector Virtual Appliance**

For enhanced security, you can configure a custom CA-signed certificate for the Horizon Cloud Connector virtual appliance.

**Prerequisites**

- Verify that the full certificate chain is available in the PEM format.
- Verify that the private key is available in the PEM format.
- Verify that the FQDN and Subject Alt Name is included in the issued certificate.

Procedure

1. Open an SSH session to your deployed Horizon Cloud Connector virtual appliance.
2. Copy the CA-signed certificate in the directory `/root/server.crt`.
3. Copy the CA-signed key in the directory `/root/server.key`.
4. Back up the existing certificate.
   - (Horizon Cloud Connector version 1.4 or later) Use the following command:
     ```bash
cp /opt/container-data/certs/hze-nginx/server.crt /opt/container-data/certs/hze-nginx/server.crt.orig
```
   - (Horizon Cloud Connector version 1.3 or earlier) Use the following command:
     ```bash
cp /etc/nginx/ssl/server.crt /etc/nginx/ssl/server.crt.orig
```
5. Back up the existing key.
   - (Horizon Cloud Connector version 1.4 or later) Use the following command:
     ```bash
cp /opt/container-data/certs/hze-nginx/server.key /opt/container-data/certs/hze-nginx/server.key.orig
```
   - (Horizon Cloud Connector version 1.3 or earlier) Use the following command:
     ```bash
cp /etc/nginx/ssl/server.key /etc/nginx/ssl/server.key.orig
```
6. Copy the existing nginx conf file.
   - (Horizon Cloud Connector version 1.4 or later) Use the following command:
     ```bash
cp /opt/container-data/conf/hze-nginx/nginx.conf /opt/container-data/conf/hze-nginx/nginx.conf.orig
```
   - (Horizon Cloud Connector version 1.3 or earlier) Use the following command:
     ```bash
cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.orig
```
7. Copy the CA certificate in the appropriate directory for your virtual appliance version.
   - (Horizon Cloud Connector version 1.4 or later) Use the following command:
     ```bash
cp /root/server.crt /opt/container-data/certs/hze-nginx/server.crt
```
   - (Horizon Cloud Connector version 1.3 or earlier) Use the following command:
     ```bash
cp /root/server.crt /etc/nginx/ssl/server.crt
```
8 Copy the CA certificate key file in the appropriate directory for your virtual appliance version.

- (Horizon Cloud Connector version 1.4 or later) Use the following command:

```
cp /root/server.key /opt/container-data/certs/hze-nginx/server.key
```

- (Horizon Cloud Connector version 1.3 or earlier) Use the following command:

```
cp /root/server.key /etc/nginx/ssl/server.key
```

9 Verify the owner and permissions for the certificate and key file.

- (Horizon Cloud Connector version 1.4 or later) Use the following commands:

```
chown -R hze-nginx:hze-nginx /opt/container-data/certs/hze-nginx
chmod 644 /opt/container-data/certs/hze-nginx/server.crt
chmod 600 /opt/container-data/certs/hze-nginx/server.key
```

- (Horizon Cloud Connector version 1.3 or earlier) Use the following commands:

```
chown -R root:root /etc/nginx/ssl
chmod -R 600 /etc/nginx/ssl
```

10 Verify that the issued FQDN in the certificate matches the server name directive in the server listen 443 block in the nginx configuration file.

- (Horizon Cloud Connector version 1.4 or later) The nginx configuration file is located at `/opt/container-data/conf/hze-nginx/nginx.conf`.

- (Horizon Cloud Connector version 1.3 or earlier) The nginx configuration file is located at `/etc/nginx/nginx.conf`.

11 Verify and restart nginx.

- (Horizon Cloud Connector version 1.4 or later) Use the following commands:

```
docker exec -i hze-nginx sudo nginx -t
systemctl restart hze-nginx
```

- (Horizon Cloud Connector version 1.3 or earlier) Use the following commands:

```
nginx -t
systemctl restart nginx
```

12 (Horizon Cloud Connector version 1.4 or later) Update the SSL thumbprints in the welcome screen.

Use the following commands:

```
docker exec -i hze-core sudo /opt/vmware/bin/configure-welcome-screen.py
/usr/bin/killall --quiet vami_login
```
13 Test the new certificate by reloading the Horizon Cloud Connector user interface URL in a Web browser.

14 (Optional) If the certificate works correctly, remove the backed-up files.

- (Horizon Cloud Connector version 1.4 or later) Use the following commands:
  ```
  rm /opt/container-data/certs/hze-nginx/server.crt.orig
  rm /opt/container-data/certs/hze-nginx/server.key.orig
  rm /opt/container-data/conf/hze-nginx/nginx.conf.orig
  ```

- (Horizon Cloud Connector version 1.3 or earlier) use the following commands:
  ```
  rm /etc/nginx/ssl/server.crt.orig
  rm /etc/nginx/ssl/server.key.orig
  rm /etc/nginx/nginx.conf.orig
  ```

15 Remove the copied CA certificates and key files in the root directory.

Use the following commands:

```
rm /root/server.crt
rm /root/server.key
```

**Synchronize the Horizon Cloud Connector Virtual Appliance with an NTP Server**

To ensure that the Horizon Cloud Connector virtual appliance authenticates correctly with Horizon Cloud and the required Connection Server instances, you must synchronize the virtual appliance's clock with a Network Time Protocol (NTP) server. Synchronize the clock on the Horizon Cloud Connector virtual appliance with the clock on the physical ESXi host on which the virtual appliance resides, after first ensuring that the host itself is properly synchronized with an NTP server.

**Procedure**

- (Preferred method) Synchronize the Horizon Cloud Connector virtual appliance with the physical ESXi host on which the virtual appliance resides.
  
  a Verify that the ESXi host's clock is properly synchronized with an NTP server.

  For more information, see the VMware vSphere Documentation.

  b Use vSphere Client to open the Edit Settings window of the Horizon Cloud Connector virtual appliance and enable the **Synchronize Time with Host** option.

  For detailed instructions, see the VMware vSphere Documentation.

**Note** In Horizon Cloud Connector 1.5 and later, **Synchronize Time with Host** is enabled by default.
(Alternative method) If you are unable to synchronize the Horizon Cloud Connector virtual appliance with the physical ESXi host, you can synchronize the virtual appliance directly with an NTP server.

**Note**  The preferred method of time synchronization is to synchronize the virtual appliance with the physical ESXi host. Use the following steps only if you are unable to perform the preferred method.

a. Open an SSH connection to the Horizon Cloud Connector virtual appliance, and log in as the root user.

b. Using a text editor such as `vi`, open the `timesyncd.conf` file for editing.

   ```
   vi /etc/systemd/timesyncd.conf
   ```

c. Edit the `[Time]` section so that it resembles the following example. Replace `ntpAddress` with the domain name of the NTP server that you want to use.

   ```
   [Time]
   #FallbackNTP=time1.google.com time2.google.com time3.google.com time4.google.com
   NTP=ntpAddress
   ```

   Save your changes to the `timesyncd.conf` file and exit the text editor.

d. Restart the virtual appliance's network service.

   ```
   systemctl restart systemd-networkd
   ```

e. Restart the virtual appliance's timesync service.

   ```
   systemctl restart systemd-timesyncd
   ```

f. Verify that the clock on the virtual appliance is now synchronized with the specified NTP server.

**Manually Activate Horizon Cloud Services for Horizon Cloud Connector 1.8 or Later**

If you deployed Horizon Cloud Connector 1.8 or later and selected the **Basic Feature** profile in the deployment wizard, only the Horizon subscription license service is activated. If you want to activate additional Horizon Cloud Services for your cloud-connected Horizon pod, you can do so by running commands in a Secure Shell session on the Horizon Cloud Connector appliance.

You can optionally activate one or more of the following cloud-hosted services:

**Cloud Monitoring Service**

The Cloud Monitoring Service (CMS) allows you to monitor capacity, usage, and health within and across your fleet of cloud-connected pods. To activate the CMS, you must first activate the Connection Server Monitoring Service which supports the CMS capabilities for a particular Horizon pod.
For more information about the CMS, see the topic *Introducing the Cloud Monitoring Service's Unified Visibility, Health Monitoring, and Help Desk Features Provided in Horizon Cloud* in the *Administration Guide*.

**Cloud Broker Client Service**

The Cloud Broker Client Service supports the use of Universal Broker with your Horizon pod. You must activate the Cloud Broker Client Service if you want to use Universal Broker and configure multi-cloud assignments based on resources in your Horizon pod.

For more information about Universal Broker and multi-cloud assignments, see the topics under *Setting Up a Brokering Method and End-User Assignments in Your Horizon Cloud Tenant Environment* in the *Administration Guide*.

**Image Locality Service**

The Image Locality Service supports the use of the Horizon Image Management Service with your Horizon pod. You must activate the Image Locality Service if you want to use the Horizon Image Management Service to track and manage system images from your Horizon pod.

For more information about the Horizon Image Management Service, see the topics under *Managing Horizon Images from the Cloud*.

**Important** Observe the following guidelines:

- Do not perform these activation steps if you deployed Horizon Cloud Connector 1.7 or earlier, or if you deployed version 1.8 or later of the appliance with the Full Feature profile. In either of these cases, all supported Horizon Cloud services are already activated and running.
- Use these steps only to activate services if you selected the Basic Feature profile during the appliance deployment.
- Once you have activated a service, do not attempt to deactivate it manually. Deactivating a service can produce unexpected results.

**Procedure**

1. Navigate to the deployed Horizon Cloud Connector appliance in your pod's vSphere environment and configure the resource capacity required by the additional service or services that you want to activate.

<table>
<thead>
<tr>
<th>Additional Service to Activate</th>
<th>Minimum Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Server Monitoring Service</td>
<td>Total of 7 vCPUs, 8 GB memory (RAM), 40 GB datastore</td>
</tr>
<tr>
<td>Cloud Broker Client Service</td>
<td>Total of 6 vCPUs, 8 GB memory (RAM), 40 GB datastore</td>
</tr>
<tr>
<td>Image Locality Service</td>
<td>Total of 6 vCPUs, 7.5 GB memory (RAM), 40 GB datastore</td>
</tr>
<tr>
<td>Two or more of the above services</td>
<td>Total of 8 vCPUs, 8 GB memory (RAM), 40 GB datastore</td>
</tr>
</tbody>
</table>
2  Activate and start each service that you want to use.
   a  Open a Secure Shell (SSH) session on the Horizon Cloud Connector appliance, and log in as the root user.
   b  Run the commands corresponding to each service that you want to activate.

| Connection Server Monitoring Service (required for the Cloud Monitoring Service) | systemctl enable csms  
|                                                                                   | systemctl restart csms |
| Cloud Broker Client Service                                                      | systemctl enable cbcs  
|                                                                                   | systemctl restart cbcs |
| Image Locality Service                                                           | systemctl enable ils   
|                                                                                   | systemctl restart ils  |

3  If you activated the Connection Server Monitoring Service, go to Settings > General Settings and verify that the Cloud Monitoring Service toggle is switched on.

Verify the Horizon Pod and Virtual Appliance Are Ready to Be Paired

In this step in the workflow of onboarding a Horizon pod to Horizon Cloud, you run the precheck.sh diagnostic tool to validate that the pod and Horizon Cloud Connector are both ready for the pairing process. By first running the diagnostics and remediating any blocking issues found in system components and configurations, you can maximize your chances of success when pairing the pod with Horizon Cloud.

**Note**  The precheck.sh diagnostic tool is only available for Horizon Cloud Connector 1.6 or later. If you have downloaded and deployed Horizon Cloud Connector 1.5 or earlier, disregard the following procedure and proceed directly to Complete Pairing the Horizon Pod with Horizon Cloud Using the Horizon Cloud Connector Configuration Portal.

The precheck.sh diagnostic tool validates the health of the services and components that are required to pair your Horizon pod successfully with Horizon Cloud. In addition, the tool checks whether:

- The configurations related to certificates and proxy settings are correct.
- Connectivity with Horizon Cloud and Connection Server can be established.
- Any SSL-related issues exist for Horizon Cloud Connector.

**Prerequisites**

Verify the following:

- You have completed the steps in Download and Deploy the Horizon Cloud Connector into Your Pod’s Environment, including the steps to Enable SSH Access to the Horizon Cloud Connector Before Pairing It with Your Horizon Connection Server.
- The Horizon Cloud Connector virtual appliance is powered on.

**Procedure**

1. Open an SSH session to your deployed Horizon Cloud Connector virtual appliance.
2. Run the diagnostic tool by using the following command. Replace `CS-FQDN` with the fully qualified domain name (FQDN) of the pod’s Connection Server.

   ```bash
   sudo /opt/vmware/bin/precheck.sh CS-FQDN
   ```

   If the diagnostic tool discovers an issue that prevents the pairing of your Horizon pod with Horizon Cloud, it reports the following information:

   - Name of the problem component or service
   - Status of the problem component or service
   - Associated error message and details
   - Suggested remediation steps, if any, to restore the component or service to a healthy and ready state

**Note** The diagnostic tool always reports one or both of the following expected conditions as part of its output. Both conditions are normal and expected at this stage of the onboarding workflow, and neither one blocks the pairing of the Horizon pod with Horizon Cloud.

- **Component/Service Name:** "Cloud Broker Client Service"
  - Status: "NOT_INITIALIZED"
  - Message: Service is not initialized.

  This condition pertains to the optional Universal Broker service, which remains in the NOT_INITIALIZED state until it is enabled as described in Setting Up Horizon Universal Broker for Multi-Cloud Assignments. You can still successfully pair the Horizon pod with Horizon Cloud when Universal Broker is in the NOT_INITIALIZED state. Therefore, this condition does not represent a blocking issue and you can disregard it.

- **Component/Service Name:** "Connector Client Service"
  - Status: "FAIL"
  - Message: Connector service is initialized post on-boarding.

  The Horizon Cloud Connector client service is initialized after you complete the pairing procedure, because the initialization process requires connectivity to Horizon Cloud. Therefore, the FAIL condition is expected at this stage of the onboarding workflow. After you pair the Horizon pod with Horizon Cloud, the Horizon Cloud Connector client service is initialized and the FAIL condition clears.
If the diagnostic tool reports an issue that interferes with the pairing process, investigate the affected component or service and perform the suggested remediation steps. As previously noted, you can disregard error conditions for "Cloud Broker Client Service" and "Connector Client Service" because they are not blocking issues.

As needed, repeat steps 2 and 3 to run the diagnostic tool again and troubleshoot problems until the tool does not report any blocking issues that prevent the pairing process. The Horizon pod and Horizon Cloud Connector are now ready for the pairing process.

**Note** If you attempt the pairing process without first clearing any blocking issues reported by the diagnostic tool, the pairing process might fail.

Continue with the pod onboarding workflow by following the steps in Complete Pairing the Horizon Pod with Horizon Cloud Using the Horizon Cloud Connector Configuration Portal.

**Complete Pairing the Horizon Pod with Horizon Cloud Using the Horizon Cloud Connector Configuration Portal**

In this step in the workflow of onboarding a Horizon pod to Horizon Cloud, you use the Horizon Cloud Connector configuration portal to specify details that the Horizon Cloud Connector uses to pair with the Horizon pod's Connection Server. Completing these steps successfully results in that pod connected to your Horizon Cloud tenant environment.

**Important** To ensure the proper functioning of the Horizon subscription license and other cloud-hosted services for a pod, you must pair only one Horizon Cloud Connector appliance with that pod. The pairing of more than one appliance with a pod is allowed only under certain circumstances such as appliance updates and troubleshooting procedures.

For an illustration of how the Horizon pod, Horizon Cloud, and Horizon Cloud Connector relate to each other in the pairing process, see the diagram shown in Connect Horizon Cloud Service with an Existing Horizon Pod to Use Horizon Subscription Licenses or Cloud-Hosted Services or Both.

**Note** If you encounter connectivity issues with the Horizon Cloud Connector configuration portal, see the troubleshooting information in VMware Knowledge Base (KB) article 79859.

**Prerequisites**

Verify that you have completed the required preparation steps:

- Verify that you have completed the steps in the applicable subtopics under Download and Deploy the Horizon Cloud Connector into Your Pod's Environment.

- If you have deployed Horizon Cloud Connector 1.6 or later, verify that you have completed the steps in Verify the Horizon Pod and Virtual Appliance Are Ready to Be Paired.

Also, verify that:

- The Horizon Cloud Connector virtual appliance is powered on.
You have the URL for displaying the browser-based Horizon Cloud Connector configuration portal. This URL is based on the IP address of the virtual appliance, such as https://IP-address/ where IP-address is the appliance's IP address. Alternatively, if you have mapped a fully qualified domain name (FQDN) to the Horizon Cloud Connector virtual appliance's IP address in your DNS server, the configuration portal's URL is that FQDN.

Verify that you have fulfilled all the items described in Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector, especially:

- You have met the DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod when using the Horizon Cloud Connector to pair a Horizon pod with Horizon Cloud.

- Your DNS configuration in your network topology enables the deployed Horizon Cloud Connector to resolve the FQDN of the pod's Connection Server. If the deployed Horizon Cloud Connector cannot resolve the Connection Server using DNS, the onboarding wizard will encounter an unexpected error at the step where you enter the pod's domain credentials.

- The Horizon Cloud Connector virtual appliance must reach the Internet to talk to the Horizon Cloud control plane and display the browser-based configuration portal. If your environment requires use of a proxy server and proxy configuration with deployed appliances, verify that you have configured the deployed Horizon Cloud Connector appliance with the proxy settings required for your environment. See the proxy-related information in Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector, Horizon Cloud Connector Known Considerations, and Modifying Proxy Settings for Horizon Cloud Connector 1.6 or Later.

- You have the credentials of the My VMware account that is associated with the Horizon Cloud customer account to which you are pairing the pod. As described in Connect Horizon Cloud Service with an Existing Horizon Pod to Use Horizon Subscription Licenses or Cloud-Hosted Services or Both, a My VMware account is required to authenticate with the cloud management plane to set up the connector and establish the connection to use that license for the Horizon subscription offerings.

Procedure

1. Get the URL for launching the web-based configuration portal.

   - (Horizon pods on premises or in VMware Cloud on AWS) Get the URL from the appliance's blue console screen.
(Horizon pods in Azure VMware Solution) Get the URL by navigating to the appliance VM in the Azure portal VM Properties and noting the IP address or FQDN of the appliance VM. Construct the URL as follows: https://IP-address or https://FQDN/

2 Using a browser, navigate to the URL that you obtained in the previous step.

**Important** In this step, the Horizon Cloud Connector makes a connection to Horizon Cloud to display the login screen, which will be used to authenticate your My VMware account credentials with the cloud control plane. This connection is outbound HTTPS using port 443. If you do not see a login screen, verify that you have met the DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod.

The login screen for logging in to the Horizon Cloud Connector configuration portal appears.

3 In the login screen, enter the My VMware account credentials and click **Login**.

The following screenshot is an example of the login screen with the credentials entered before clicking **Login**.

![Login Screen](image)

When the Terms of Service message appears, click **Accept** to continue.

The configuration portal displays the first step of the pod onboarding wizard. The following screenshot illustrates this step before any fields are filled in.
4 In the **Connect to Horizon Connection Server** field, enter the FQDN of the pod’s Connection Server instance to which you are pairing the Horizon Cloud Connector. As you type in the field, the **Connect** button appears.

![Connect to Horizon Connection Server](image)

5 When you have typed in the FQDN, click **Connect**.

![Connect to Horizon Connection Server](image)

The Horizon Cloud Connector attempts to communicate with the specified Connection Server and retrieve its certificate information. This process can take a few minutes. When communication is established, the page displays the retrieved certificate information. If the Connection Server does not have a valid Root CA certificate, a warning message appears saying that the certificate cannot be automatically validated and you must confirm its validity by clicking the check box. The following screenshot is an example of this situation.
If you see this message, verify that the displayed certificate information is accurate and click the check box so you can proceed to the next step.

**Note** If the Connection Server has a valid Root CA certificate, the wizard automatically validates the information and you can proceed to the next step.

The following screenshot illustrates the screen after clicking the check box.

6 In the credentials section, type the domain name and the administrator credentials used by the Connection Server and click **Connect**.

This administrator account must have the Horizon predefined Administrators role with root access for the pod. For more information about the requirements of the administrator account, see [Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector](#).

The following screenshot illustrates this area of the screen.
Note At this point, the system detects whether the specified Connection Server instance is already paired with another instance of the Horizon Cloud Connector. In this case, the page displays a message asking whether you want to delete the existing pairing and pair this Connection Server with the new Horizon Cloud Connector instance. If the new Horizon Cloud Connector instance is at a later version than the existing instance, you also have the option to perform an appliance update by copying the existing configuration into the new Horizon Cloud Connector instance, as described in Manually Update the Horizon Cloud Connector Virtual Appliance.

Click the appropriate action button in the message to continue pairing the pod using the following steps.

Step 2 of the wizard appears.

7 In this wizard step, provide details about the pod.

The following screenshot is an example of this step filled in.
These details are used in the cloud management plane to associate the paired Connection Server instance and Horizon Cloud Connector with your Horizon Cloud tenant environment. As an example, the specified name, location, and description will be visible in the administrative console so that you can identify this pod from your other pods that are connected to the control plane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a friendly name to identify this pod in your Horizon Cloud tenant environment.</td>
</tr>
<tr>
<td>Data Center Location</td>
<td>Select an existing location or click New to specify a new one to use for this pod. In the cloud-based administrative console, your pods are grouped and displayed according to the locations you specify. In the City Name text box, 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. Currently, due to a known issue, the location names are not localized.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional: Enter a description for this pod.</td>
</tr>
</tbody>
</table>

8 Proceed to the next wizard step by clicking **Save**.

The wizard's configuring step appears. The system checks the connection to the specified Connection Server instance and completes the final configuration steps. The following screenshot is an example of this step.

When the system determines the pod is successfully connected to the Horizon Cloud control plane, a congratulations screen appears with some guidance text and action buttons for post-configuration management tasks. The screen also shows the health status of activated cloud-hosted services. A gray dash icon indicates that the service is deactivated and therefore has no health status to display.

The following screenshot is an example of this screen.
You might see components that always appear in a deactivated state. Such components are planned for use in a future service release. Also, the action buttons on the congratulations screen can vary depending on the version of Horizon Cloud Connector that you have deployed:

- The **Configure vCenter Server and Network Details** button is available only if you have deployed Horizon Cloud Connector 1.7 or later.

- The **Configure Automatic Cloud Connector Updates** button is available only if you have deployed Horizon Cloud Connector 1.6 or earlier and your Horizon Cloud tenant account is configured for automated updates of the Horizon Cloud Connector. For details about that feature, see the topic **Automated Updates of the Horizon Cloud Connector Virtual Appliance** in the *Administration Guide*. 

Note: You might see components that always appear in a deactivated state. Such components are planned for use in a future service release. Also, the action buttons on the congratulations screen can vary depending on the version of Horizon Cloud Connector that you have deployed:
Note  (Horizon pods in Azure VMware Solution) Due to a known issue with Horizon Cloud Connector 1.7, certain components such as Cloud Broker Client Service, Cloud Gateway Service, Connector Client Service, and HZE-gateway might display with an error state. These error displays are incorrect and can be disregarded.
**Important**  (Horizon pods on premises or in VMware Cloud on AWS) If you have deployed Horizon Cloud Connector 1.7 or later, the **Horizon Cloud Connector vCenter Server Details** window automatically opens in front of the congratulations screen. To support automated updates and the proper functionality of Horizon Cloud Connector, you must enter these mandatory vCenter Server and network details as described in the topic **Automated Updates of the Horizon Cloud Connector Virtual Appliance** in the *Administration Guide*. If you close the **Horizon Cloud Connector vCenter Server Details** window without entering the mandatory details, you will encounter persistent warning messages until you click the **Configure vCenter Server and Network Details** button and enter the details.

The options provided in the **Horizon Cloud Connector vCenter Server Details** window can vary depending on the version of Horizon Cloud Connector that you have deployed. The following screenshot shows an example of the window as it initially appears when you have deployed version 1.9 of the appliance.

The following screenshot shows an example of the window as it initially appears when you have deployed version 1.8 or earlier of the appliance.
Results

When you reach this point, the pairing workflow is complete. At this point, VMware activates the subscription license, typically within 30 minutes after you paired the pod with the cloud control plane. When VMware has activated the subscription license, a message appears in your pod’s web-based management console that indicates your pod is using the subscription type of license. The following screenshot is a sample illustration.

Attention If 4 hours pass and you still do not see the Connected to License Service message in your pod’s web-based management console’s licensing area, contact your VMware representative.

What to do next

From this point, the pod is successfully paired with Horizon Cloud. For details about those Horizon Cloud Connector administrative and maintenance tasks that are typically done from this point on, see the topic Typical Administrative and Maintenance Tasks You Perform on the Horizon Cloud Connector After the Horizon Pod is Paired with Horizon Cloud in the Administration Guide.

Note If you have just onboarded your first pod into a new tenant account using Horizon Cloud Connector 1.8 or later and you selected the Basic Feature profile in the deployment wizard, manually turn off the Cloud Monitoring Service (CMS) setting. Due to a known limitation, the CMS setting does not automatically turn off when you select the Basic Feature profile. Turning off the CMS setting manually ensures that the administration console does not make unnecessary attempts to connect to the CMS service.

1 Select Settings > General Settings.
2 Turn off the Cloud Monitoring Service toggle.
When Adding a Horizon Pod on Microsoft Azure as Your Very First Pod in Your Horizon Cloud Pod Fleet

This topic applies to pod-manager-based Horizon pods. Such pods are based on the Horizon Cloud pod-manager technology. The Horizon Cloud pod-manager technology runs solely in a Microsoft Azure subscription and does not require a VMware SDDC. This pod type is different from a Horizon pod on VMware SDDC type, which is based on Horizon Connection Server software components.

You add a pod-manager-based pod to your environment by using the automated pod deployment wizard directly from the Horizon Cloud Administration Console. The wizard deploys the required VMware software components into your Microsoft Azure cloud subscription. The deployed VMware software creates an appropriately configured entity, called a pod, which pairs with the control plane. After the pod is deployed, then you use the control plane to provision VDI desktops and RDSHs, and entitle access to desktops and remote applications to your end users.

About Deploying a Pod-Manager-Based Pod

The pod deployed by Horizon Cloud into Microsoft Azure has a physical regional location in a Microsoft Azure cloud. In the pod deployment wizard, you select where to place the pod, according to the regions available for your particular Microsoft Azure subscription. You also select an existing virtual network (VNet) that the pod will use in your selected region. You have the option to deploy an external gateway configuration with the pod, with that external gateway’s resources deployed either into the same VNet as the pod or into a separate VNet that is peered with the pod’s VNet.

Note You preconfigure your Microsoft Azure environment with the pod VNet (and with the external gateway VNet if using that configuration option). You can either create in advance those subnets that the pod and external gateway configuration require, or let the pod deployer create the subnets during deployment. If you do not create the subnets in advance, the pod deployer creates the subnets as it deploys the required VMs and resources into your environment. If you choose to have the pod deployer create its required subnets, you have to know what IP address spaces you want to use for the pod’s subnets before you start the deployment wizard. If you choose to create the subnets in advance, you must ensure they meet certain requirements before you start the deployment process. For details about requirements when you create the subnets in advance, see In Advance of Pod Deployment, Create the Horizon Cloud Pod’s Required Subnets on your VNet in Microsoft Azure and When Using Existing Subnets for a Horizon Cloud Pod in Microsoft Azure.
You can deploy more than one pod into Microsoft Azure and manage all of them from the same administrative console. The pods you deploy after the first one can reuse the same VNet as your first pod or use different VNets. Also, each pod can be in a different Microsoft Azure region, using a VNet in each region.

**Important**  This pod in Microsoft Azure is not a tenant. This pod does not adhere to the exact same set of characteristics that defines a tenant and which you would expect from a tenant. For example, even though a tenant would have a one-to-one mapping to an Active Directory domain and be isolated from other tenants, all of the Horizon Cloud pods in Microsoft Azure that are deployed using the same Horizon Cloud customer account record need to be able to reach the same Active Directory servers and the DNS configuration needs to resolve all of those Active Directory domains.

To do multi-tenancy, you would set up multiple Horizon Cloud customer account records. The Horizon Cloud customer account record, which is created when you registered with VMware to use the Horizon Cloud Service and is associated with your My VMware credentials, is more like a tenant. A Horizon Cloud customer account record is isolated from other Horizon Cloud customer account records. A single customer account record maps to multiple pods, and when someone uses any of the account credentials associated with that customer account record to log in to the administrative console, the console reflects all of the pods that are mapped to that customer account record.

The pod deployment process automatically creates a set of resource groups in your Microsoft Azure capacity. Resource groups are used to organize the assets that the environment needs and creates, such as:

- VMs for the pod's manager instance (multiple VMs for a pod that is enabled for high availability)
- VMs for the Unified Access Gateway instances and their load balancers
- VM for the connector VM in the external gateway configuration when you deploy that configuration in a VNet separate from the pod's VNet
- VMs for the RDSH-capable golden images
- VMs for the VDI desktop golden images
- VMs for the assignable (published, sealed) images that are made from the golden images
- VMs for the RDSH farms that provide the RDSH desktops and remote applications
- VMs for the VDI desktops
- Additional assets that the VMs and the environment require for supported operations, such as network interfaces, IP addresses, disks, key vaults, Microsoft Azure Database for PostgreSQL server resource, and various items along those lines. The pod deployment process can create the required virtual subnets also, using the values you specify in the deployment wizard.
The following diagram illustrates a deployed pod that is enabled for high availability, has both the external and internal types of gateway configurations, and where the external gateway resides in the same VNet as the pod itself. In this diagram, RG means resource group. The Unified Access Gateway instances in the external gateway configuration have NICs on the demilitarized (DMZ) network. With an external gateway configuration, you can have your end users located in the Internet, outside your corporate network, accessing their pod-provisioned virtual desktops and applications through that configuration. With an internal gateway configuration, you can have your end users located in your intranet, inside your corporate network, making trusted connections to their pod-provisioned virtual desktops and applications through that gateway. The pod deployment wizard provides the option to deploy the pod with both configurations up front. Alternatively, you can deploy the pod with only one gateway configuration or with none at all, and edit the deployed pod to add the non-chosen gateway configuration later.

You can also choose not to enable the high availability option in the deployment wizard, and then edit the deployed pod later to enable high availability on it. Starting in this release, a new pod is always deployed with a Microsoft Azure Database for PostgreSQL server resource and a pod load balancer, even when you do not enable the high availability option in the wizard. Having those resources available allows for enabling high availability on an already deployed pod. The second pod manager VM is only deployed when high availability is enabled on the pod. For more information, see the High Availability and Your Horizon Cloud Pod in Microsoft Azure documentation topic in the Administration Guide.
Figure 3-1. Illustration of the Horizon Cloud Pod Architecture for a Pod with High Availability Enabled and Configured with Both External and Internal Gateway Configurations, the External Gateway Deployed into the Same VNet as the Pod, Three NICs on the External Gateway VMs, Two NICs on the Internal Gateway VMs, and a Public IP Enabled for the External Gateway’s Load Balancer
The following diagram illustrates the resources that are deployed when you choose the option to have the external gateway residing in its own VNet, separate from the pod's VNet. The two VNets must be peered. This diagram also applies when you choose the option to have the external gateway's resources deployed using a Microsoft Azure subscription that is different than the one used for the pod. Because VNets cannot cross subscriptions, choosing to deploy the external gateway into its own subscription is a subset of choosing the external gateway to reside in its own VNet.

**Tip** Deploying the external gateway configuration into its own VNet gives you the ability to deploy these Horizon Cloud pods into complex Microsoft Azure environments that use hub-spoke network topology in Microsoft Azure.

**Figure 3-2. Illustration of the External Gateway's Architecture Elements When the External Gateway is Deployed into Its Own VNet, Separate from the Pod's VNet**

---

**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><strong>Useful Microsoft Azure References</strong></th>
<th><strong>Description</strong></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). <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>Hub-spoke network topology in Azure</td>
<td>Use this article to learn about hub-spoke network topology 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 deployed for a pod: the load balancer for the pod manager VMs and the load balancers for the gateway configurations.</td>
</tr>
<tr>
<td>What is Azure Database for PostgreSQL?</td>
<td>Use this article to learn about the Microsoft Azure Database for PostgreSQL service.</td>
</tr>
<tr>
<td>What is Windows Virtual Desktop?</td>
<td>Use this article to learn about Microsoft Windows Virtual Desktop and how it relates to Microsoft Windows 10 Enterprise multi-session and Microsoft Windows 7 Enterprise with Extended Security Updates. When your Horizon Cloud tenant account has the configuration for Horizon Cloud Service on Microsoft Azure extending Microsoft Windows Virtual Desktop, support is provided for using Microsoft Windows 10 Enterprise multi-session and Microsoft Windows 7 Enterprise with your pods deployed in Microsoft Azure.</td>
</tr>
</tbody>
</table>
Additional VMware Resources

The following resources provide in-depth technical details about the service.

<table>
<thead>
<tr>
<th>Additional VMware Technical Resources</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements Checklist</td>
<td>Use this checklist to learn about the assets you need to obtain and configure prior to beginning the pod deployment process.</td>
</tr>
<tr>
<td>Networking and Active Directory Considerations on Microsoft Azure with VMware Horizon Cloud</td>
<td>Use this article to learn about the various options and best practices for networking connections and using Microsoft Active Directory with your Horizon Cloud pods in Microsoft Azure.</td>
</tr>
<tr>
<td>Horizon Cloud Service on Microsoft Azure Security Considerations</td>
<td>Use this article to obtain information about the security details of the environment and the types of data stored.</td>
</tr>
<tr>
<td>Horizon Cloud on Microsoft Azure: RDS Desktop and App Scalability (technical paper download)</td>
<td>Use this article to gain insight from analyses on RDS desktop and remote application scalability and optimal user densities, as well as cost considerations related to farm deployment and power management settings.</td>
</tr>
</tbody>
</table>

High-Level Workflow for Adding a Horizon Pod on Microsoft Azure as Your First Pod to Your Horizon Cloud Tenant Environment

This is a high-level list of the steps when you are arriving at your very first cloud-connected pod by running the pod deployer to deploy a pod-manager-based pod into your Microsoft Azure subscription. This pod type is based on the VMware Horizon Cloud pod-manager technology (in contrast to a Horizon pod which is based on Horizon Connection Server software components). 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. When your customer account is configured to use App Volumes features with your pods in Microsoft Azure,
you can also provision applications from those App Volumes features and entitle those to your end users.

**Important** This workflow below is not applicable for a Horizon pod on Azure VMware Solution (AVS). A Horizon pod on AVS is a Horizon pod on VMware SDDC, because AVS is a vSphere cluster, as described in the Microsoft documentation *Tutorial: Deploy an Azure VMware Solution private cloud in Azure* and a vSphere cluster is a VMware SDDC by definition of a VMware SDDC (software-defined data center). The following Tech Zone articles provide details about a Horizon pod on AVS: *Horizon on Azure VMware Solution Configuration* and *Horizon on Azure VMware Solution Architecture*.

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

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

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

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

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

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

4. Deploy the pod.

5. Register your Active Directory domain with the deployed pod, which includes providing the names of service accounts. Ensure these service accounts meet the requirements described in *Service Accounts That Horizon Cloud Requires for its Operations*.

6. Assign the appropriate roles to individuals in your organization for authenticating to and performing operations in the administrative console. There are two types of roles that are used in Horizon Cloud. See *Best Practices about the Two Types of Roles You Give to People to Use the Cloud-Based Console to Work in Your Horizon Cloud Environment*. 
In the rare, atypical situation where your tenant environment already has Horizon Cloud pods in Microsoft Azure that are running manifests older than manifest 1600.0, you must give the Horizon Cloud Super Administrators role to an Active Directory group that includes the domain join account as a member. See the topic Assign Horizon Cloud Administrative Roles to Active Directory Groups in the Administration Guide.

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

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

Related to the preceding step, if you select the single-pod broker configuration in that previous step and you plan to use Workspace ONE Access with the pod or you plan to have Horizon Clients connecting directly to the pod (not through a pod gateway configuration), then perform these steps:

- In your DNS server, map a fully qualified domain name (FQDN) to the pod manager's Microsoft Azure load balancer IP address
- Obtain an SSL certificate based on that mapped FQDN

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

**Attention**  When your environment is configured for single-pod brokering and you are integrating Workspace ONE Access with the pod, you must upload an SSL certificate to the pod and configure your Workspace ONE Access Connector to point to the pod, not to the pod's Unified Gateway Access configurations.

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

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

10 Upload an SSL certificate to the pod directly, using the pod's summary page in the administrative console, if you plan to have one or both of the use cases described in the preceding step. See Configure SSL Certificates on the Horizon Cloud Pod's Manager VMs.

**Tip**  If the only access use case you will ever want to support is where connections will go to the pod's Unified Access Gateway instances through the load balancer connected to those instances, then uploading the SSL certificate to the pod directly is superfluous. Still, performing the immediately preceding step above and this step here is a recommended practice, because it ensures that if you do one day give out that FQDN to users to enter in their Horizon Clients, those clients can have trusted connections. Performing the immediately preceding step and this one here also provides you the ability to one day more quickly integrate the pod in a single-pod-broker environment with Workspace ONE Access because you would have the FQDN mapped and the SSL certificate already in place on the pod.

11 Optional: If your Horizon Cloud tenant account is not already on-boarded with the VMware Cloud Services Engagement Platform, consider onboarding it now. Onboarding to the
VMware Cloud Services Engagement Platform is a prerequisite to activating the Horizon Infrastructure Monitoring features for your pods deployed in Microsoft Azure. See Onboard Your Horizon Cloud Tenant to VMware Cloud Services Engagement Platform Using the Cloud-Based Console.

12 Optional: Activate Horizon Infrastructure Monitoring. A prerequisite to this activation is that your Horizon Cloud tenant must be onboarded to the VMware Cloud Services Engagement Platform. See Horizon Infrastructure Monitoring and the Pods in Your Horizon Cloud Environment.

13 Import a base image. For the various ways of importing a base image, see Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure.

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

14 As described in Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure, depending on the method used to create the base image, the agent in the new image VM might not yet be paired with pod manager VM in which the VM was created. If you see a message that says the agent is not paired, use the Imported VM page's **Reset Agent Pairing** action to complete that pairing.

15 Depending on the type of end-user assignment the image is ultimately intended for, perform one or more of the following steps as appropriate.

- In an image VM that will be used for provisioning VDI desktops or native applications, install the third-party applications you want your end users to use in their VDI desktops, and configure other applicable customizations, such as setting desktop wallpaper, installing the NVIDIA GPU drivers (for GPU-enabled images), and so on. Also optimize the image for Microsoft Sysprep best practices, if not done as part of the import image process. See Customize the Image VM's Microsoft Windows Client Operating System, Install NVIDIA Graphics Drivers in a GPU-Enabled Image, and Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance.

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

- In a RDS-capable image that will be used for provisioning RDSH-based session desktops and remote applications, install the third-party applications you want to provide to your end users from that RDS image and configure other applicable customizations, such as setting desktop wallpaper, installing the NVIDIA GPU drivers (for GPU-enabled images), and so on. Also optimize the image for Microsoft Sysprep best practices, if not done as part of the import image process. If the imported VM is running one of the Microsoft Windows 10 Enterprise multi-session systems that includes Office 365 ProPlus by default,
you should verify the VM is configured for shared computer activation for Office 365 ProPlus as described in the Microsoft documentation topic Overview of shared computer activation for Office 365 ProPlus. If Office 365 ProPlus is not configured for shared computer activation in the imported VM, use the method described in that Microsoft document that is appropriate for your situation. See Customize the Image VM’s Microsoft Windows Server Operating System, Customize the Image VM’s Microsoft Windows 10 Enterprise Multi-Session Operating System, Install NVIDIA Graphics Drivers in a GPU-Enabled Image, and Five Key Steps to Take with Your Golden Images to Get Optimal Remote Experience Performance.

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

16 Convert that image into an assignable image, also known as sealing or publishing the image. See Convert a Configured Virtual Machine to an Assignable Image.

17 To provision session-based RDSH desktops and remote applications from a published server image:

a Create a desktops RDSH farm to provide session desktops, and then create assignments to entitle end users to use those desktops. See Create a Farm 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 Create a Farm, Import New Remote Applications from RDSH Farms, and Create a Remote Application Assignment.

18 To provision VDI desktops from a published VDI desktop image, create a dedicated or floating VDI desktop assignment. See About Desktop Assignments for Your Horizon Cloud Environment’s Pods in Microsoft Azure and its section about creating these desktop assignments.

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

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

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

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

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

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

After the pod is onboarded and you can access the Capacity page in the administrative console, navigate to the Capacity page to see the `vwm-hcs-ID-uag.region.cloudapp.azure.com` value needed to map your FQDN in your DNS. For details on how to locate the Microsoft Azure load balancer’s FQDN in the console, see Obtain the Pod Gateway’s Load Balancer Information to Map in Your DNS Server.

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

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

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

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

After the above workflow steps are completed, your end users can use the Horizon Client or Horizon HTML Access (the web client) to launch their entitled desktops and remote applications:

- In an environment configured with Universal Broker, by using your Universal Broker brokering FQDN in their client.
- In an environment configured with single-pod brokering, by using your FQDN in their client, the one you mapped using a CNAME record in your DNS.

You can find in-depth details on how to accomplish each workflow step in the topics that are linked from each step above.

### Preparing to Deploy a Horizon Cloud Pod on Microsoft Azure

Before you log in to the Horizon Cloud Administration Console and run the pod deployment wizard for the first time, you must perform these preparatory tasks. This pod deployment wizard deploys the pod-manager-based type of pod.

**Remember** This wizard deploys the pod-manager-based type of pod into Microsoft Azure. The console currently does not provide a deployment wizard to automate a Horizon pod in Azure VMware Solution (AVS), which uses the Horizon Connection Server technology. For information about deploying an Horizon pod in AVS, see Tech Zone's [Horizon on Azure VMware Solution Architecture](#) and [Deploying Horizon with Azure VMware Solution](#).

1. Fulfill the prerequisites described in the [VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist For New Pod Deployments - Updated As Appropriate for Pods That Deploy Starting From the January 2021 Service Release](#), especially:

   - Ensure your Microsoft Azure account and subscription encompasses the pod's required number and sizes of virtual machines, including the optional Unified Access Gateway configurations if you plan to deploy those. See Microsoft Azure Virtual Machine Requirements for a Horizon Cloud Pod in Microsoft Azure.

   If you plan to deploy the pod with an external gateway configuration that uses its own subscription, separate from the pod's subscription, ensure that other subscription encompasses the external gateway's required number and sizes of virtual machines. For this use case, that separate subscription will need its own VNet, because VNets do not span subscriptions. Also, this subscription must be in the same region as the pod's subscription because the supported VNet topology is connecting VNets within the same Microsoft Azure region.
- As described in the VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist For New Pod Deployments - Updated As Appropriate for Pods That Deploy Starting From the January 2021 Service Release:
  - Ensure that your subscription does not restrict use of Azure StorageV1 account type.
  - If you are not planning to specify custom resource tags in the pod deployment wizard, ensure that your subscription does not restrict creation of untagged resource groups or require specific tags on its resource groups.
  - Ensure that your subscription does not have Azure Policies on it that would block, deny, or restrict creation of the pod's components in that subscription.

  **Caution** The pod deployment process will fail early on if your subscription does not match those preceding items, because the first step of creating the temporary jump box's resource group and deploying the jump box will fail to complete. Therefore, if your pod deployment process times out after two hours, first check if your subscription has Azure Policies in place that would block, deny, or restrict creation of resource groups based on particular criteria.

- Ensure a virtual network (VNet) exists in the region in which you are going to deploy the pod and that virtual network meets the requirements for a Horizon Cloud pod. If you do not have an existing VNet, create one that meets the requirements. See Configure the Required Virtual Network in Microsoft Azure.

  If you plan to deploy the pod with an external gateway configuration that uses its own VNet, separate from the pod's VNet — or that uses its own subscription separate from the pod's subscription, ensure that VNet exists in the same region as the pod's VNet, and that it meets the Configure the Required Virtual Network in Microsoft Azure. For this use case, those two VNets must be peered.

  **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.

- If you want to manually create the subnets for the pod on your VNet in advance of deploying the pod, ensure that the required number of subnets is created on the VNet, that their address spaces meet the Configure the Required Virtual Network in Microsoft Azure, and that they are empty of resources. In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure.

  **Caution** These subnets you create on your VNet for a pod deployment must be empty. You can create the subnets prior to deploying the pod, but do not put any resources on those 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.
If you do not want to create the subnets in advance, the pod deployment process will create them using the CIDR information you enter into the on-screen wizard.

- Ensure that virtual network is configured to point to a valid Domain Name Services (DNS) server that is resolving external names. See Configure the DNS Server Settings Needed by the VNet Topology You Will Use for Your Horizon Cloud Pods in Microsoft Azure.

**Important** The pod deployment process requires external and internal name resolution. If the VNet points to a DNS server that cannot resolve external names, the deployment process will fail.

- If you plan to deploy the pod with an external gateway configuration into an existing resource group that you create in a subscription separate from the pod's subscription — instead of having the deployer auto-create that resource group — ensure that resource group exists in that subscription before you start the pod deployment wizard. Decide whether to set the permissions that Horizon Cloud needs at the resource-group level or at the subscription level. See Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions.

- Ensure you have an Active Directory setup that is supported for use with this release, your virtual network can reach it, and the DNS server can resolve its name. See Active Directory Domain Configurations.
Create the required number of service principals, according to your planned deployment options. If you are deploying the pod's external gateway configuration into its own subscription, then you need a service principal for that subscription as well as for the subscription used for the pod itself. For detailed steps, see Create the Required Service Principal Needed by the Horizon Cloud Pod Deployer by Creating an Application Registration.

**Important** Each service principal that you configure for Horizon Cloud's use must be assigned an appropriate role in that service principal's associated subscription. The role to a service principal must allow the actions that Horizon Cloud needs to operate on the Horizon Cloud managed resources in that service principal's associated Microsoft Azure subscription. The service principal for the pod's subscription needs a role that allows for actions to successfully deploy the pod, to operate on the pod and the pod-managed resources to fulfill the administrator workflows initiated using the administrative console, and to maintain the pod over time. When using a separate subscription for the pod's external Unified Access Gateway configuration, the service principal for that subscription needs a role that allows for actions to successfully deploy the resources needed for that gateway configuration, to operate on those Horizon Cloud-managed resources to fulfill the administrator workflows, and to maintain those gateway-related resources over time.

As described in Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions, the service principal must be granted access using one of the following methods:

- At the subscription level, assign the Contributor role. The Contributor role is one of the Microsoft Azure built-in roles. The Contributor role is described in Built-in roles for Azure resources in the Microsoft Azure documentation.

- At the subscription level, assign a custom role that you have set up to provide the service principal with Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions that Horizon Cloud needs for deployment of the pod-related resources and for ongoing administrator-initiated workflows and pod maintenance operations.

- When using a separate subscription for the external Unified Access Gateway configuration and deploying into an existing resource group, an valid combination is to grant access to the service principal to access that resource group and associated VNet using a role that provides narrow-scope permissions plus grant access for the service principal to access the subscription using the built-in Reader role.

Also, the role must be assigned directly to the service principal used for Horizon Cloud. The use of a group-based assignment of a role to the service principal — in which the role is assigned to a group and the service principal is a member in that group — is unsupported.

From the Microsoft Azure portal, for the pod's subscription and the subscription for its external gateway (if using that deployment option), get the values for the Microsoft Azure subscription ID, application ID, application authentication key, and Microsoft Azure AD Directory ID from the Microsoft Azure portal. These resources are used by Horizon Cloud to perform its operations in your Microsoft Azure subscription. See Subscription-Related Information for the Horizon Cloud Pod Deployment Wizard.
4 If you are deploying the pod with a Unified Access Gateway configuration, obtain the signed TLS/SSL server certificate that can allow your end users' clients to trust connections to the desktops and remote applications. This certificate should match your FQDN that your end users will use in their clients and be signed by a trusted Certificate Authority (CA). Also, all certificates in the certificate chain must have valid time frames, including any intermediate certificates. If any certificate in the chain is expired, unexpected failures can occur later in the pod onboarding process.

Unified Access Gateway presents your CA-signed certificate, so that the end users' clients can trust the connections. To support trusted access from the Internet, you deploy an external Unified Access Gateway configuration for the pod. To support trusted access within your corporate network, you use an internal Unified Access Gateway configuration. Both configuration types can be deployed during the initial pod deployment process or post-pod deployment using the Edit Pod workflow.

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

5 If your signed SSL server certificate that you will use with the Unified Access Gateway configuration is not in PEM format or is not a single PEM file containing the full entire certificate chain with the private key, convert the certificate information to the required PEM format. See the steps in [Convert a Certificate File to the PEM Format Required for Pod Deployment](#).

6 If you are not already registered for access to Horizon Cloud, verify that one of these two items is in place:

- Obtain a My VMware account and register Horizon Cloud access with that account.
- If your group or organization used the VMware Cloud Services Engagement Platform to register for Horizon Cloud or they registered for use of Horizon Cloud using VMware Cloud services or Workspace ONE, you would have received an invitation email with an activation link when they invited you to join their VMware Cloud services org space in, as described in the VMware Cloud services documentation topic [Add Users to Your Organization](#). If you received such an email, complete the email's instructions before trying to access Horizon Cloud.

After you have completed those preparatory tasks, use one of these two ways to access the Horizon Cloud environment:

- Enter My VMware credentials at cloud.horizon.vmware.com, when that specific account is registered for Horizon Cloud.
- Take the single sign-on with VMware Cloud Services path from cloud.horizon.vmware.com, when Horizon Cloud is registered for your use through your group's org as described in the preceding paragraph.
After logging in, you'll see the Add Cloud Capacity area on the screen and can click Manage > Add Pod to start the pod deployment wizard. Complete the wizard by entering the required information in each screen. For detailed steps, see Using the Horizon Cloud Administration Console to Perform an Automated Deployment of a Pod into Microsoft Azure.

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

**Microsoft Azure Virtual Machine Requirements for a Horizon Cloud Pod in Microsoft Azure**

Pod deployments, deployments of the pod's gateway configurations, and standard operations require specific types and sizes of virtual machines (VMs) in your Microsoft Azure cloud capacity. Your subscription needs the appropriate quotas and configuration to support these VMs. When you are using the option to deploy the pod's external gateway in a separate subscription, that subscription needs the quota and configuration to support that external gateway configuration. When you activate the Horizon Infrastructure Monitoring feature for a pod in Microsoft Azure, your pod's subscription needs the appropriate quota and configuration to support deployment of the Horizon Edge Virtual Appliance into that subscription.

**Important**  The pod deployment wizard validates that your Microsoft Azure environment has sufficient quota of cores to build the pod and the gateway configuration you specified, if any. If the wizard determines there is not sufficient quota given the subscription information you specified in the wizard, an on-screen message will display and the wizard will not proceed to its next step.

Starting with the September 2019 release's pod manifest version, both for pods newly deployed at that version and pods updated to that version, each pod has a Microsoft Azure load balancer and Microsoft Azure Database for PostgreSQL server. When a pod is updated to the September 2019 manifest or later versions, the updated pod include a Microsoft Azure load balancer and Microsoft Azure Database for PostgreSQL server. The Microsoft Azure Database for PostgreSQL server is deployed using the Single Server deployment.

**Note**  GPU-enabled VMs are only available in some Microsoft Azure regions. See Microsoft Azure Products by region for details.

In the tables below, the VM specification column provides:

- The series names that are used in the Microsoft Azure documentation
- The vCPUs family names that are used in the quotas displayed in the Microsoft Azure portal
- The specific name of the VM type from that family
To see a subscription’s current quotas in the Microsoft Azure portal, navigate to All services > Subscriptions, click the subscription, and then click Usage + quotas. For more information about sizes for Microsoft Windows virtual machines in Microsoft Azure, see this topic and its subtopics in the Microsoft Azure documentation: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes.

Jump Box VMs

Jump box VMs are temporarily created in your Microsoft Azure subscriptions for the purposes described in the tables below.

Table 3-3. Pod Jump box VM Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>Microsoft Azure VM Specification</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump box</td>
<td>Linux Standard F Family: Standard_F2 (2 cores, 4 GB memory) OS disk: Standard HDD 30 GiB</td>
<td>1 per pod</td>
<td>A VM created in your Microsoft Azure environment and used during the initial pod creation, and during subsequent software updates on the environment. One jump box VM for each pod you deploy. This jump box VM is deleted automatically when the pod creation or update process is finished and the VM is no longer needed.</td>
</tr>
</tbody>
</table>

**Note** A jump box VM is newly deployed for creating a pod, for building out an update’s green components when the next version of the pod software is available, for orchestrating the blue/green update process on the pod, and for the process of adding a gateway configuration to an existing pod.

Table 3-4. When Having the External Gateway in a Separate VNet: Jump box VM Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>Microsoft Azure VM Specification</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jump box</td>
<td>Linux Standard F Family: Standard_F2 (2 cores, 4 GB memory) OS disk: Standard HDD 30 GiB</td>
<td>1 per pod</td>
<td>When optionally deploying the external gateway in its own VNet or own subscription, it needs a jump box VM separate from the jump box VM used for the pod’s own core resources. This jump box VM is created in your Microsoft Azure environment in a separate resource group from the pod’s jump box VM, and is used during the initial deployment of the external gateway configuration, and during subsequent software updates on that external gateway. One jump box VM for each external gateway in its own VNet or subscription that you deploy. This jump box VM is deleted automatically when the external gateway deployment or update process is finished and the VM is no longer needed.</td>
</tr>
</tbody>
</table>

**Note** A jump box VM is newly deployed for creating one of these external gateways in its own VNet or subscription (during pod creation or when using the Edit Pod workflow to add the external gateway to an existing pod), for building out an update’s green components for that external gateway when the next version of the external gateway or pod software is made available to you, for orchestrating the blue/green update process on that external gateway.
Pod Manager VMs

These VMs are generally considered the heart of the pod itself. The pod manager VMs are responsible for facilitating the connection of the end-user clients to the Horizon agent software running in the pod-provisioned virtual desktops.
### Table 3-5. Pod Management VM Requirements - For the Pod's Core VMs, Not Including Gateway Configurations

<table>
<thead>
<tr>
<th>VM</th>
<th>Microsoft Azure VM Specification</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
</table>
| Pod without high availability enabled: Pod management instances | Linux - Standard Dv3 Family: Standard_D4_v3 (4 cores, 16 GB memory). OS disk: Standard HDD 30 GiB | 1 per pod during steady-state operations  
2 per pod during the end-to-end time for the pod's blue/green update process. | For a pod without high availability enabled, during steady-state operations, one VM exists, is powered on, and runs the pod. When a new pod manifest is made available to you by VMware Operations, and the system begins building out the green components for the pod's blue/green update process, a second instance is created and powered on. As part of the end-to-end update process, you schedule the time at which the system switches to using the green components. After the switch is completed, the pod is using the newly created VM for steady-state operations and the previously used one in the blue component set is stopped and then deleted. Your environment's size must accommodate the two pod manager instances running side-by-side for the end-to-end update time period starting from the time when the system starts building out the pod's green components for the blue/green update process, to when update activities are completed and the pod is switched over to using the new green components. See the Administration Guide for a description of the pod's blue/green update process. |
4 per pod during the end-to-end time for the pod's blue/green update process. | For a high-availability-enabled pod, during steady-state operations, two VMs exist, are powered on, and run the pod. When a new pod manifest is made available to you by VMware Operations, and the system begins building out the green components for the pod's blue/green update process, a second instance per pod manager VM is created and powered on. At that time, the total running pod manager VMs is four (4). As part of the end-to-end update process, you schedule the time at which the system switches to using the green components. After the switch is completed, the pod is using the two newly created VM for steady-state operations and the previously used two in the blue component set are stopped and then deleted. Your environment's size must accommodate the four pod manager instances running side-by-side for the end-to-end update time period starting from the time when the system starts building out the pod's green components for the blue/green update process, to when update activities are completed and the pod is |
Table 3-5. Pod Management VM Requirements - For the Pod’s Core VMs, Not Including Gateway Configurations (continued)

<table>
<thead>
<tr>
<th>VM</th>
<th>Microsoft Azure VM Specification</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>switched over to using the new green components. See the Administration Guide for a description of the pod’s blue/green update process.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Gateway-Related VMs

Gateway-related VMs are:

- The Unified Access Gateway instances configured to function as secure gateways for the end-user clients accessing the pod-provisioned resources.
- When you deploy the external gateway into a separate VNet, the gateway connector VM that handles the cloud management operations on that external gateway configuration.

**Note** Starting with the July 2020 quarterly release, you can choose from a list of supported VM models for the Unified Access Gateway instances when you are deploying a brand new gateway — either at the time of deploying the whole pod or when adding a new gateway. Prior to the July 2020 release, the gateway instances were required to use the Standard_A4_v2 VM model. The list of supported VM models that you can choose from in the on-screen wizard will depend on which VM models are available in the Microsoft Azure region into which you are deploying the gateway instances. The displayed choices will also depend on your VM quota in the Microsoft Azure subscription that you are using for the gateway deployment. The pod deployment wizard’s VM Model menu will dynamically reflect the VM models that meet those requirements.

Software updates will maintain the gateway instances’ VM models. Whatever the gateway instances’ VM model is prior to a pod update will be their VM model after the update.
### Table 3-6. Unified Access Gateway VM Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>Microsoft Azure VM Specification</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Access Gateway</td>
<td>Starting in this release, you can choose from the following VM models for new gateway deployments.</td>
<td>Varied based on whether you choose to have an external or internal Unified Access Gateway configuration, or both types for the same pod.</td>
<td>Unified Access Gateway is an optional feature that is deployed for your pod when you configure the gateway settings in the deployment wizard. If you decide to have Unified Access Gateway instances for the pod, your environment must accommodate these instances running during the pod’s end-to-end blue/green update process. The number of steady-state instances depends on whether you choose to have both external and internal Unified Access Gateway configurations. When you have only an external or only an internal Unified Access Gateway configuration, during steady-state operations, two instances exist, are powered on, and provide the Unified Access Gateway capabilities. During an update process, two additional instances are created and powered on to run the software updates on Unified Access Gateway. After the update is completed, the pod migrates to using the newly created VMs and the previously used ones in the blue component set are stopped and then deleted. When you have both internal and external Unified Access Gateway configurations, during steady-state operations, four instances exist, are powered on, and provide the Unified Access Gateway capabilities. Two instances provide the capabilities for the external configuration and two instances provide the capabilities for the internal configuration. During an update process, two additional instances per configuration are created and powered on to run the software updates on Unified Access Gateway. After the update is completed, the pod migrates to using the newly created VMs and the previously used ones in the blue component set are stopped and then deleted. Your environment’s size must accommodate the indicated Unified Access Gateway instances running side-by-side for the end-to-end update time period starting from the time when the system starts building out the pod’s green components for the blue/green update process, to when update activities are started.</td>
</tr>
<tr>
<td>instances</td>
<td>- Linux Standard Av2 Family:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Standard_A4_v2 (4 cores, 8 GB memory), OS disk: Standard HDD 20 GiB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Linux Standard F5v2 Family:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Standard_F8s_v2 (8 cores, 16 GB memory), OS disk: SSD 32 GiB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For an external-only or an internal-only configuration.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 2 per pod during steady-state operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 4 per pod during the end-to-end time for pod-related blue/green update activities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For a pod with both an external and internal Unified Access Gateway configuration,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 4 per pod during steady-state operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 8 per pod during the end-to-end time for pod-related blue/green update activities.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3-6. Unified Access Gateway VM Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>Microsoft Azure VM Specification</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>completed and the pod is switched over to using the new green components. See the Administration Guide for a description of the pod's blue/green update process.</td>
</tr>
</tbody>
</table>

Table 3-7. When Having the External Gateway in a Separate VNet: Gateway Connector VM Requirements

| VM                                      | Microsoft Azure VM Specification | Quantity | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|----------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|                                                                                                                                                                                                                                                                                                                                 |
| Gateway Connector instance              | Linux Standard Av2 Family:       | 1 per this external-gateway type during steady-state operations 2 per this external-gateway type during the end-to-end time for pod-related blue/green update activities.                                                                                     | When the external gateway is deployed into a separate VNet, this VM is created and used for the cloud management operations on that external gateway configuration. During an update process, an additional instance is created and powered on to run the software updates on the Unified Access Gateway in the external gateway configuration. After the update is completed, migration to the newly created VM occurs and the previously used one is stopped and then deleted. If you decide to use this optional configuration, your environment must accommodate these instances running end-to-end during the pod-related blue/green update activities. |                                                                                                                                                                                                                                                                                                                                 |
|                                         | Standard_A1_v2 (1 cores, 2 GB memory) | 1 per this external-gateway type during steady-state operations 2 per this external-gateway type during the end-to-end time for pod-related blue/green update activities.                                                                                     | When the external gateway is deployed into a separate VNet, this VM is created and used for the cloud management operations on that external gateway configuration. During an update process, an additional instance is created and powered on to run the software updates on the Unified Access Gateway in the external gateway configuration. After the update is completed, migration to the newly created VM occurs and the previously used one is stopped and then deleted. If you decide to use this optional configuration, your environment must accommodate these instances running end-to-end during the pod-related blue/green update activities. |                                                                                                                                                                                                                                                                                                                                 |
|                                         | OS disk: Standard HDD 10 GiB      |          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                 |

**Golden Image VMs**

A golden image is a Microsoft Windows operating system VM that is configured so that Horizon Cloud can convert it into a published image. Sometimes you'll see these VMs referred to as gold patterns.
## Table 3-8. Image VM Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>Microsoft Azure VM Specification</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Golden images</td>
<td>For GPU-enabled golden images, the system uses:</td>
<td></td>
<td>A golden image is a Microsoft Windows operating system VM that is configured so that Horizon Cloud can convert it into a published image. An RDSH-capable Windows operating system VM provides the base used to create the RDSHs in farms that provide session-based desktops and remote applications to your end users. A Windows client operating system VM provides the base used to create the VDI desktops. Each golden image is a combination of Microsoft Windows operating system and whether it is GPU-enabled or not. So if you want your pod to provide: RDSH desktops using Microsoft Windows 2016 Datacenter, no GPU RDSH desktops using Microsoft Windows 2016 Datacenter, with GPU Then you need at least 2 golden image VMs. The process of converting a golden image into a published image is sometimes called publishing the image, or also called sealing the image. The resulting published image is sometimes called a sealed image or an assignable image, because it is in a finalized state for use in assignments. The system automatically powers off the golden image when it is published (when you perform the <strong>Convert to Image</strong> action on the golden image in the administrative console). When you update a published image, the system powers the VM on again. <strong>Note</strong> When you duplicate an image using the console, the system temporarily powers on the golden image’s VM to obtain its configuration for the duplicate, and then powers it off again. For information about how to create a golden image, see the topic Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure in the Administration Guide.</td>
</tr>
<tr>
<td>Golden images</td>
<td>- The NV-series NV6 Standard (from the Standard NV Family vCPUs)</td>
<td>Varied,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- OS disk: Standard HDD 127 GiB</td>
<td>based on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For non-GPU-enabled golden images and Microsoft Windows RDSH-capable operating systems, the system uses:</td>
<td>your needs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- The Standard_D4_v3 (from the Standard Dv3 Family vCPUs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- OS disk: Standard HDD 127 GiB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If Microsoft does not provide the Dv3-series in the Microsoft Azure region where you deployed the pod, the system uses the Standard_D3_v2 instead from the Standard Dv2 Family.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For non-GPU-enabled golden images and Microsoft Windows operating system VM that is configured so that Horizon Cloud can convert it into a published image. An RDSH-capable Windows operating system VM provides the base used to create the RDSHs in farms that provide session-based desktops and remote applications to your end users. A Windows client operating system VM provides the base used to create the VDI desktops. Each golden image is a combination of Microsoft Windows operating system and whether it is GPU-enabled or not. So if you want your pod to provide: RDSH desktops using Microsoft Windows 2016 Datacenter, no GPU RDSH desktops using Microsoft Windows 2016 Datacenter, with GPU Then you need at least 2 golden image VMs. The process of converting a golden image into a published image is sometimes called publishing the image, or also called sealing the image. The resulting published image is sometimes called a sealed image or an assignable image, because it is in a finalized state for use in assignments. The system automatically powers off the golden image when it is published (when you perform the <strong>Convert to Image</strong> action on the golden image in the administrative console). When you update a published image, the system powers the VM on again. <strong>Note</strong> When you duplicate an image using the console, the system temporarily powers on the golden image’s VM to obtain its configuration for the duplicate, and then powers it off again. For information about how to create a golden image, see the topic Creating Desktop Images for a Horizon Cloud Pod in Microsoft Azure in the Administration Guide.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- The Standard_D2_v3 (from the Standard Dv3 Family vCPUs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- OS disk: Standard HDD 127 GiB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If Microsoft does not provide the Dv3-series in the Microsoft Azure region where you deployed the pod, the system uses the Standard_D2_v2 instead from the Standard Dv2 Family.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Farm VMs

RDSH farm VMs are the RDS-capable instances that provide session-based desktops and remote applications to your end users. You need at least one RDSH farm to deliver session desktops and one RDSH farm to deliver remote applications. To meet administrator or end-user needs, you can decide to deploy additional farms.

**Note** In the current service release, you cannot deliver both session-based desktops and remote applications from the same farm.
### Table 3-9. Farm VM Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>Microsoft Azure VM Specification</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDSH farm</td>
<td>You can customize the set of Microsoft Azure VM types that you want available for selection when creating farms in your pod. You can customize your own list from the set of Microsoft Azure VM sizes that are generally available in the standard Microsoft Azure regions. For more information about customizing the set of VM types available to use in your farms, see the Horizon Cloud Administration Guide. When creating or editing a farm, you can customize the OS disk size of the farm’s RDSH instances to change it from the system default value. For specific details about the Windows VM sizes that are generally available in the standard Microsoft Azure regions, see the Microsoft documentation at <a href="https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes">https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes</a>. Note: For production environments, ensure the VM types you use for your farms have a minimum of two (2) CPUs. Meeting this criteria avoids unexpected end-user connection issues. This criteria is a result of the Horizon Agent recommendations to have a minimum of 2 CPUs to install or update Horizon Agent from version 7.x or later. This Horizon Agent criteria is stated in the Horizon product documentation starting at version 7.8 (the references to a 2 CPU minimum starts with this version 7.8 of Install Horizon Agent on a Virtual Machine).</td>
<td>Varied, based on your needs and how you have customized the VM sizes in your Horizon Cloud environment.</td>
<td>The power state of these VMs varies, depending on the farm configuration settings and the end-user demand.</td>
</tr>
</tbody>
</table>
VDI Desktop VMs
VDI desktop VMs are the instances that provide VDI desktops to your end users.

**Note**  A new feature in the July 2020 quarterly service release is the use of App Volumes features with pods in Microsoft Azure. When you use the console's App Volumes capture process to add native applications to your Horizon Cloud inventory, the system creates a VDI desktop assignment of two VMs to support the capture process. The VM type used for this system-generated assignment is the same model as is used for the published image you selected in the console for the application capture process.
### Table 3-10. VDI Desktop VM Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>Microsoft Azure VM Specification</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDI desktops</td>
<td>You can customize the set of Microsoft Azure VM types that you want available for selection when creating VDI desktop assignments in your pod. You can customize your own list from the set of Microsoft Azure VM sizes that are generally available in the standard Microsoft Azure regions. For more information about customizing the set of VM types available to use in your VDI desktop assignments, see the <em>Horizon Cloud Administration Guide</em>.</td>
<td>Varied, based on your needs and how you have customized the VM sizes in your Horizon Cloud environment.</td>
<td>The power state of these VMs varies, depending on the VDI desktop assignment settings and the end-user demand.</td>
</tr>
</tbody>
</table>

**Note** A small set of Microsoft Azure VM sizes that Microsoft has determined are not appropriate for VDI use cases are automatically omitted from use, such as Standard_B2ls and Standard_B1s.

When creating or editing a VDI desktop assignment, you can customize the OS disk size of the VDI desktop instances to change it from the system default.
Table 3-10. VDI Desktop VM Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>Microsoft Azure VM Specification</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For specific details about those Windows VM sizes, see the Microsoft documentation at <a href="https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes">https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes</a>. Note For production environments, ensure the VM types you use for your VDI desktop assignments have a minimum of two (2) CPUs. Meeting this criteria avoids unexpected end-user connection issues. This criteria is a result of the Horizon Agent recommendations to have a minimum of 2 CPUs to install or update Horizon Agent from version 7.x or later. This Horizon Agent criteria is stated in the Horizon product documentation starting at version 7.8 (the references to a 2 CPU minimum starts with this version 7.8 of Install Horizon Agent on a Virtual Machine).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Horizon Edge Virtual Appliance

This appliance is created in a pod's Microsoft Azure subscription when you use the Horizon Cloud Administration Console to activate Horizon Infrastructure Monitoring on that pod.

Table 3-11. Horizon Edge Virtual Appliance Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>Microsoft Azure VM Specification</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Edge Virtual Appliance</td>
<td>Linux - Standard Dv3 Family: Standard_D4_v3 (4 cores, 16 GB memory). OS disk: Standard HDD 30 GiB</td>
<td>1 per pod</td>
<td>When the Horizon Infrastructure Monitoring feature is activated on a pod, this VM is created and used to collect the monitoring data and communicate that data to the Cloud Monitoring Service (CMS).</td>
</tr>
</tbody>
</table>

VMware Horizon Cloud Service on Microsoft Azure Service Limits

This topic describes some of the common VMware Horizon Cloud Service on Microsoft Azure limits, which are also called supported maximums. This topic currently describes the supported maximums on both the number of desktop and farm RDSH VMs you can deploy in a single
subscription and on the total number of concurrent connected sessions you can have per pod. Over time, this topic will be updated to list more of the known limits.

The service is tested up to a certain number of deployed VMs in a single subscription and the number of simultaneous connections that a pod can accommodate.

**Maximum of 2,000 desktop VMs and farm RDSH VMs per subscription**

This limit is based on Microsoft Azure API limits that are given on a single subscription. To work well within these API limits during standard operations, Horizon Cloud supports up to a maximum of 2,000 desktop VMs and farm RDSH VMs per subscription.

The 2,000 number per subscription includes VDI desktop VMs and farm RDSH VMs, and applies across all pods in the single subscription. For example, if you have one pod in your subscription, you might have up to 2,000 VDI desktops on that pod, or 1,950 VDI desktops plus 50 farm RDSH VMs. If you have more than one pod in your subscription, the number of VDI desktops and farms RDSH VMs across all of the pods must not total more than 2,000.

**Maximum of 2,000 sessions per pod**

Horizon Cloud supports running up to 2,000 concurrent connected sessions per pod. That 2,000 number includes connections to VDI desktops, RDS desktops, and RDS applications served by the pod. The pod’s session-handling capabilities determine this maximum.

**Configure the Required Virtual Network in Microsoft Azure**

Your Microsoft Azure environment must have an existing virtual network before you can deploy the Horizon Cloud pod into the environment. If you do not already have a virtual network (VNet) in the region into which you are deploying, you must create the virtual network. If you want to have the pod’s external gateway deployed into its own VNet — separate from the pod’s VNet, you must create that VNet also and then peer the two VNets. If you want to have the pod’s external gateway using its own subscription, separate from the pod’s, then you must create a separate VNet to use for that external gateway in that subscription and peer the two VNets. Because a single VNet does not span subscriptions, choosing to deploy an external gateway into its own subscription also will require the external gateway to use a VNet that is separate from and peered with the pod’s VNet.

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

<table>
<thead>
<tr>
<th>Subnet creation</th>
<th>Subnets needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>For this configuration, you can either create subnets in advance on the VNet and specify those in the pod deployment wizard, or directly type into the wizard the address spaces for the needed subnets and the pod deployer will create the subnets in the VNet.</td>
<td>Pod deployment using this configuration requires following subnets:</td>
</tr>
<tr>
<td><strong>Important</strong> If your existing VNet is peered, the deployer cannot automatically update the VNet’s address space. If the VNet is peered, the best practice is to create the subnets in advance as described in <strong>In Advance of Pod Deployment, Create the Horizon Cloud Pod’s Required Subnets on your VNet in Microsoft Azure</strong>. If you do not want to create the subnets in advance and you enter subnet CIDRs in the deployment wizard that are not contained within the VNet’s existing address space, the wizard will display an error message and you will need to specify valid subnet address spaces to proceed, or use an unpeered virtual network.</td>
<td>■ Management subnet, for IP addresses used by the VMs involved in management activities of the pod itself</td>
</tr>
<tr>
<td>■ Primary VM subnet — also known as the tenant subnet or the desktop subnet. This subnet provides IP addresses used for the RDSH server VMs and VDI desktop VMs on that subnet. When the internal Unified Access Gateway configuration is specified in the Pod deployment using this configuration requires following subnets:</td>
<td></td>
</tr>
</tbody>
</table>

- Management subnet, for IP addresses used by the VMs involved in management activities of the pod itself

- Primary VM subnet — also known as the tenant subnet or the desktop subnet. This subnet provides IP addresses used for the RDSH server VMs and VDI desktop VMs on that subnet. When the internal Unified Access Gateway configuration is specified in the Pod deployment using this configuration requires following subnets:
<table>
<thead>
<tr>
<th>Into which VNet are you deploying the external gateway?</th>
<th>Subnet creation</th>
<th>Subnets needed</th>
</tr>
</thead>
</table>

deployment wizard, the Unified Access Gateway VMs also consume IP addresses from this subnet.

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

- DMZ subnet, for IP addresses used by the optional external Unified Access Gateway configuration.

When you have the deployer automatically create the subnets, the deployer always creates the new subnets in the corresponding VNet.
<table>
<thead>
<tr>
<th>Into which VNet are you deploying the external gateway?</th>
<th>Subnet creation</th>
<th>Subnets needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>terms of the VNet's address space, the deployer handles the subnet address spaces you enter into the wizard as follows:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ If you specify address spaces in the wizard that are not already in the VNet's address space, the deployer automatically updates the VNet's configuration to add those address spaces. Then it creates the new subnets in the VNet.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ If the address spaces specified in the wizard are already contained within the VNet's existing address space, the deployer simply creates the new subnets in the VNet using the specified address spaces.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When deploying a pod with the choice to have the external gateway using its own VNet or subscription, separate from the pod's VNet or subscription:

For this configuration, because there are two VNets involved and these VNets must be peered, the best practice is to create the subnets in advance on the VNet and specify those in the pod deployment wizard. Create the subnets in advance as described in In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure. Even though the deployment wizard gives you the option of directly typing into the wizard the address spaces for the needed subnets to have the deployer create the subnets for you, if you specify address spaces that are not already in the VNet's address space, the deployer will not be able to add them to the VNet because it is a peered VNet. In this case, one VNet will have the subnets for the pod and one VNet will have the subnets for the external gateway. Those two VNets must be peered. Let's refer to the pod's VNet as VNet-1 and the external gateway's VNet as VNet-2. For each of these VNets, you can either specify the subnets in advance as described in In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure. Even though the deployment wizard gives you the option of directly typing into the wizard the address spaces for the needed subnets to have the deployer create the subnets for you, if you specify address spaces that are not already in the VNet's address space, the deployer will not be able to add them to the VNet because it is a peered VNet. In this case, one VNet will have the subnets for the pod and one VNet will have the subnets for the external gateway. Those two VNets must be peered. Let's refer to the pod's VNet as VNet-1 and the external gateway's VNet as VNet-2. For each of these VNets, you can either specify the

In this type of deployment, the pod's VNet (VNet-1) gets a management subnet and a desktop subnet, used for the same purposes as described for when the external gateway is in the pod's own VNet. However, the pod's VNet does not get a DMZ subnet in this configuration because the DMZ subnet would be used by the external Unified Access Gateway configuration, which is in the other VNet (VNet-2) in this configuration. In this deployment configuration, the external gateway's VNet gets the following subnets:

■ Management subnet, for IP addresses used by the VMs involved in management activities of the external gateway itself (the temporary jump box, the gateway's connector VM, and the external gateway's Unified Access Gateway instances)

■ Back-end subnet used by the external gateway's Unified Access Gateway instances

■ DMZ subnet used by the external gateway's Unified Access Gateway instances
Into which VNet are you deploying the external gateway?

<table>
<thead>
<tr>
<th>Subnet creation</th>
<th>Subnets needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>address spaces for the subnets that the pod deployer will automatically create or specify subnets that you have created in advance.</td>
<td></td>
</tr>
</tbody>
</table>

You perform these steps using the Microsoft Azure portal appropriate for your registered account. For example, there are specific portal endpoints for these Microsoft Azure clouds.

- Microsoft Azure Commercial (standard global regions)
- Microsoft Azure China
- Microsoft Azure US Government

Log in to the portal using the URL appropriate for your account.

Procedure

1. From the Microsoft Azure portal's left navigation bar, click **Virtual networks** and then click **Add**.

   The **Create virtual network** wizard appears, displaying its Basics step.

2. Follow the wizard's on-screen steps to specify the following information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription</td>
<td>Select the same subscription that you are planning to use when you deploy the pod.</td>
</tr>
<tr>
<td>Resource Group</td>
<td>You can either choose an existing resource group or have a new one created when the virtual network is created.</td>
</tr>
<tr>
<td>Name</td>
<td>Specify a name for the VNet.</td>
</tr>
<tr>
<td>Region</td>
<td>Select the same Microsoft Azure region into which you are planning to deploy the pod.</td>
</tr>
<tr>
<td>Address space</td>
<td>Specify the VNet's address space.</td>
</tr>
<tr>
<td>Subnet and Address range</td>
<td>Microsoft Azure requires creating one subnet when creating a VNet. You can either retain the default values or customize the name and range. If you want to use this subnet for one of the pod's required subnets, specify the appropriate address range according to the pod deployer requirements. As an example, if you want to use this subnet for the pod's tenant subnet, ensure it has an IP address range to match the /27 minimum that the deployment wizard requires. See In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure. Important If you use this subnet for one of the pod's required subnets, you cannot also use it for other resources.</td>
</tr>
</tbody>
</table>

Retain the default values for the optional settings.

3. Proceed to the review step and then click **Create**.
Results

The virtual network (VNet) is created in your Microsoft Azure account.

What to do next

If you are manually creating the required subnets instead of having the pod deployment process create them, configure the newly created VNet with the subnets you will use for the pod. See the steps in In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure and When Using Existing Subnets for a Horizon Cloud Pod in Microsoft Azure.

Configure the newly created VNet with a working DNS service and connectivity to the Active Directory service you will use with your pod. See the steps in Configure the DNS Server Settings Needed by the VNet Topology You Will Use for Your Horizon Cloud Pods in Microsoft Azure.

Ensure your VNet configuration, in terms of your firewalls and other network behavior, adheres to the pod deployment DNS, ports, and protocols requirements described in DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features and Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later.

**Important** The pod's temporary jump box VM and pod's manager VM require outbound Internet access on your Microsoft Azure VNet. If you are deploying an external gateway in its own VNet, that VNet must support the external gateway's temporary jump box and gateway connector VM having outbound Internet access. If you require proxy-based outbound Internet access, you will need to specify the proxy server information as you complete the fields in the pod deployment wizard.

In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure

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

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

- For the management subnet, a CIDR of /27 or more is required. This subnet is for IP addresses used by the VMs involved in management activities of the pod itself.

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

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

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

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

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

**Prerequisites**

Ensure your Microsoft region has the VNet that you plan to use for your pod. See [Configure the Required Virtual Network in Microsoft Azure](#).

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

**Procedure**

1. In the Microsoft Azure portal, navigate to the VNet for which you need to create the described subnets.

2. Click **Subnets**.

3. Click **+ Subnet**.

   The **Add subnet** screen appears.

4. Provide the information for the required fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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. If this subnet is going to be the management subnet, in the **Service endpoints** section, select the Microsoft.Sql service.

6. Click **OK**.

   The subnet is added to the VNet.

7. Repeat steps 3 through 5 to add the remaining required subnets.
8 If you are going to deploy the external gateway in its own VNet, repeat the steps for that VNet's subnets.

Results

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

What to do next

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

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

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

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

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

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

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

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

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

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

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

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

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

**Configure the DNS Server Settings Needed by the VNet Topology You Will Use for Your Horizon Cloud Pods in Microsoft Azure**

The VNets that your Horizon Cloud pods are deployed into must have the ability to resolve both internal machine names and external names. During the pod deployment process, the deployer securely downloads the pod software into your Microsoft Azure environment from external addresses in the Horizon Cloud control plane. The ability to resolve internal virtual machine (VM)
names is needed for the pod’s Horizon Cloud Active Directory domain-join operations with the VMs that get deployed in your Microsoft Azure environment.

Important Ultimately, the key requirement is that the pod-related VMs that need to reach specific DNS names are able to do that. That you have your VNet topology configured so that both internal machine names and external names can be resolved by the pod-related VMs that need to do that. You need to ensure that whatever VNet topology you are using in Microsoft Azure that you want to deploy the pod into will allow the pod VMs deployed onto the relevant required subnets can get that DNS name resolution. For specifics on the DNS resolution requirements, see DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features.

If you are going to use the feature to have the external gateway deployed into its own VNet separate from the pod's VNet, those VNets must be peered and you and your networking team must ensure that your peered VNets topology provides for that topology’s DNS settings to meet the pod's key DNS requirements, as described in the previous paragraph. The Horizon Cloud documentation set is not covering details of such advanced VNet topologies that your networking team might have customized for your use.

In a Microsoft Azure subscription, internal network connectivity is not set up by default. For production environments, you or your networking team would typically configure the virtual network’s DNS settings to point at a valid DNS server that can resolve external names as well as work in Microsoft Azure for your corporate machines. For example, you might want to deploy a Microsoft Windows Server 2016 virtual machine in that virtual network to act as the DNS server, and configure the virtual network’s DNS setting to point to the IP address of that deployed DNS server.

For proof-of-concept environments, if your organization's privacy and security policies allow, you can configure the internal DNS to delegate to an external public DNS for external name resolution. Some organizations and ISPs provide public recursive name servers to use for such purposes, such as OpenDNS at 208.67.222.222 or Google Public DNS at 8.8.8.8. For a sample list of public recursive name servers, see the Wikipedia article Public recursive name server.

Prerequisites

Ensure your Microsoft Azure region has the VNet topology that you plan to specify in the pod deployer wizard. See Configure the Required Virtual Network in Microsoft Azure.

Ensure that the DNS server settings that you or your networking team are going to configure for that VNet topology can reach and resolve the specific external names required for a successful pod deployment. For details, see DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features.

Procedure

1. From the Microsoft Azure portal's left navigation bar, click Virtual networks and then click the virtual network that you are going to use for your pod.
2 Display the virtual network’s DNS server settings by clicking **DNS servers**.

3 Using the **Custom** option, add the address of the DNS server you want to use for name resolution and click **Save**.

**What to do next**

Ensure the pod deployer's access requirements for DNS, ports, and protocols are met from your VNet topology. See [DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features](#) and [Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later](#).

**Active Directory Domain Configurations**

A Horizon Cloud environment requires registering at least one Active Directory (AD) domain with the Horizon Cloud pod. This topic describes the configurations that are supported for use with your Horizon Cloud pods in Microsoft Azure.

The supported configurations are:

- On-premises AD server and connecting that on-premises AD with your Microsoft Azure environment using VPN/MPLS or Microsoft Azure Express Route.
- AD server running in your Microsoft Azure environment.
- Using Microsoft Azure Active Directory Domain Services. For an overview of these services that Microsoft Azure provides, see this [Azure AD Domain Services article](#) in the Microsoft documentation.
For an in-depth technical description of each supported configuration, some options for each, and the advantages and disadvantages of each, see the VMware technical paper Networking and Active Directory Considerations on Microsoft Azure with VMware Horizon Cloud.

**Important** Your fleet of cloud-connected pods can consist of Horizon Cloud pods in Microsoft Azure along with Horizon pods installed in the VMware SDDCs (software-defined data centers) that are supported for such pods. As a result, all of those cloud-connected pods must have line of sight to the same set of Active Directory domains. If your pod fleet already consists of cloud-connected Horizon pods and you are deploying your first Horizon Cloud pod into Microsoft Azure, you must ensure that pod will be able to have line of sight to the Active Directory domains that are already registered with your Horizon Cloud environment. See all of the Active Directory-related topics linked from the Getting Started Using Your Horizon Cloud Environment topic for more details.

**DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features**

For successful end-to-end use of the service's features, you must ensure the Domain Name Service (DNS) names described in this documentation article are resolvable and reachable from the management and tenant subnets using the specific ports and protocols as indicated in this article's tables. The pod deployment process that instantiates a pod-manager-based pod into a Microsoft Azure subscription requires that the deployer-related appliances have access to specific DNS names over your selected VNet. Then after the pod is successfully instantiated in your subscription with its pod-related appliances up and running, various day-to-day service operations require network access to specific DNS names, as well as the pod update process for updating the pod's software when VMware makes the new software available to you. This article describes these DNS requirements.

**Some Overarching Key Points**

**About these required DNS names**

The Horizon Cloud pod deployer that automates the process to instantiate pod-manager-based pods and their associated gateways in your Microsoft Azure subscriptions requires network access to specific DNS addresses over those subscriptions' VNets. For the pod deployer to successfully instantiate the pod's components in your subscription, you must configure your firewalls to allow the key deployer-related appliances the network access they need to access those DNS addresses. Each DNS address's purpose is stated in the following tables. In addition to allowing network communication to those DNS addresses, your DNS configuration must resolve specific names as described in this article. When you choose the option to deploy the external gateway in its own VNet separate from the pod manager's VNet, that VNet's subnet must meet the same DNS requirements as the pod manager's VNet's management subnet.
The pod deployment process uses a jump box VM. This jump box VM has ports and protocol requirements for the pod deployment process, as well as for configuring settings for the pod’s Unified Access Gateway VMs when you are deploying a Unified Access Gateway configuration for the pod. See *Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates*.

Deploying the external gateway into its own VNet also uses its own jump box VM, separate from the pod’s. That jump box VM has its own ports and protocol requirements for the gateway deployment process. See *When the External Gateway is Deployed in its Own VNet: Ports and Protocols Required by the External Gateway Configuration’s Jump Box During Gateway Deployments and Updates*.

Besides the pod deployer and its workflows, various service features require access to specific DNS addresses for those features to work end to end. Those DNS names are also provided in the following tables.

Some of these DNS names have a regional element to them.

The activation of Horizon Infrastructure Monitoring on a pod will automatically instantiate the Horizon Edge Virtual Appliance in the pod manager’s VNet and management subnet. The Horizon Edge Virtual Appliance has its own DNS name requirements. Therefore, before you activate Horizon Infrastructure Monitoring on a pod, ensure you meet the DNS requirements of the Horizon Edge Virtual Appliance as indicated in the following tables.

**About ports and protocols after a pod is deployed, for ongoing service-related operations**

After a pod is successfully deployed, specific ports and protocols are required for ongoing Horizon Cloud operations. The specific ports and protocols required depends on whether the pod is at the manifest version for the September 2019 release, or is at a previous manifest version.

- For a pod created after the September 2019 release or updated to that release's manifest version or later, see *Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later*. Such pods have manifest versions of 1593 or later.

- For a pod created before the September 2019 release and not yet updated to that release's manifest version, see *Ports and Protocols Requirements for a Horizon Cloud Pod Deployed Prior to the September 2019 Release*. Such pods have manifest versions of 1493.1 or earlier.

**Regional Control Plane DNS Names**

Your Welcome to Horizon Service email will indicate which regional control plane instance your tenant account was created in. Due to a known issue that existed when the welcome email was sent to you, the email you received might display the system string names used for the regions instead of human-friendly names. If you see a system string name in your welcome email, you can use the following table to relate what is shown in your email with the regional control plane DNS names.
Table 3-12. Regions in Your Welcome Email Mapped to Regional Control Plane DNS Names

<table>
<thead>
<tr>
<th>Your welcome email says</th>
<th>Regional DNS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>cloud.horizon.vmware.com</td>
</tr>
<tr>
<td>EU_CENTRAL_1 or Europe</td>
<td>cloud-eu-central-1.horizon.vmware.com</td>
</tr>
<tr>
<td>AP_SOUTHEAST_2 or Australia</td>
<td>cloud-ap-southeast-2.horizon.vmware.com</td>
</tr>
<tr>
<td>PROD1_NORTHCENTRALUS2_CP1 or USA-2</td>
<td>cloud-us-2.horizon.vmware.com</td>
</tr>
<tr>
<td>PROD1_NORTHEUROPE_CP1 or Europe-2</td>
<td>cloud-eu-2.horizon.vmware.com</td>
</tr>
<tr>
<td>PROD1_AUSTRALIAEAST_CP1 or Australia-2</td>
<td>cloud-ap-2.horizon.vmware.com</td>
</tr>
<tr>
<td>Japan</td>
<td>cloud-jp.horizon.vmware.com</td>
</tr>
<tr>
<td>UK</td>
<td>cloud-uk.horizon.vmware.com</td>
</tr>
</tbody>
</table>

For the regional DNS addresses listed in the following tables for the Horizon Edge Virtual Appliance, those addresses use the same regions as the regional control plane DNS names.

DNS Requirements for the Overarching Pod Deployment Process, Pod Updates, Activation of Various Service Features, and Ongoing Operations

For successful end-to-end use of the service's features, you must ensure the following DNS names are resolvable and reachable from the management and tenant subnets using the specific ports and protocols as indicated in the following tables. Some of the service features that require the ability to reach specific DNS names are:

- The pod deployer that automatically deploys a pod-manager-based Horizon pod into your Microsoft Azure subscription
- The pod update feature, that updates the pod's software to a more recent software version
- The import-image process that uses the Import from Marketplace wizard
- The agent-related features, such as automated agent update (AAU)
- Universal Broker
- Horizon Infrastructure Monitoring and its Horizon Edge Virtual Appliance
- Features related to the Cloud Management Service (CMS)

**Most especially for pod deployment, pod updates, and when activating the Horizon Infrastructure Monitoring on a pod**

You must ensure the following DNS names are resolvable and reachable from the management and tenant subnets using the specific ports and protocols as indicated in the following tables. The appliances used in these workflows use specific outbound ports to securely download the software that these processes need into your Microsoft Azure environment. Those DNS names are also used so that the appropriate workflow-related appliances can communicate with the cloud control plane.
For new pod deployments, you must configure your network firewall, network security group (NSG) rules, and proxy servers such that the key deployment-related appliances have the ability to contact the DNS addresses on the ports that they requires. Otherwise, the pod deployment process will fail.

Activating Horizon Infrastructure Monitoring on a pod will instantiate the Horizon Edge Virtual Appliance into the same VNet and management subnet as that pod’s pod-manager appliances. You must ensure the configuration your network firewall, NSG rules, and proxy servers allows the Horizon Edge Virtual Appliance to contact the DNS addresses on the ports that it requires. Otherwise, deployment of that appliance will fail.

**When you are using the feature to deploy the external gateway into its own VNet**

The management subnet in that VNet must meet the same DNS requirements as stated in the table below for the management subnet in the pod’s VNet. The external gateway VNet’s back-end subnet and DMZ subnet do not have specific DNS requirements.

**When you are deploying the pod with either an external gateway, an internal gateway, or both**

You must upload a certificate that the pod deployer will configure in those gateway configurations. If the certificate or certificates that you supply for this purpose use CRLs (Certificate Revocation Lists) or OCSP (Online Certificate Status Protocol) settings that refer to specific DNS names, then you must ensure outbound Internet access on the VNet to those DNS names is resolvable and reachable. During configuration of your supplied certificate in the Unified Access Gateway gateway configuration, the Unified Access Gateway software will reach out to those DNS names to check the certificate’s revocation status. If those DNS names are not reachable, pod deployment will fail during its Connecting phase. These names are highly dependent on the CA that you used to obtain the certificates, and therefore are not in VMware’s control.

**DNS Requirements for New Pod Deployment, Pod Updates, and Service Operations that Apply on a Tenant-Wide Basis**

The following table describes the DNS requirements for a new pod deployment, pod updates, and service operations that are applicable on a tenant-wide basis. For Horizon Infrastructure Monitoring activation and Horizon Edge Virtual Appliance DNS requirements, see the section after this one. Because the Horizon Infrastructure Monitoring feature is activated on a per-pod basis, its DNS requirements warrant their own descriptive table.
Table 3-13. DNS Requirements for New Pod Deployment, Pod Updates, and Service Operations that Apply on a Tenant-Wide Basis

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>One of the following names, depending on which regional control plane instance is</td>
<td>443</td>
<td>TCP</td>
<td>Regional control plane instance</td>
</tr>
<tr>
<td></td>
<td>specified in your Horizon Cloud tenant account. The regional instance is set when</td>
<td></td>
<td></td>
<td>- United States: cloud.horizon.vmware.com, cloud-us-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>the account is created, as described in Deployments and Onboarding to Horizon Cloud</td>
<td></td>
<td></td>
<td>- Europe: cloud-eu-central-1.horizon.vmware.com, cloud-eu-2.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud.horizon.vmware.com</td>
<td></td>
<td></td>
<td>- Japan: cloud-jp.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-us-2.horizon.vmware.com</td>
<td></td>
<td></td>
<td>- United Kingdom: cloud-uk.horizon.vmware.com</td>
</tr>
<tr>
<td></td>
<td>- cloud-eu-central-1.horizon.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- cloud-eu-2.horizon.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- cloud-ap-southeast-2.horizon.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- cloud-ap-2.horizon.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- cloud-jp.horizon.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- cloud-uk.horizon.vmware.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>softwareupdate.vmware.com</td>
<td>443</td>
<td>TCP</td>
<td>VMware software package server. Used for downloading updates of the agent-related software</td>
</tr>
<tr>
<td></td>
<td>Used for downloading updates of the agent-related software used in the system's image-</td>
<td></td>
<td></td>
<td>used in the system's image-related operations.</td>
</tr>
<tr>
<td>Subnet Source</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>
</tbody>
</table>
| Management   | One of the following names, depending on which of the regional DNS names apply to your account.  
  - d1mes20qfad06k.cloudfront.net  
  - hydra-softwarelib-cdn.azureedge.net | 443  | TCP      | Horizon Cloud content delivery server. On the management subnet, this site is used for downloading the VHDs (virtual hard disks) for the pod’s manager and Unified Access Gateway VMs. Also used for the VHD for the gateway connector VM, in the case where the external gateway is in its own VNet)  
  d1mes20qfad06k.cloudfront.net corresponds to regional instances for cloud.horizon.vmware.com, cloud-eu-central-1.horizon.vmware.com, cloud-ap-southeast-2.horizon.vmware.com, cloud-ap-2.horizon.vmware.com, cloud-jp.horizon.vmware.com, cloud-uk.horizon.vmware.com  
Table 3-13. DNS Requirements for New Pod Deployment, Pod Updates, and Service Operations that Apply on a Tenant-Wide Basis (continued)

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>packages.microsoft.com</td>
<td>443 and 11371</td>
<td>TCP</td>
<td>Microsoft software package server. Used to securely download the Microsoft Azure Command Line Interface (CLI) software.</td>
</tr>
<tr>
<td>Management</td>
<td>azure.archive.ubuntu.com</td>
<td>80</td>
<td>TCP</td>
<td>Ubuntu software package server. Used by the pod-related Linux-based VMs for Ubuntu operating system updates.</td>
</tr>
<tr>
<td>Management</td>
<td>api.snapcraft.io</td>
<td>443</td>
<td>TCP</td>
<td>Ubuntu software package server. Used by the pod's Linux-based VMs for Ubuntu operating system updates.</td>
</tr>
<tr>
<td>Management</td>
<td>archive.ubuntu.com</td>
<td>80</td>
<td>TCP</td>
<td>Ubuntu software package server. Used by the pod's Linux-based VMs for Ubuntu operating system updates.</td>
</tr>
<tr>
<td>Management</td>
<td>changelogs.ubuntu.com</td>
<td>80</td>
<td>TCP</td>
<td>Ubuntu software package server. Used by the pod's Linux-based VMs for tracking Ubuntu operating system updates.</td>
</tr>
<tr>
<td>Management</td>
<td>security.ubuntu.com</td>
<td>80</td>
<td>TCP</td>
<td>Ubuntu software package server. Used by the pod's Linux-based VMs for security-related Ubuntu operating system updates.</td>
</tr>
</tbody>
</table>
Table 3-13. DNS Requirements for New Pod Deployment, Pod Updates, and Service Operations that Apply on a Tenant-Wide Basis (continued)

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Management    | One of the following, depending on which Microsoft Azure cloud you are deploying your pod into:  
- Microsoft Azure (global): login.microsoftonline.com  
- Microsoft Azure Germany: login.microsoftonline.de  
- Microsoft Azure China: login.chinacloudapi.cn  
- Microsoft Azure US Government: login.microsoftonline.us | 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 3-13. DNS Requirements for New Pod Deployment, Pod Updates, and Service Operations that Apply on a Tenant-Wide Basis (continued)

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>One of the following, depending on which Microsoft Azure cloud you are deploying your pod into:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Azure (global): graph.windows.net</td>
<td>443</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Azure Germany: graph.cloudapi.de</td>
<td>443</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Azure China: graph.chinacloudapi.cn</td>
<td>443</td>
<td>TCP</td>
<td>Used for the pod's ability to programmatically work with the Azure Key Vault cloud service. Azure Key Vault is a cloud service that provides a secure store for secrets.</td>
</tr>
</tbody>
</table>
Table 3-13. DNS Requirements for New Pod Deployment, Pod Updates, and Service Operations that Apply on a Tenant-Wide Basis (continued)

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Management    | If your firewall or network security group (NSG) supports the use of service tags, one of the following:  
  - Global Azure SQL service tag: Sql  
  - Region-specific SQL service tag for the Azure region where the pod is deployed: Sql.region, such as Sql.WestUS.  
  If your firewall or network security group (NSG) does not support the use of service tags, you can use the hostname of the database. This name follows the pattern *.postgres.database.azure.com. | 5432 | TCP      | Used for pod communication to the Microsoft Azure PostgreSQL database server. Starting with the September 2019 release, pods that are newly deployed after that release date and pods that are updated to that release’s manifest version are configured with a Microsoft Azure PostgreSQL database server. For information about service tags in security groups, see the Microsoft Azure documentation topic at Service tags. |
<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>One of the following names, depending on which regional control plane instance is</td>
<td>443</td>
<td>TCP</td>
<td>Regional instance of the Universal Broker service</td>
</tr>
<tr>
<td></td>
<td>specified in your Horizon Cloud tenant account. The regional instance is set when</td>
<td></td>
<td></td>
<td>United States: connector-azure-us.vmwarehorizon.com</td>
</tr>
<tr>
<td></td>
<td>the account is created, as described in Deployments and Onboarding to Horizon Cloud</td>
<td></td>
<td></td>
<td>Europe: connector-azure-eu.vmwarehorizon.com</td>
</tr>
<tr>
<td></td>
<td>for Microsoft Azure and Horizon Pods.</td>
<td></td>
<td></td>
<td>Australia: connector-azure-aus.vmwarehorizon.com</td>
</tr>
<tr>
<td></td>
<td>- connector-azure-us.vmwarehorizon.com</td>
<td></td>
<td></td>
<td>Japan: connector-azure-jp.vmwarehorizon.com</td>
</tr>
<tr>
<td></td>
<td>- connector-azure-eu.vmwarehorizon.com</td>
<td></td>
<td></td>
<td>United Kingdom: connector-azure-uk.vmwarehorizon.com</td>
</tr>
</tbody>
</table>
Table 3-13. DNS Requirements for New Pod Deployment, Pod Updates, and Service Operations that Apply on a Tenant-Wide Basis (continued)

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Tenant        | One of the following names, depending on which of the regional DNS names apply to your account.  
- d1mes20qfad06k.cloudfront.net  
- hydra-softwarelib-cdn.azureedge.net | 443   | TCP      | Horizon Cloud content delivery server. On the tenant subnet, this site is used by the system's automated Import Image process for downloading the installer for the agent-related software.  
d1mes20qfad06k.cloudfront.net corresponds to regional instances for cloud.horizon.vmware.com, cloud-eu-central-1.horizon.vmware.com, cloud-ap-southeast-2.horizon.vmware.com.  
hydra-softwarelib-cdn.azureedge.net corresponds to regional instances for cloud-us-2.horizon.vmware.com, cloud-eu-2.horizon.vmware.com, cloud-ap-2.horizon.vmware.com, cloud-jp.horizon.vmware.com, cloud-uk.horizon.vmware.com |
| Tenant        | Depending on which regional control plane applies to your Horizon Cloud account:  
North America:  
- kinesis.us-east-1.amazonaws.com  
- query-prod-us-east-1.cms.vmware.com  
Europe:  
- kinesis.eu-central-1.amazonaws.com  
- query-prod-eu-central-1.cms.vmware.com | 443   | TCP      | Cloud Monitoring Service (CMS) |
### Horizon Edge Virtual Appliance DNS Requirements

Activating Horizon Infrastructure Monitoring on a pod will instantiate the Linux-based Horizon Edge Virtual Appliance in your Microsoft Azure subscription. The Horizon Edge Virtual Appliance is deployed into the pod's subscription with a NIC on the pod's management subnet — the same management subnet as that pod's pod-manager appliances. In the following table, the listed purposes are in context of this virtual appliance.

**Note** There are no DNS names with *uk* in this table like there are in the preceding table. As stated in the Release Notes, this Horizon Infrastructure Monitoring feature is currently in Limited Availability.

#### Table 3-14. Horizon Infrastructure Monitoring DNS Requirements

<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port/Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>azure.archive.ubuntu.com</td>
<td>80 and 443 / TCP</td>
<td>Ubuntu software package server. Used by the Linux-based appliance for Ubuntu operating system updates.</td>
</tr>
<tr>
<td></td>
<td>archive.ubuntu.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>changelogs.ubuntu.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>security.ubuntu.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>*.blob.core.windows.net</td>
<td>443 / TCP</td>
<td>Used for programmatic access to the Azure Blob Storage. Used to download the Docker images from those DNS addresses that the appliance’s module requires.</td>
</tr>
<tr>
<td></td>
<td>horizonedgeprod.azurecr.io</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Table 3-13. DNS Requirements for New Pod Deployment, Pod Updates, and Service Operations that Apply on a Tenant-Wide Basis (continued)
<table>
<thead>
<tr>
<th>Subnet Source</th>
<th>Destination (DNS name)</th>
<th>Port/Protocol</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Management    | *.azure-devices.net, or one of the region-specific names below, depending on which regional control plane applies to your tenant account: North America:  
  - edgehubprodna.azure-devices.net  
  Europe:  
  - edgehubprodeu.azure-devices.net  
  Australia:  
  - edgehubprodap.azure-devices.net  
  Japan:  
  - edgehubprodjp.azure-devices.net | 443 / TCP | Used to connect the appliance to the Horizon Cloud control plane, to download configurations for the appliance’s module, and to update the appliance’s module’s runtime status. |
| Management    | *.docker.com  
  *.docker.io  
  docker.io  
  cloud.google.com  
  gcr.io  
  dl.k8s.io  
  k8s.gcr.io  
  storage.googleapis.com  
  cloud.weave.works  
  packages.cloud.google.com  
  apt.kubernetes.io | 443 / TCP | Used to download Docker binaries and Kubernetes binaries that the appliance needs. |
| Management    | Depending on which regional control plane applies to your tenant account: North America:  
  - kinesis.us-east-1.amazonaws.com  
  - sauron.horizon.vmware.com  
  Europe:  
  - kinesis.eu-central-1.amazonaws.com  
  - sauron-eu.horizon.vmware.com  
  Australia:  
  - kinesis.ap-southeast-2.amazonaws.com  
  - sauron-ap.horizon.vmware.com  
  Japan:  
  - kinesis.ap-northeast-1.amazonaws.com  
  - sauron-jp.horizon.vmware.com | 443 / TCP | Used to send the pod monitoring data collected by the appliance to the Horizon Cloud control plane. |
Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates

As described in Microsoft Azure Virtual Machine Requirements for a Horizon Cloud Pod in Microsoft Azure, a jump box VM is used in the initial creation of a pod and during subsequent software updates on the pod's environment. After a pod is created, the jump box VM is deleted. Then, when a pod is being updated, the jump box VM is re-created to run that update process and is deleted when the update has completed. Such updates include when a pod is edited to add a Unified Access Gateway configuration.

**Note**  A pod that is either deployed new in Microsoft Azure starting with the September 2019 release or which is updated to the September 2019 release manifest level and has high availability enabled will have two manager VMs. The following paragraphs use the plural word VMs to indicate the jump box VM must communicate with all of the pod's manager VMs, whether the pod has only one or has two.

During those processes, that jump box VM communicates with:

- The pod’s manager VMs using SSH to the manager VMs' port 22. As a result, during the pod deployment process and pod update process, the requirement that communication between the jump box VM and the manager VMs' port 22 must be met. The manager VMs' port 22 must be allowed between the jump box VM as a source and the manager VMs as a destination.

- The Unified Access Gateway VMs using HTTPS to those VMs' port 9443, in the case where a pod is deployed with, or edited to add, a Unified Access Gateway configuration. As a result, during the pod deployment process and pod update process, when the pod configuration includes Unified Access Gateway, the requirement that communication between the jump box VM and the Unified Access Gateway VMs' port 9443 must be met. The Unified Access Gateway VMs' port 9443 must be allowed between the jump box VM as a source and the Unified Access Gateway VMs as a destination.

Because these VMs are assigned IP addresses dynamically, the network rules to allow this communication should use:

- The management subnet CIDR as both the source and destination, with destination port 22, source port any, and protocol TCP.

- The management subnet CIDR as both the source and destination, with destination port 9443, source port any, and protocol TCP, when a Unified Access Gateway configuration is involved.

**Note** Ongoing pod operations do not require availability of port 22 on the pod’s manager VMs. However, if you make a support request to VMware and the support team determines the way to debug that request is to deploy a jump box VM for SSH communication to your pod's manager VMs, then you will have to meet this port requirement during the time the VMware support team needs the port for debugging your issue. The VMware support team will inform you of any requirements, as appropriate for any support situation.
When the External Gateway is Deployed in its Own VNet: Ports and Protocols Required by the External Gateway Configuration’s Jump Box During Gateway Deployments and Updates

As described in Microsoft Azure Virtual Machine Requirements for a Horizon Cloud Pod in Microsoft Azure, a jump box VM is used in the initial creation of the external gateway in its own VNet and during subsequent software updates on that gateway. After the external gateway is created in its own VNet, the jump box VM is deleted. Then, when that external gateway is being updated, the jump box VM is re-created to run that update process and is deleted when the update has completed. Such updates include when a pod is edited to add an external gateway in its own VNet.

During those processes, that jump box VM communicates with:

- During those processes, that jump box VM communicates with the gateway connector VM using SSH to that connector VM’s port 22. As a result, during the gateway deployment process and update process, the requirement that communication between the jump box VM and the connector VMs' port 22 must be met. The connector VMs’ port 22 must be allowed between the jump box VM as a source and the connector VMs as a destination.

- The Unified Access Gateway VMs using HTTPS to those VMs' port 9443. As a result, during the pod deployment process and pod update process, when the pod configuration includes Unified Access Gateway, the requirement that communication between the jump box VM and the Unified Access Gateway VMs' port 9443 must be met. The Unified Access Gateway VMs’ port 9443 must be allowed between the jump box VM as a source and the Unified Access Gateway VMs as a destination.

Because these VMs are assigned IP addresses dynamically, the network rules to allow this communication should use:

- The management subnet CIDR as both the source and destination, with destination port 22, source port any, and protocol TCP.

- The management subnet CIDR as both the source and destination, with destination port 9443, source port any, and protocol TCP.

Note: Ongoing pod operations do not require availability of port 22 on the gateway connector’s VM. However, if you make a support request to VMware and the support team determines the way to debug that request is to deploy a jump box VM for SSH communication to that gateway’s connector VM, then you will have to meet this port requirement during the time the VMware support team needs the port for debugging your issue. The VMware support team will inform you of any requirements, as appropriate for any support situation.

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

For ongoing Horizon Cloud operations, a pod that is either deployed new in Microsoft Azure starting with the September 2019 release and later, or which is updated to the September 2019 release level, has specific port and protocol requirements that are different from a pod that was
deployed previously. Pods deployed new or updated to the September 2019 release have manifest versions of 1600 or later.

**Important** In addition to the ports and protocols described here, you must meet DNS requirements. For details, see DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features.

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 the Horizon Cloud Administration Guide.

**Ports and Protocols Required by Key Pod Components for Ongoing Operations**

In addition to the DNS requirements, the following tables list ports and protocols that are required for the pod to operate properly for ongoing operations after deployment. Some of these tables also list ports and protocols that are required for specific scenarios or when you have enabled particular features on the pod.

In the tables below, the term manager VM refers to the pod's manager VM. In the Microsoft Azure portal, this VM has a name that contains a part like `vmw-hcs-podID`, where `podID` is the pod's UUID, and a node part.

**Important** A pod that is enabled for high availability has two manager VMs. A pod that has high availability switched on has only one manager VM. In the tables below, wherever you see the term manager VM, it applies to all of the manager VMs in your high-availability-enabled pod unless otherwise indicated.

All pods at the September 2019 release's manifest version or later have a pod Microsoft Azure load balancer. The table rows that involve the pod's load balancer apply for all pods at the manifest level of 1600 or later.

**Table 3-15. Pod Operations Ports and Protocols**

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Ports</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager VM</td>
<td>Pod’s other manager VM</td>
<td>4101</td>
<td>TCP</td>
<td>For a pod that is enabled with high availability, this traffic is JMS routing between the manager VMs.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Unified Access Gateway VMs</td>
<td>944 3</td>
<td>HTTPS</td>
<td>This port is used by the pod manager VM over the management subnet to configure settings in the pod’s Unified Access Gateway configuration. This port requirement applies when initially deploying a pod with a Unified Access Gateway configuration and when editing a pod to add a Unified Access Gateway configuration or update settings for that Unified Access Gateway configuration.</td>
</tr>
<tr>
<td>Pod’s Microsoft Azure load balancer</td>
<td>Manager VM</td>
<td>808 0</td>
<td>HTTP</td>
<td>Health checks of the VMs in the load balancer’s backend pool. When a pod at this release’s manifest version is not enabled with high availability, the load balancer has one manager VM is its backend pool to check.</td>
</tr>
<tr>
<td>Source</td>
<td>Target</td>
<td>Port(s)</td>
<td>Protocol</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------</td>
<td>---------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Domain controller</td>
<td>389</td>
<td>TCP, UDP</td>
<td>LDAP services. Server that contains a domain controller role in an Active Directory configuration. Registering the pod with an Active Directory is a requirement.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Global catalog</td>
<td>326</td>
<td>TCP</td>
<td>LDAP services. Server that contains global catalog role in an Active Directory configuration. Registering the pod with an Active Directory is a requirement.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Domain controller</td>
<td>88</td>
<td>TCP, UDP</td>
<td>Kerberos services. Server that contains a domain controller role in an Active Directory configuration. Registering the pod with an Active Directory is a requirement.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>DNS server</td>
<td>53</td>
<td>TCP, UDP</td>
<td>DNS services.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>NTP server</td>
<td>123</td>
<td>UDP</td>
<td>NTP services. Server that provides NTP time synchronization.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>True SSO Enrollment Server</td>
<td>3211</td>
<td>TCP</td>
<td>True SSO Enrollment Server. Optional if you are not using True SSO Enrollment Server capabilities with your pods.</td>
</tr>
<tr>
<td>Manager VM</td>
<td>Workspace ONE Access service</td>
<td>443</td>
<td>HTTPS</td>
<td>Note This row is applicable to environments with a single-pod-broker configuration. This information is not for environments with a Universal Broker configuration. In a single-pod-broker configured environment, the Workspace ONE Access Connector communicates with a pod to obtain the end-user entitlements (the assignments). Optional if you are not integrating Workspace ONE Access with the pod. In a single-pod-broker configured environment, this connection is used to create a trust relationship between the pod and the Workspace ONE Access service, where the Workspace ONE Access Connector is synched with the pod. Ensure that the pod can reach the Workspace ONE Access environment you are using on port 443. When you are using the Workspace ONE Access cloud service, see also the list of Workspace ONE Access service IP addresses to which the Workspace ONE Access Connector and the pod must have access in the VMware Knowledge Base article 2149884.</td>
</tr>
</tbody>
</table>
Table 3-15. Pod Operations Ports and Protocols (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port(s)</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transient Jump box VM</td>
<td>Manager VM</td>
<td>22</td>
<td>TCP</td>
<td>As described above in Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates, a transient jump box is used during pod deployment and pod update processes. Even though ongoing processes do not require these ports, during pod deployment and pod update processes, this jump box VM must communicate with the manager VMs using SSH to the manager VMs' port 22. For details about the cases for which the jump box VM needs this communication, see Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates. Note A pod that is at manifest version 1600 or later and has the high availability feature enabled on it, will have two manager VMs. The preceding paragraph uses the plural word VMs to indicate the jump box VM must communicate with all of the pod's manager VMs, whether the pod has only one or has two.</td>
</tr>
<tr>
<td>Transient Jump box VM</td>
<td>Unified Access Gateway VMs</td>
<td>944 3</td>
<td>HTTPS</td>
<td>This port is used by the jump box VM over the management subnet to configure settings in the pod's Unified Access Gateway configuration. This port requirement applies when initially deploying a pod with a Unified Access Gateway configuration and when editing a pod to add a Unified Access Gateway configuration to a pod.</td>
</tr>
</tbody>
</table>

Gateway Connector VM Ports and Protocols Requirements

This table applies to the gateway's connector VM that is used when you have deployed the external gateway in a separate VNet. In addition to the DNS requirements, the ports and protocols in the following table are required for the external gateway to operate properly for ongoing operations after deployment.

In the table below, the term connector VM refers to the gateway's connector VM which manages the connection between the cloud management plane and the external gateway. In the Microsoft Azure portal, this VM has a name that contains a part like vmw-hcs-ID, where ID is the gateway's deployer ID, and a node part.
Table 3-16. 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>Connector VM</td>
<td>DNS server</td>
<td>53</td>
<td>TCP, UDP</td>
<td>DNS services.</td>
</tr>
<tr>
<td>Connector VM</td>
<td>NTP server</td>
<td>123</td>
<td>UDP</td>
<td>NTP services. Server that provides NTP time synchronization.</td>
</tr>
<tr>
<td>Transient Jump box VM</td>
<td>Connector VM</td>
<td>22</td>
<td>TCP</td>
<td>As described above in Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates, a transient jump box is used during deployment of the external gateway and during update processes. Even though ongoing processes do not require these ports, during deployment and update processes, this jump box VM must communicate with the connector VM using SSH to the connector VMs’ port 22.</td>
</tr>
</tbody>
</table>

Unified Access Gateway VM Ports and Protocols Requirements

In addition to the DNS and above primary ports and protocols requirements, the ports and protocols in the following tables are related to the gateways that you have configured on the pod to operate properly for ongoing operations after deployment.

For connections using a high-availability-enabled pod configured with Unified Access Gateway instances, traffic must be allowed from the pod’s Unified Access Gateway instances to targets as listed in the table below. During pod deployment, a Network Security Group (NSG) is created in your Microsoft Azure environment for use by the pod’s Unified Access Gateway software.

Table 3-17. Port Requirements for Traffic from the Pod’s Unified Access Gateway Instances

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Access Gateway</td>
<td>Pod's Microsoft Azure load balancer</td>
<td>8443</td>
<td>TCP</td>
<td>Login authentication traffic. The traffic from the Unified Access Gateway instances reaches the pod's manager VM through the pod's load balancer.</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>4172</td>
<td>TCP, UDP</td>
<td>PCoIP</td>
</tr>
</tbody>
</table>
| Unified Access Gateway| Horizon agent in the desktop or farm RDSH VMs | 22443 | TCP, UDP | Blast Extreme  
By default, when using Blast Extreme, client-drive redirection (CDR) traffic and USB traffic is side-channeled in this port. If you prefer instead, the CDR traffic can be separated onto the TCP 9427 port and the USB redirection traffic can be separated onto the TCP 32111 port. |
| Unified Access Gateway| Horizon agent in the desktop or farm RDSH VMs | 9427 | TCP      | Optional for client driver redirection (CDR) and multimedia redirection (MMR) traffic. |
Table 3-17. Port Requirements for Traffic from the Pod's Unified Access Gateway Instances (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>32111</td>
<td>TCP</td>
<td>Optional for USB redirection traffic.</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Your RADIUS instance</td>
<td>1812</td>
<td>UDP</td>
<td>When using RADIUS two-factor authentication with that Unified Access Gateway configuration. The default value for RADIUS is shown here.</td>
</tr>
</tbody>
</table>

Ports and Protocols Required by Universal Broker

To support the use of Universal Broker for the brokering of end-user assignments from a pod, you must configure port 443 as described in the following table. The active pod manager establishes a persistent WebSocket connection with the Universal Broker service through port 443 and receives connection requests from the Universal Broker service through a randomly selected port.

Table 3-18. Port Requirements for Universal Broker

<table>
<thead>
<tr>
<th>Source</th>
<th>Source Port</th>
<th>Target</th>
<th>Target Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active pod manager</td>
<td>Randomly selected from available ports</td>
<td>Universal Broker service</td>
<td>443</td>
<td>HTTPS initially, then WebSocket</td>
<td>Establishes a persistent WebSocket connection with the Universal Broker service</td>
</tr>
</tbody>
</table>

Ports and Protocols Required by the Horizon Edge Virtual Appliance

When you activate Horizon Infrastructure Monitoring for a pod, the Horizon Edge Virtual Appliance is deployed and configured in that pod's subscription. The appliance has a single NIC on the pod's management subnet and an NSG is automatically configured on that NIC. That NSG's rule specify the allowed traffic into the appliance and out from the appliance. The following table lists the ports and protocols from that NSG that are needed during the activation process, as the appliance is deployed and configures the pod manager VMs so that it can collect the monitoring data it is designed to collect from those components. This table also lists the ports and protocols that are needed during the appliance's steady-state operations of collecting the data it is designed to collect in this current service release.
### Table 3-19. Port Requirements for the Horizon Edge Virtual Appliance

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Ports</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Edge Virtual Appliance</td>
<td>DNS server</td>
<td>53</td>
<td>TCP</td>
<td>DNS services</td>
</tr>
<tr>
<td>Horizon Edge Virtual Appliance</td>
<td>Pod manager VMs</td>
<td>9172</td>
<td>Any</td>
<td>In steady-state operations over the management subnet, for the appliance to collect the monitoring data that it is designed to collect.</td>
</tr>
<tr>
<td>Horizon Edge Virtual Appliance</td>
<td>Cloud control plane</td>
<td>443</td>
<td>TCP</td>
<td>In steady-state operations over the management subnet, for the appliance to communicate the monitoring data to the cloud control plane. Also, during deployment of the appliance, this port is used to download specific externally located software components, such as the Microsoft Azure CLI software, that are required for the appliance to perform its configuration of the pod manager VMs for collection of the monitoring data.</td>
</tr>
<tr>
<td>Horizon Edge Virtual Appliance</td>
<td>Pod manager VMs</td>
<td>4002</td>
<td>TCP</td>
<td>In steady-state operations over the management subnet, for the appliance to collect the monitoring data that it is designed to collect.</td>
</tr>
</tbody>
</table>
End-User Connection Traffic Ports and Protocols Requirements

For detailed information about the various Horizon Clients that your end users might use with your Horizon Cloud pod, see the Horizon Client documentation page at https://docs.vmware.com/en/VMware-Horizon-Client/index.html. Which ports must be opened for traffic from the end users’ connections to reach their pod-provisioned virtual desktops and remote applications depends on the choice you make for how your end users will connect:

When you choose the deployer option for having an external gateway configuration in the pod’s own VNet

The deployer deploys Unified Access Gateway instances in your Microsoft Azure environment, along with a Microsoft Azure load balancer resource to those instances in that load balancer’s backend pool. That load balancer communicates with those instances' NICs on the DMZ subnet, and is configured as a public load balancer in Microsoft Azure. The diagram Figure 3-1. Illustration of the Horizon Cloud Pod Architecture for a Pod with High Availability Enabled and Configured with Both External and Internal Gateway Configurations, the External Gateway Deployed into the Same VNet as the Pod, Three NICs on the External Gateway VMs, Two NICs on the Internal Gateway VMs, and a Public IP Enabled for the External Gateway’s Load Balancer depicts the location of this public load balancer and the Unified Access Gateway instances. When your pod has this configuration, traffic from your end users on the Internet goes to that load balancer, which distributes the requests to the Unified Access Gateway instances. For this configuration, you must ensure that those end-user connections can reach that load balancer using the ports and protocols listed below. Post-deployment, the external gateway's load balancer is located in the resource group named vmw-hcs-podID-uag, where podID is the pod’s UUID.

When you choose the deployer option for having an internal Unified Access Gateway configuration

An internal gateway configuration is deployed into the pod’s own VNet by default. The deployer deploys Unified Access Gateway instances in your Microsoft Azure environment, along with a Microsoft Azure load balancer resource to those instances in its backend pool. That load balancer communicates with those instances' NICs on the tenant subnet, and is configured as an internal load balancer in Microsoft Azure. The diagram Figure 3-1. Illustration of the Horizon Cloud Pod Architecture for a Pod with High Availability Enabled and Configured with Both External and Internal Gateway Configurations, the External Gateway Deployed into the Same VNet as the Pod, Three NICs on the External Gateway VMs, Two NICs on the Internal Gateway VMs, and a Public IP Enabled for the External Gateway’s Load Balancer depicts the location of this internal load balancer and the Unified Access Gateway instances. When your pod has this configuration, traffic from your end users in your corporate network goes to that load balancer, which distributes the requests to the Unified Access Gateway instances. For this configuration, you must ensure that those end-user connections can reach that load balancer using the ports and protocols listed below. Post-deployment, the internal gateway's load balancer is located in the resource group named vmw-hcs-podID-uag-internal, where podID is the pod’s UUID.
When you choose the deployer options either for having an external gateway configuration in its own VNet and not the pods, or the option to use its own subscription (which is a special sub-case of using its own VNet because V Nets do not span subscriptions)

The deployer deploys Unified Access Gateway instances in your Microsoft Azure environment, along with a Microsoft Azure load balancer resource to those instances in that load balancer’s backend pool. That load balancer communicates with those instances' NICs on the DMZ subnet, and is configured as a public load balancer in Microsoft Azure. The diagram Figure 3-2. Illustration of the External Gateway’s Architecture Elements When the External Gateway is Deployed into Its Own VNet, Separate from the Pod’s VNet depicts the location of this public load balancer and the Unified Access Gateway instances in the gateway’s own VNet. When your pod has this configuration, traffic from your end users on the Internet goes to that load balancer, which distributes the requests to the Unified Access Gateway instances. For this configuration, you must ensure that those end-user connections can reach that load balancer using the ports and protocols listed below. Post-deployment, the external gateway’s load balancer is located in the resource group named \textit{vmw-hcs-ID-uag}, where \textit{ID} is the value show in the \textbf{Deployer ID} field of the pod’s details page. As described in the \textit{Administration Guide}, you get to the pod’s details page from the console’s Capacity page.

Unsupported for pod manifests 2298 and later: When you have removed the Unified Access Gateway configurations and continue running with zero Unified Access Gateway configurations on the pod

A pod at manifest 2298 or later must have at least one gateway configuration to have supported operations. This scenario is only possible for manifests earlier than 2298.

\textbf{Attention}  In production systems, for internal-user access, the best practice is to use an internal Unified Access Gateway gateway configuration on the pod, and not direct connections to the pod.

In a configuration where you have single-pod brokering and Workspace ONE Access integrated with the pod, you typically have your end users connect through Workspace ONE Access. In this scenario, you must configure Workspace ONE Access and the Workspace ONE Access Connector pointing directly to the pod. Your end users are connecting to their pod-provisioned resources using Workspace ONE Access. For this configuration, you upload an SSL certificate to the pod’s manager VMs using the pod’s summary page in the console, as described in the \textit{VMware Horizon Cloud Service Administration Guide}. Then you complete the steps to integrate Workspace ONE Access with the pod.
<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic. Can also carry client-drive redirection (CDR), multimedia redirection (MMR), USB redirection, and tunneled RDP traffic. SSL (HTTPS access) is enabled by default for client connections. Port 80 (HTTP access) can be used in some cases. See the topic Understanding What URL Content Redirection Is in the VMware Horizon Cloud Service Administration Guide.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>4172</td>
<td>TCP, UDP</td>
<td>PCoIP via PCoIP Secure Gateway on Unified Access Gateway</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>UDP</td>
<td>Blast Extreme via the Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>844, 3</td>
<td>UDP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic (adaptive transport).</td>
</tr>
<tr>
<td>Browser</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>
Table 3-21. Internal End User Connections Ports and Protocols when the Pod Configuration has Internal Unified Access Gateway instances

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic. Can also carry client-drive redirection (CDR), multimedia redirection (MMR), USB redirection, and tunneled RDP traffic. SSL (HTTPS access) is enabled by default for client connections. Port 80 (HTTP access) can be used in some cases. See the topic Understanding What URL Content Redirection Is in the VMware Horizon Cloud Service Administration Guide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4172</td>
<td>TCP, UDP</td>
<td>PCoIP via PCoIP Secure Gateway on Unified Access Gateway</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>443</td>
<td>UDP</td>
<td>Blast Extreme via the Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>844</td>
<td>UDP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic (adaptive transport).</td>
</tr>
<tr>
<td>Browser</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>
Table 3-22. Internal End User Connections Ports and Protocols when using Direct Pod Connections, Such as Over VPN

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Pod's Microsoft Azure load balancer</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic. The traffic from the clients reaches the pod's manager VMs through the pod's load balancer.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>4172</td>
<td>TCP, UDP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>22443</td>
<td>TCP, UDP</td>
<td>Blast Extreme</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>32111</td>
<td>TCP</td>
<td>USB redirection</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>9427</td>
<td>TCP</td>
<td>Client-drive redirection (CDR) and multimedia redirection (MMR)</td>
</tr>
<tr>
<td>Browser</td>
<td>Horizon agent in the desktop or farm RDSH VMs</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>

Ports and Protocols Requirements for Traffic from the Horizon Agent in the Base VM, VDI Desktop VMs, and Farm RDSH VMs

The following ports must allow traffic between the Horizon agent-related software that is installed in the base VMs, desktop VMs, and farm RDSH VMs and the pod's manager VMs.
<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon agent in the base imported VM,</td>
<td>Manager VM</td>
<td>4001</td>
<td>TCP</td>
<td>Java Message Service (JMS, non-SSL), used by the agent in the VM to</td>
</tr>
<tr>
<td>golden images, desktop VMs, farm RDSH VMs</td>
<td></td>
<td></td>
<td></td>
<td>communicate with the pod as part of the certificate thumbprint</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>verification and exchange to secure an SSL connection to the pod. After</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>the keys are negotiated and exchanged between the VM and the pod</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>manager, the agent uses port 4002 to create a secured SSL connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>For example, the <strong>Reset Agent Pairing</strong> action on the Imported VMs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>page requires communication over port 4001 for that</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>agent pairing workflow between the base imported VM and the pod.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note</strong> Both ports 4001 and 4002 are required for steady-state</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>operations. There are times when the agent might need to re-key</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>with the pod, so port 4001 must be kept open.</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 agent in the base imported VM,</td>
<td>Manager VM</td>
<td>4002</td>
<td>TCP</td>
<td>Java Message Service (JMS, SSL), used by the agent in these VMs to</td>
</tr>
<tr>
<td>golden images, desktop VMs, farm RDSH VMs</td>
<td></td>
<td></td>
<td></td>
<td>communicate with the pod using a secured SSL connection.</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>FlexEngine agent (the agent for VMware</td>
<td>Those file shares that</td>
<td>445</td>
<td>TCP</td>
<td>FlexEngine agent access to your SMB file shares, if you are using</td>
</tr>
<tr>
<td>Dynamic Environment Manager) in the desktop</td>
<td>you set up for use by the</td>
<td></td>
<td></td>
<td>VMware Dynamic Environment Manager capabilities.</td>
</tr>
<tr>
<td>or farm RDSH VMs</td>
<td>FlexEngine agent that</td>
<td></td>
<td></td>
<td>runs in the desktop or farm RDSH VMs</td>
</tr>
<tr>
<td></td>
<td>runs in the desktop or</td>
<td></td>
<td></td>
<td>farm RDSH VMs</td>
</tr>
<tr>
<td></td>
<td>farm RDSH VMs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note** Instead of listing DNS names, IP addresses, ports, and protocols in a Horizon Cloud Knowledge Base (KB) article, we have provided them here as part of the core Horizon Cloud documentation.

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

For ongoing Horizon Cloud operations, a pod that was deployed in Microsoft Azure prior to the September 2019 release has specific port and protocol requirements that are different from a pod that is deployed at the manifest version of the September 2019 release, or which is updated.
to the September 2019 release’s manifest version. A pod that was deployed prior to the September 2019 release has a manifest version of 1493.1 or earlier.

**Important** In addition to the ports and protocols described here, you must meet DNS requirements. For details, see DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features.

If your pod manifest is 1600.x or later, the ports and protocols requirements are different. See Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release’s Manifest or Later.

### Ports and Protocols Required for Ongoing Operations for a Pod of Manifest Version

In addition to the DNS requirements, the ports and protocols in the following tables are required for the pod to operate properly for ongoing operations after deployment.

**Note** In this section’s tables, the term manager VM refers to the pod’s manager VM. In the Microsoft Azure portal, this VM has a name that contains a part like `vmw-hcs-podID`, where `podID` is the pod’s UUID, and a node part.

#### Table 3-23. Pod Operations Ports and Protocols

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Ports</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager VM</td>
<td>Domain controller</td>
<td>389</td>
<td>TCP, 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>3211</td>
<td>TCP</td>
<td>True SSO Enrollment Server. Optional if you are not using True SSO Enrollment Server capabilities with your pods.</td>
</tr>
</tbody>
</table>
Table 3-23. Pod Operations Ports and Protocols (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target Service</th>
<th>Port(s)</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager VM</td>
<td>Workspace ONE Access service</td>
<td>443</td>
<td>HTTPS</td>
<td><strong>Note</strong> This row is applicable to environments with a single-pod-broker configuration. This information is not for environments with a Universal Broker configuration. In a single-pod-broker configured environment, the Workspace ONE Access Connector communicates with a pod to obtain the end-user entitlements (the assignments). Universal Broker feature is available for pods of manifest 2298 and later, and not for earlier manifests. Optional if you are not integrating Workspace ONE Access with the pod. In a single-pod-broker configured environment, this connection is used to create a trust relationship between the pod and the Workspace ONE Access service, where the Workspace ONE Access Connector is synched with the pod. Ensure that the pod can reach the Workspace ONE Access environment you are using on port 443. When you are using the Workspace ONE Access cloud service, see also the list of Workspace ONE Access service IP addresses to which the Workspace ONE Access Connector and the pod must have access in the VMware Knowledge Base article 2149884.</td>
</tr>
<tr>
<td>Transient Jump box VM</td>
<td>Manager VM</td>
<td>22</td>
<td>TCP</td>
<td>As described in <a href="#">Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates</a>, a transient jump box is used during pod deployment and pod update processes. Even though ongoing processes do not require these ports, during pod deployment and pod update processes, this jump box VM must communicate with the pod's manager VM using SSH to the manager VM's port 22. For details about the cases for which the jump box VM needs this communication, see <a href="#">Ports and Protocols Required by the Pod Jump Box During Pod Deployments and Pod Updates</a>.</td>
</tr>
</tbody>
</table>

Which ports must be opened for traffic from the end users' connections to reach their pod-provisioned virtual desktops and remote applications depends on the choice you make for how your end users will connect:

- When you choose the option for having an external gateway configuration, Unified Access Gateway instances are automatically deployed in your Microsoft Azure environment, along with a Microsoft Azure load balancer resource to those instances in its backend pool. That load balancer communicates with those instances' NICs on the DMZ subnet, and is configured as a public load balancer in Microsoft Azure. The diagram Figure 3-1. Illustration of the Horizon Cloud Pod Architecture for a Pod with High Availability Enabled and Configured with Both External and Internal Gateway Configurations, the External Gateway Deployed into the Same VNet as the Pod, Three NICs on the External Gateway VMs, Two NICs on the Internal Gateway VMs, and a Public IP Enabled for the External Gateway's Load Balancer depicts the location of this public load balancer and the Unified Access Gateway instances. When your pod has this configuration, traffic from your end users on the Internet goes to that load balancer, which distributes the requests to the Unified Access Gateway instances. For this...
configuration, you must ensure that those end-user connections can reach that load balancer using the ports and protocols listed below. For the deployed pod, the external gateway's load balancer is located in the resource group named `vmw-hcs-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 Azure load balancer resource to those instances in its backend pool. That load balancer communicates with those instances' NICs on the tenant subnet, and is configured as an internal load balancer in Microsoft Azure. The diagram Figure 3-1. Illustration of the Horizon Cloud Pod Architecture for a Pod with High Availability Enabled and Configured with Both External and Internal Gateway Configurations, the External Gateway Deployed into the Same VNet as the Pod, Three NICs on the External Gateway VMs, Two NICs on the Internal Gateway VMs, and a Public IP Enabled for the External Gateway's Load Balancer depicts the location of this internal load balancer and the Unified Access Gateway instances. When your pod has this configuration, traffic from your end users in your corporate network goes to that load balancer, which distributes the requests to the Unified Access Gateway instances. For this configuration, you must ensure that those end-user connections can reach that load balancer using the ports and protocols listed below. For the deployed pod, the internal gateway's load balancer is located in the resource group named `vmw-hcs-podID-uag-internal`, where `podID` is the pod's UUID.

- When you do not choose either Unified Access Gateway configurations, you can instead have your end users connecting directly to the pod, such as using a VPN. For this configuration, you upload an SSL certificate to the pod's manager VM using the pod's summary page in the administrative console, as described in the VMware Horizon Cloud Service Administration Guide.

For detailed information about the various Horizon Clients that your end users might use with your Horizon Cloud pod, see the Horizon Client documentation page at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.
Table 3-24. External End User Connections Ports and Protocols when the Pod Configuration has External Unified Access Gateway instances

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic. Can also carry client-drive redirection (CDR), multimedia redirection (MMR), USB redirection, and tunneled RDP traffic. SSL (HTTPS access) is enabled by default for client connections. Port 80 (HTTP access) can be used in some cases. See the topic Understanding What URL Content Redirection Is in the VMware Horizon Cloud Service Administration Guide.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>4172</td>
<td>TCP, UDP</td>
<td>PCoIP via PCoIP Secure Gateway on Unified Access Gateway</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>UDP</td>
<td>Blast Extreme via the Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>844</td>
<td>UDP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic (adaptive transport).</td>
</tr>
<tr>
<td>Browser</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>
Table 3-25. Internal End User Connections Ports and Protocols when the Pod Configuration has Internal Unified Access Gateway instances

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic. Can also carry client-drive redirection (CDR), multimedia redirection (MMR), USB redirection, and tunneled RDP traffic. SSL (HTTPS access) is enabled by default for client connections. Port 80 (HTTP access) can be used in some cases. See the topic Understanding What URL Content Redirection Is in the VMware Horizon Cloud Service Administration Guide.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>4172</td>
<td>TCP, UDP</td>
<td>PCoIP via PCoIP Secure Gateway on Unified Access Gateway</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>UDP</td>
<td>Blast Extreme via the Unified Access Gateway for data traffic.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>844</td>
<td>UDP</td>
<td>Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic (adaptive transport).</td>
</tr>
<tr>
<td>Browser</td>
<td>Microsoft Azure load balancer for these Unified Access Gateway instances</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>
Table 3-26. Internal End User Connections Ports and Protocols when using Direct Pod Connections, Such as Over VPN

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Client</td>
<td>Manager VM</td>
<td>443</td>
<td>TCP</td>
<td>Login authentication traffic</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>4172</td>
<td>TCP, UDP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>22443</td>
<td>TCP, UDP</td>
<td>Blast Extreme</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>32111</td>
<td>TCP</td>
<td>USB redirection</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>9427</td>
<td>TCP</td>
<td>Client-drive redirection (CDR) and multimedia redirection (MMR)</td>
</tr>
<tr>
<td>Browser</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>443</td>
<td>TCP</td>
<td>HTML Access</td>
</tr>
</tbody>
</table>

For connections using a pod configured with Unified Access Gateway instances, traffic must be allowed from the pod's Unified Access Gateway instances to targets as listed in the table below. During pod deployment, a Network Security Group (NSG) is created in your Microsoft Azure environment for use by the pod's Unified Access Gateway software.

Table 3-27. 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>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm server VMs</td>
<td>9427</td>
<td>TCP</td>
<td>Client-drive redirection (CDR) and multimedia redirection (MMR)</td>
</tr>
</tbody>
</table>

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.
Table 3-27. Port Requirements for Traffic from the Pod's Unified Access Gateway Instances (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Access Gateway</td>
<td>Horizon agent in the desktop or farm 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>4001</td>
<td>TCP</td>
<td>Java Message Service (JMS, non-SSL), used by the agent in the VM when the agent is not yet paired with the pod. The agent communicates with the pod to get the information it needs to pair with the pod. After the agent is paired, it uses port 4002 to communicate with the pod.</td>
</tr>
<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, SSL), used by the agent to communicate with the pod when the agent is already paired with the pod.</td>
</tr>
<tr>
<td>FlexEngine agent (the agent for VMware Dynamic Environment Manager) in the desktop or farm server VMs</td>
<td>Those file shares that you set up for use by the FlexEngine agent that runs in the desktop or farm server VMs</td>
<td>445</td>
<td>TCP</td>
<td>FlexEngine agent access to your SMB file shares, if you are using VMware Dynamic Environment Manager capabilities.</td>
</tr>
</tbody>
</table>
As part of the pod deployment process, the deployer creates network security groups (NSGs) on the network interfaces (NICs) on all of the deployed VMs. For details about the rules defined in those NSGs, see the Horizon Cloud Administration Guide.

**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.

**Create the Required Service Principal Needed by the Horizon Cloud Pod Deployer by Creating an Application Registration**

The Horizon Cloud pod deployer needs a service principal to access and use your Microsoft Azure subscription’s capacity for your Horizon Cloud pods. When you register a Microsoft Azure AD application, the service principal is also created. Also, you must generate an authentication key and assign a role to the service principal at the subscription level. If you are going to use the feature to have the external gateway use its own subscription, separate from the pod’s, you must also perform similar steps for a service principal associated with that subscription.
For up-to-date and in-depth details and screenshots for creating a service principal, see the Microsoft Azure documentation's documentation topic How to: Use the portal to create an Azure AD application and service principal that can access resources.

Important Each service principal that you configure for Horizon Cloud's use must be assigned an appropriate role in that service principal's associated subscription. The role to a service principal must allow the actions that Horizon Cloud needs to operated on the Horizon Cloud managed resources in that service principal's associated Microsoft Azure subscription. The service principal for the pod's subscription needs a role that allows for actions to successfully deploy the pod, to operate on the pod and the pod-managed resources to fulfill the administrator workflows initiated using the administrative console, and to maintain the pod over time. When using a separate subscription for the pod's external Unified Access Gateway configuration, the service principal for that subscription needs a role that allows for actions to successfully deploy the resources needed for that gateway configuration, to operate on those Horizon Cloud-managed resources to fulfill the administrator workflows, and to maintain those gateway-related resources over time.

As described in Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions, the service principal must be granted access using one of the following methods:

- At the subscription level, assign the Contributor role. The Contributor role is one of the Microsoft Azure built-in roles. The Contributor role is described in Built-in roles for Azure resources in the Microsoft Azure documentation.

- At the subscription level, assign a custom role that you have set up to provide the service principal with Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions that Horizon Cloud needs for deployment of the pod-related resources and for ongoing administrator-initiated workflows and pod maintenance operations.

- When using a separate subscription for the external Unified Access Gateway configuration and deploying into an existing resource group, an valid combination is to grant access to the service principal to access that resource group and associated VNet using a role that provides narrow-scope permissions plus grant access for the service principal to access the subscription using the built-in Reader role.

Also, the role must be assigned directly to the service principal used for Horizon Cloud. The use of a group-based assignment of a role to the service principal — in which the role is assigned to a group and the service principal is a member in that group — is unsupported.

You perform these steps using the Microsoft Azure portal appropriate for your registered account. For example, there are specific portal endpoints for these Microsoft Azure clouds.

- Microsoft Azure Commercial (standard global regions)
- Microsoft Azure China
Microsoft Azure US Government

**Note**  When performing these steps, you can collect some of the values that you will need for the deployment wizard, as described in *Subscription-Related Information for the Horizon Cloud Pod Deployment Wizard*, specifically:

- Application ID
- Authentication key

**Caution**  Even though you can set the secret key’s expiration duration to a specific timeframe, if you do that, you must remember to refresh the key before it expires or the associated Horizon Cloud pod will stop working. Horizon Cloud cannot detect or know what duration you set. For smooth operations, set the key’s expiration to *Never*.

If you prefer not to set the expiration to *Never* and prefer instead to refresh the key before it expires, you must remember to log in to Horizon Cloud before the expiration date, and in the pod’s details where the subscription information is listed, enter the new key value in the associated pod’s subscription information. For detailed steps, see the Update the Subscription Information Associated with Deployed Pods topic in the Administration Guide.

In the steps below, Step 7.a illustrates the service principal being granted access at the subscription level.

**Prerequisites**

If you want to assign a custom role to the service principal instead of the built-in Contributor role, verify that the custom role exists in your subscription. Verify that the custom role permits the management operations required by Horizon Cloud, as described in Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions.

**Procedure**

1. From the Microsoft Azure portal’s left navigation bar, click **Azure Active Directory** (Azure Active Directory), then click **App registrations** (App registrations).
2. Click **New application registration**.
3. Type a descriptive name and select a supported account type.
4 In the Redirect URI section, select **Web**, type `http://localhost:8000`, and click **Register**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>The name is up to you. The name is a way you can differentiate this service principal used by Horizon Cloud from any other service principals that might exist in this same subscription.</td>
</tr>
<tr>
<td><strong>Redirect URI</strong></td>
<td>Ensure <strong>Web</strong> is selected. Type <code>http://localhost:8000</code> as shown. Microsoft Azure marks this as a required field. Because Horizon Cloud does not need a sign-on URL for the service principal <code>http://localhost:8000</code> is used to satisfy the Microsoft Azure requirement.</td>
</tr>
</tbody>
</table>

The newly created app registration is displayed on screen.

5 Copy the application ID and directory (tenant) ID and save them to a location where you can retrieve them later when you run the deployment wizard.

From the service principal's details screen, create the service principal's authentication secret key.

   a Click **Certificates & secrets** *(Certificates and secrets)*.
   b Click **New client secret**.
c Type a description, select an expiration duration, and click **Add**.

The key description must be 16 characters or less, for example `Hzn-Cloud-Key1`.

**Caution** You can set the expiration duration to **Never** or to a specific timeframe. However, if you set a specific duration, you must remember to refresh the key before it expires and enter the new key into Horizon Cloud, using the console and in the pod's details where the pod's subscription information is listed. Otherwise, the associated pod will stop working. Horizon Cloud cannot detect or know what duration you set in the Microsoft Azure portal.

---

**Hzn-Cloud-Principal - Certificates & secrets**

![Hzn-Cloud-Principal - Certificates & secrets](image)

**Add a client secret**

- **Description**: `Hzn-cloud-key1`
- **Expires**
  - In 1 year
  - In 2 years
  - Never

**Important** Keep this screen open until you copy the secret value and paste the value into a location where you can retrieve it later. Do not close the screen until you have copied the secret value.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>EXPIRES</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hzn-cloud-key1</td>
<td>12/31/2299</td>
<td><img src="image" alt="Secret Value" /></td>
</tr>
</tbody>
</table>

d Copy the secret value to a location where you can retrieve it later when you run the deployment wizard.
 Assign a role to the service principal at the subscription level.

**Caution** If the service principal's assigned role does not permit the operations that the pod deployer requires, according to the options you select in the deployment wizard, the wizard will block you from completing the wizard's steps. For the permissions the assigned role must provide, see Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions.

a. Navigate to your subscription's settings screen by clicking *All services* in the Microsoft Azure portal's main navigation bar, clicking *Subscriptions*, and then clicking the name of the subscription that you will use with the pod.

**Note** At this point, from the screen, you can copy the subscription ID which you will later need in the deployment wizard.

b. Click *Access control (IAM)* and then click *Add role assignment* to open the *Add role assignment* screen.

c. In the *Add role assignment* screen, for *Role*, select the role you are assigning, according to the rules described in Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions.
d Use the Select box to search for your service principal by the name you gave it.

The following screenshot illustrates this step where the Contributor role is selected for the service principal.

```
Role
  Contributor
Assign access to
  Azure AD user, group, or application

Select
  Hzn

Hzn-Cloud-Principal
```

**Note** Make sure the Assign access to drop-down list is set to Azure AD user, group, or application.

e Click your service principal to make it a selected member and then click Save.
Verify that your subscription has the registered resource providers that the pod requires.

a. From the Access control (IAM) screen you are on from the previous step, navigate to the subscription's list of resource providers by clicking (Resource providers) in the subscription's menu.

b. Verify that the following resource providers have (Registered) status, and if not, register them.

- Microsoft.Compute
- microsoft.insights
- Microsoft.Network
- Microsoft.Storage
- Microsoft.KeyVault
- Microsoft.Authorization
- Microsoft.Resources
- Microsoft.ResourceHealth
- Microsoft.DBforPostgreSQL
- Microsoft.Sql

Results

At this point, you've created and configured the service provider for the pod, and you have the subscription-related values you need in the first step of the pod deployment wizard. The four subscription-related values are:

- Subscription ID
- Azure Active Directory ID
- Application ID
- Application key value

**What to do next**

Verify that you have collected all of the subscription-related information you will enter in the deployment wizard. See Subscription-Related Information for the Horizon Cloud Pod Deployment Wizard.

If you are going to use a separate subscription for deploying the external Unified Access Gateway configuration into an existing resource group, and you want to grant granular, narrow-scope permissions instead of access at the subscription level, see Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions for details. Ensure the appropriate access is granted to the service principal to meet the Horizon Cloud deployer's requirements.

**Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions**

The service principal used by Horizon Cloud to perform operations in your Microsoft Azure subscription and resource groups needs an assigned role that specifies the permitted operations that service principal can perform in that subscription and its resource groups. Even though using the Microsoft Azure built-in Contributor role provides for all of the operations needed by Horizon Cloud, it does that by granting the broadest number of permissions. Instead of using that Microsoft Azure built-in Contributor role at the subscription level, you can create a custom role with the minimum set of permissions — scoped to the minimum set of operations that Horizon Cloud requires in the associated subscription — and assign that custom role to the service principal at the subscription level. If you adopt the approach to have a separate subscription for the pod's external Unified Access Gateway configuration and select to have the gateway resources deployed into a resource group that you create and maintain, you have the option of assigning the service principal more granular, narrow-scope permissions within that separate subscription.

The overarching concept is that Horizon Cloud needs to perform certain operations in your subscription and its resource groups to successfully create and maintain the resources needed to have a pod and its gateway configurations. As a simple example, because the pod and gateway architecture require virtual machines with NICs, Horizon Cloud needs the ability to create virtual machines and NICs in your subscription and attach those NICs to subnets in the subscription's VNet. Some of the options you choose for your pod and gateway deployments determine the specific set of operations that Horizon Cloud needs to perform. You can restrict Horizon Cloud's abilities in your subscription to the minimum operations required, by following the rules described below, according to the options you are adopting for deploying a pod and for its external gateway configuration.

For details about custom roles in Microsoft Azure and the steps you take to create a custom role, see the Microsoft Azure documentation topic Custom roles for Azure resources. For details about how a role works, its structure, and the structure of the management operations, see Understand role definitions for Azure resources in the Microsoft Azure documentation. As described in that
documentation topic, a role definition is a collection of permissions. This role definition is called the role for short. The role lists the management operations that can be performed, as well as operations that cannot be performed, by the service principal to which that role is assigned. A management operation is a combination of the resource and action performed on that resource.

Overview of the Available Use Cases

When discussing Horizon Cloud required operations in your Microsoft Azure subscriptions and resource groups, there are these use cases.

<p>| Note | The role for the service principal created for the subscription that is specified for the rest of the pod resources in the two-subscription use case must follow the same rules as needed for the single-subscription use case. |</p>
<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A single subscription used by Horizon Cloud for pods and their external Unified Access Gateway configurations.</td>
<td>In this case, access must be granted to the service principal at the subscription level. The role assigned to the service principal at that level must allow the actions that Horizon Cloud needs to perform in your subscription to successfully create in that subscription the required resources and operate on those resources over time. As an example, in this case, the role must provide the ability to create the default resource groups, network security groups, virtual machines, and so on.</td>
</tr>
<tr>
<td>Two subscriptions, and you want Horizon Cloud to auto-create the gateway's required resource groups and resources in the external gateway's specified subscription, same as it does in the subscription for the rest of the pod resources.</td>
<td>When using this option, the service principal for each subscription must be granted access at the subscription level, with permissions that allow actions same as those for the single subscription use case described above.</td>
</tr>
<tr>
<td>Two subscriptions as above, but instead of having Horizon Cloud auto-create the external gateway's required resource groups and resources, you create a resource group in advance in that external gateway's specified subscription, and want Horizon Cloud to deploy the external gateway's resources into that existing resource group.</td>
<td>Two options for granting access to the service principal used for deploying the external gateway:</td>
</tr>
<tr>
<td>Two options for granting access to the service principal used for deploying the external gateway:</td>
<td>- Grant access at the subscription level, same as in the above case.</td>
</tr>
<tr>
<td>- Use the following combination:</td>
<td>- At the subscription level, grant access using the built-in Reader role.</td>
</tr>
<tr>
<td>- At the level of the named resource group, grant access using permissions defined in a custom role. The permissions granted at the resource-group level must provide for the operations that Horizon Cloud requires to perform in the resource group to deploy and configure the external gateway's resources there.</td>
<td>- At the level of the named resource group, grant access using permissions defined in a custom role. The permissions granted at the resource-group level must provide for the operations that Horizon Cloud requires to perform in the resource group to deploy and configure the external gateway's resources there.</td>
</tr>
<tr>
<td>In addition to the permissions on the resource group, Horizon Cloud needs the permissions to perform the following actions, depending on your deployment plans:</td>
<td>In addition to the permissions on the resource group, Horizon Cloud needs the permissions to perform the following actions, depending on your deployment plans:</td>
</tr>
<tr>
<td>- If this deployment will use subnets that you create in advance on that subscription's VNet, Horizon Cloud needs the ability to create NICs and network security groups (NSGs) on those subnets.</td>
<td>- If this deployment will use subnets that you create in advance on that subscription's VNet, Horizon Cloud needs the ability to create NICs and network security groups (NSGs) on those subnets. The permissions required on the VNet that the subnet belongs to are Microsoft.Network/virtualNetworks/subnets/* and Microsoft.Network/networkSecurityGroups/*</td>
</tr>
<tr>
<td>- If this deployment will have Horizon Cloud generate the subnets, in addition to the above Microsoft.Network/virtualNetworks/subnets/* and Microsoft.Network/networkSecurityGroups/*</td>
<td>- If this deployment will have Horizon Cloud generate the subnets, in addition to the above Microsoft.Network/virtualNetworks/subnets/* and Microsoft.Network/networkSecurityGroups/*</td>
</tr>
</tbody>
</table>
permissions, Horizon Cloud needs the ability to create the subnets. The permission required on the VNet is Microsoft.Network/virtualNetworks/write.

- If your external gateway deployment will specify using a public IP address, Horizon Cloud needs the ability to create public IP addresses in the named resource group. The permission required on the named resource group is Microsoft.Network/publicIPAddresses.

When Using a Single Subscription for the Pod and Its Gateway Configurations or Using a Separate Subscription for the External Unified Access Gateway Configuration with Permissions Set at the Subscription Level

For these use cases, the permissions are assigned at the subscription level. For the custom role set on the service principal that you specify in the Subscription step in the Horizon Cloud workflows, the following actions are required in the custom role definition. The * (wild card character) grants access to all operations that match the string within the listed resource provider operation. For the descriptions of the operations, see the Microsoft Azure documentation at the links listed below.

Table 3-28. Microsoft Azure Resource Operations that Must Be Permitted in the Custom Role When Assigning Permissions at the Subscription Level

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description in the Microsoft Azure Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft.Compute/<em>/</em>/read</td>
<td><a href="https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute">https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute</a></td>
</tr>
</tbody>
</table>
Table 3-28. Microsoft Azure Resource Operations that Must Be Permitted in the Custom Role When Assigning Permissions at the Subscription Level (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description in the Microsoft Azure Documentation</th>
</tr>
</thead>
</table>
Table 3-28. Microsoft Azure Resource Operations that Must Be Permitted in the Custom Role When Assigning Permissions at the Subscription Level (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description in the Microsoft Azure Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft.DBforPostgreSQL/*</td>
<td><a href="https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftdbforpostgresql">https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftdbforpostgresql</a></td>
</tr>
<tr>
<td>Microsoft.KeyVault/*/read</td>
<td><a href="https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkeyvault">https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkeyvault</a></td>
</tr>
<tr>
<td>Operation</td>
<td>Description in the Microsoft Azure Documentation</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
</tbody>
</table>
Table 3-28. Microsoft Azure Resource Operations that Must Be Permitted in the Custom Role When Assigning Permissions at the Subscription Level (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description in the Microsoft Azure Documentation</th>
</tr>
</thead>
</table>
Table 3-28. Microsoft Azure Resource Operations that Must Be Permitted in the Custom Role When Assigning Permissions at the Subscription Level (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description in the Microsoft Azure Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft.Storage/*/read</td>
<td><a href="https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftstorage">https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftstorage</a></td>
</tr>
</tbody>
</table>

The following JSON code block is an example to illustrate what a custom role definition named Horizon Cloud Pod might look like when it has the set of preceding operations. For a description of the properties and usage information, see the Custom role properties section in the Microsoft Azure documentation topic Custom roles for Azure resources. The ID is the unique ID of the
custom role. When you create the custom role using Azure PowerShell or Azure CLI, this ID is automatically generated when you create a new role. As described in the Tutorial: Create a custom role for Azure resources using Azure CLI, `mysubscriptionId1` is the ID of your own subscription.

```
{
    "Name": "Horizon Cloud Pod",
    "Id": "uuid",
    "IsCustom": true,
    "Description": "Minimum set of Horizon Cloud pod required operations",
    "Actions": [ 
        "Microsoft.Authorization/*/read",
        "Microsoft.Compute/*/read",
        "Microsoft.Compute/availabilitySets/*",
        "Microsoft.Compute/disks/*",
        "Microsoft.Compute/images/*",
        "Microsoft.Compute/locations/*",
        "Microsoft.Compute/virtualMachines/*",
        "Microsoft.Compute/virtualMachineScaleSets/*",
        "Microsoft.Compute/snapshots/*",
        "Microsoft.DBforPostgreSQL/*",
        "Microsoft.KeyVault/*/read",
        "Microsoft.KeyVault/vaults/*",
        "Microsoft.KeyVault/vaults/secrets/*",
        "Microsoft.Network/loadBalancers/*",
        "Microsoft.Network/networkInterfaces/*",
        "Microsoft.Network/networkSecurityGroups/*",
        "Microsoft.Network/publicIPAddresses/*",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/write",
        "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
        "Microsoft.Network/virtualNetworks/subnets/*",
        "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read",
        "Microsoft.Resources/subscriptions/resourceGroups/*",
        "Microsoft.ResourceHealth/availabilityStatuses/read",
        "Microsoft.Resources/deployments/*",
        "Microsoft.Storage/*/read",
        "Microsoft.Storage/storageAccounts/*"
    ],
    "NotActions": [],
    "DataActions": [],
    "NotDataActions": [],
    "AssignableScopes": [ 
        "/subscriptions/mysubscriptionId1"
    ]
}
```
When Using a Separate Subscription for the External Unified Access Gateway Configuration, Deploying into a Custom Resource Group, with Reader Role at the Subscription Level and Additional Required Permissions Assigned at Granular Levels

For this use case, you can assign the built-in Reader role to the service principal at the subscription level, and then grant access at the level of the named resource group using a custom role that specifies the permissions in the following table. Some additional permissions on subnets and on the VNet are required, depending on your planned deployment options:

- If this external gateway deployment will use subnets that you create in advance, Horizon Cloud needs the ability to create NICs and network security groups (NSGs) on those subnets. The permissions required on the VNet that the subnet belongs to are `Microsoft.Network/virtualNetworks/subnets/*` and `Microsoft.Network/networkSecurityGroups/*`.

- If this external gateway deployment will have Horizon Cloud generate the subnets, in addition to the above `Microsoft.Network/virtualNetworks/subnets/*` and `Microsoft.Network/networkSecurityGroups/*` permissions, Horizon Cloud needs the ability to create the subnets. The permission required on the subscription's VNet is `Microsoft.Network/virtualNetworks/write`.

- If your deployment will specify using a public IP address for the external gateway configuration, Horizon Cloud needs the ability to create public IP addresses in the named resource group. The permission required on the named resource group is `Microsoft.Network/publicIPAddresses`.

The following permitted operations are required in the named resource group. The `*` (wild card character) grants access to all operations that match the string within the listed resource provider operation. For the descriptions of the operations, see the Microsoft Azure documentation at the links listed below.

Table 3-30. Microsoft Azure Resource Operations that Must Be Permitted on the Specified Resource Group

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description in the Microsoft Azure Documentation</th>
</tr>
</thead>
</table>
Table 3-30. Microsoft Azure Resource Operations that Must Be Permitted on the Specified Resource Group (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description in the Microsoft Azure Documentation</th>
</tr>
</thead>
</table>
Table 3-30. Microsoft Azure Resource Operations that Must Be Permitted on the Specified Resource Group (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description in the Microsoft Azure Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft.DBforPostgreSQL/*</td>
<td><a href="https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftdbforpostgresql">https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftdbforpostgresql</a></td>
</tr>
<tr>
<td>Operation</td>
<td>Description in the Microsoft Azure Documentation</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Microsoft.Network/publicIPAddresses/*, if your deployment will specify using a public IP address for the external gateway deployment.</td>
<td><a href="https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork">https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork</a></td>
</tr>
</tbody>
</table>
Table 3-30. Microsoft Azure Resource Operations that Must Be Permitted on the Specified Resource Group (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description in the Microsoft Azure Documentation</th>
</tr>
</thead>
</table>
Table 3-30. Microsoft Azure Resource Operations that Must Be Permitted on the Specified Resource Group (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description in the Microsoft Azure Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft.Storage/*/read</td>
<td><a href="https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftstorage">https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftstorage</a></td>
</tr>
</tbody>
</table>

Subscription-Related Information for the Horizon Cloud Pod Deployment Wizard

The Horizon Cloud pod deployment wizard requires you to provide the following pieces of information from your Microsoft Azure subscription. If you are deploying the external gateway into its own subscription, separate from the pod’s, the deployer requires this information for both subscriptions.

**Important** You must obtain the application key at the moment you generate it in the Microsoft Azure portal. For information, see Create the Required Service Principal Needed by the Horizon Cloud Pod Deployer by Creating an Application Registration. You can obtain the other pieces of information at any time by logging in to your Microsoft Azure portal using your Microsoft Azure account credentials.

The IDs are UUIDs, in the form 8-4-4-4-12. These IDs and key described in the following table are used in the first step of the pod deployment wizard.
<table>
<thead>
<tr>
<th>Required Value</th>
<th>How to Collect</th>
<th>Your Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment</td>
<td>You determine the Microsoft Azure cloud environment when you register for your Microsoft Azure subscription. At that point in time, your account and subscription is created within the specific Microsoft Azure environment.</td>
<td></td>
</tr>
<tr>
<td>Subscription ID</td>
<td>In the Microsoft Azure portal, navigate to your subscription’s settings screen by clicking All services in the Microsoft Azure portal’s main navigation bar, clicking Subscriptions, and then clicking the name of the subscription that you will use with the pod. Locate the displayed subscription ID.</td>
<td></td>
</tr>
<tr>
<td>Directory ID</td>
<td>In the Microsoft Azure portal, click Azure Active Directory &gt; Properties (under Manage).</td>
<td></td>
</tr>
<tr>
<td>Application ID</td>
<td>In the Microsoft Azure portal, click Azure Active Directory &gt; App registrations, and then click the application registration that you created for Horizon Cloud using the steps in Create the Required Service Principal Needed by the Horizon Cloud Pod Deployer by Creating an Application Registration.</td>
<td></td>
</tr>
<tr>
<td>Application Key</td>
<td>Obtain the key when you generate it in the Microsoft Azure portal. See Create the Required Service Principal Needed by the Horizon Cloud Pod Deployer by Creating an Application Registration.</td>
<td></td>
</tr>
</tbody>
</table>

**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 .pks format before converting to .pem files.
Procedure

1. If your certificate is in Java JKS or JCEKS format, use keytool to convert the certificate to .p12 or .pks format.

   **Important** Use the same source and destination password during this conversion.

2. If your certificate is in PKCS#12 (.p12 or .pfx) format, or after the certificate is converted to PKCS#12 format, use openssl to convert the certificate to a .pem file.

   For example, if the name of the certificate is mycaservercert.pfx, you can use the following commands to convert the certificate:

   ```bash
   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

   ```plaintext
   -----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.

   ```bash
   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.

   ```plaintext
   -----BEGIN CERTIFICATE-----
   .... (your primary SSL certificate)
   -----END CERTIFICATE-----
   ```
Note: The server certificate should come first, followed by any intermediate ones, and then the trusted root certificate.

5 If there are any unnecessary certificate entries or extraneous information between the BEGIN and END markers, edit the file to remove those.

Results

The resulting PEM file meets the requirements of the pod deployment wizard.

Using the Horizon Cloud Administration Console to Perform an Automated Deployment of a Pod into Microsoft Azure

You run the pod deployment wizard to deploy the components that together make up a pod-manager-based pod on Microsoft Azure and its gateway configurations. The pod's connector component pairs with Horizon Cloud so that you can use your Microsoft Azure capacity with Horizon Cloud.

Important: This wizard deploys the pod-manager-based type of pod into Microsoft Azure. The wizard does not deploy a Horizon pod on Azure VMware Solution (AVS), which uses the Horizon Connection Server technology. For information about manually deploying a Horizon pod on AVS, see Tech Zone's Horizon on Azure VMware Solution Architecture and Deploying Horizon with Azure VMware Solution. For that type of pod, after you have manually deployed such a pod, you can connect it to Horizon Cloud using the Horizon Cloud Connector and the steps in High-Level Workflow When You are Onboarding an Existing Manually Deployed Horizon Pod.

The deployer uses the information you provide in each step of the wizard to determine how to configure the pod. After you provide the requested information in a particular step, proceed to the next step by clicking Next.

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.

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. For the prerequisites, see Prerequisites for Running the Pod Deployment Wizard.
Pod configuration options include:

- Selecting existing subnets that you create in advance or having the pod deployer automatically create the subnets.
- Selecting whether to enable high availability for the pod. If you deploy the pod without high availability enabled, you can later edit the pod to enable it.
- Deploying with an external or internal Unified Access Gateway configuration, or deploying with both. If you deploy with only one type of gateway configuration, you can later edit the pod to add the other, non-configured type.

<table>
<thead>
<tr>
<th>If you deploy with the Unified Access Gateway configuration as...</th>
<th>You can later edit the pod to add...</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>Internal</td>
</tr>
<tr>
<td>Internal</td>
<td>External</td>
</tr>
</tbody>
</table>

- Deploying with an external Unified Access Gateway configuration in its own VNet, separate from the pod’s VNet.
- Deploying with an external Unified Access Gateway configuration in its own subscription, separate from the pod’s subscription. Because VNets do not span subscriptions, this option is a special scenario of the separate VNet case — when the external gateway is deployed using its own subscription, it also means it is in its own VNet.
- Deploying with the option for RADIUS two-factor authentication configured on the pod’s gateway configurations. If you deploy without RADIUS settings configured on the pod’s gateway configurations, you can later edit the pod to add the other, non-configured type.
- For an external Unified Access Gateway configuration, you can optionally select to not have a public IP address on the configuration’s load balancer. If you select the wizard option to not have a public IP address on the load balancer, you must specify in the wizard an IP value that you have mapped to an FQDN in your DNS server. That FQDN is the one that will be used in your end users’ Horizon clients for PCoIP connections to this gateway. In the deployment process, the deployer will configure that IP address in the Unified Access Gateway’s Horizon configuration settings. In the Unified Access Gateway documentation, this IP value is referred...
to as the PCoIP External URL. Even though the Unified Access Gateway documentation refers to it as a URL, the entered value must be an IP address. You map this IP address to an FQDN in your DNS, which is the FQDN used in your end users' Horizon clients to establish their PCoIP sessions with the pod's external Unified Access Gateway configuration.

**Caution** You cannot later edit the deployed pod to change this IP address setting for the external gateway's load balancer. Therefore, ensure that you input the public IP address in the deployment wizard that matches your DNS mapping with the FQDN, and the FQDN matches the one in the certificate that you upload in the deployment wizard.

**Procedure**

1. **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.

2. **Start the Pod Deployment Wizard for Deploying a Pod-Manager-Based Pod**
   This wizard is used to automatically deploy a pod-manager-based pod into your Microsoft Azure subscription. When using this wizard to deploy your very first pod, you start the pod deployment wizard using the **Manage > Add Pod** feature in the **Microsoft Azure** row of the Horizon Cloud Administration Console's Getting Started page.

3. **Specify the Microsoft Azure Subscription Information for the New Horizon Cloud Pod**
   In this step of the pod deployment wizard, you provide the Microsoft Azure subscription information that you want to use for this pod.

4. **Specify Pod Configuration Information for the Horizon Cloud Pod You Are Deploying Into Microsoft Azure Using the Deployment Wizard**
   In the Pod Setup step of the pod deployment wizard, you specify details such as the name of the pod, as well as networking information.

5. **Specify the Horizon Cloud Pod’s Gateway Configuration**
   In this step of the wizard, specify the information required to deploy the pod-manager-based pod with a gateway configured. Unified Access Gateway provides the gateway environment for this type of pod. When deploying the new pod, you can choose to have either an external or internal gateway configuration — or have both types on the same pod. By default, when this wizard step displays, the external gateway configuration is selected.

6. **Validate and Proceed, and then Start the Pod Deployment Process**
   After you click **Validate & Proceed**, the system verifies your specified values. If everything validates, the wizard displays a summary of the information for your review. Then you start the deployment process.
Prerequisites for Running the Pod Deployment Wizard

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

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

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

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

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

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

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

- Verify that all of the preparatory tasks are completed, as described in Preparing to Deploy a Horizon Cloud Pod on Microsoft Azure.
- Verify that you have the subscription information, as described in Subscription-Related Information for the Horizon Cloud Pod Deployment Wizard.
- Verify that you have an existing virtual network in your Microsoft Azure subscription, and in the region in which you are deploying the pod, as described in Configure the Required Virtual Network in Microsoft Azure.

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

- Verify that your VNet is configured to point to a DNS that can resolve external addresses. The pod deployer must be able to reach external addresses in the Horizon Cloud control plane to securely download the pod software into your Microsoft Azure environment.
- Verify that the pod deployer's DNS, ports, and protocols requirements are met, as described in DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features and Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later.
- If you require use of a proxy for outbound Internet access, verify you have the networking information for your proxy configuration and the authentication credentials it requires, if any. The pod deployment process requires outbound Internet access.
- Verify that you have the information for at least one NTP server that you want the pod to use for time synchronization. The NTP server can be a public NTP server or your own NTP server that you set up for this purpose. The NTP server you specify must be reachable from the virtual network you configured. When you plan to use an NTP server using its domain name instead of a numeric IP address, also ensure that the DNS configured for the virtual network can resolve the NTP server's name.
- If you do not want the deployer to automatically create the subnets it needs, verify that the required subnets have been created in advance and exist on the VNet. For the steps to create the required subnets in advance, see In Advance of Pod Deployment, Create the Horizon Cloud Pod’s Required Subnets on your VNet in Microsoft Azure and When Using Existing Subnets for a Horizon Cloud Pod in Microsoft Azure.

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

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

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

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

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

- The fully qualified domain name (FQDN) which your end users will use to access the service. If you are planning to use the same FQDN for both the external and internal gateway configurations, after the pod is deployed, you must configure the incoming end-user client traffic to route to the appropriate gateway load balancer. The goal is to set up the routing so that client traffic from the Internet is routed to the external gateway’s Microsoft Azure Public Load Balancer and client traffic from your intranet is routed to the internal gateway’s Microsoft Azure Internal Load Balancer. In this scenario where both gateways will have the same FQDN, you configure Split DNS (Split Domain Name System) to resolve the gateway address either to the external gateway or internal gateway depending on the origin network of the end-user client’s DNS query. Then the same FQDN used in the end-user client can route to the external gateway when the client is on the Internet and route to the internal gateway when the client is on your internal network.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Start the Pod Deployment Wizard for Deploying a Pod-Manager-Based Pod

This wizard is used to automatically deploy a pod-manager-based pod into your Microsoft Azure subscription. When using this wizard to deploy your very first pod, you start the pod deployment wizard using the Manage > Add Pod feature in the Microsoft Azure row of the Horizon Cloud Administration Console's Getting Started page.

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

**Important** This wizard does not support deploying a Horizon pod into Azure VMware Solution (AVS). In the current release, there is no wizard that automates deployment of a pod into Azure VMware Solution. For that type of pod, you must first manually stand up the Horizon pod in AVS and then use the Horizon Cloud Connector to connect it to Horizon Cloud. For information about standing up a Horizon pod in AVS, see Tech Zone's Horizon on Azure VMware Solution Architecture.
Prerequisites

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

Procedure

1. Log in to the administrative console using your preferred method.
   - Go to https://cloud.horizon.vmware.com and in the My VMware Credentials section of that login page, enter My VMware account's credentials. The account credentials are the primary email address, such as user@example.com, and the password that are set in the account's profile. This choice sends the authentication request to the Horizon Cloud control plane.
   - Go to https://cloud.horizon.vmware.com and in the VMware Cloud Services section of the login page, click VMware Cloud Services. Clicking that button redirects the authentication request to VMware Cloud Services, to authenticate you according to your organization's configuration there. Use this method if your organization has asked you to access their Horizon Cloud tenant using VMware Cloud Services.
   - If your organization has asked you to access their Horizon Cloud tenant using VMware Cloud Services, you can first log in to VMware Cloud Services at https://console.cloud.vmware.com. When logged in to VMware Cloud Services, then click the Horizon Cloud tile that appears under the My Services section and the browser will open the administrative console with your authentication through VMware Cloud Services.
   - If organization has asked you to access their Horizon Cloud tenant using their Workspace ONE environment, you can first log in to that Workspace ONE console, and then use the Horizon Cloud card that appears in your set of services.

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

When your login is successfully authenticated, the console displays in your browser. When you have no existing pods, the Getting Started wizard is displayed by default with the Capacity section expanded and the Add Cloud Capacity row.
Note  As described in Horizon Cloud Deployments and Onboarding Pods — Horizon Pods on VMware SDDCs and Horizon Cloud Pods on Microsoft Azure, depending on the configuration of the Horizon Cloud tenant record, you might see a blue banner about onboarding to VMware Cloud Services. That step is not required for pod deployment and can be performed later. For information about that feature, see Onboard Your Horizon Cloud Tenant to VMware Cloud Services.

2 In the Add Cloud Capacity row, click Manage > Add Pod.

The Add Cloud Capacity wizard opens to its first step.
Specify the subscription to use for this pod by following the steps in Specify the Microsoft Azure Subscription Information for the New Horizon Cloud Pod.

Specify the Microsoft Azure Subscription Information for the New Horizon Cloud Pod

In this step of the pod deployment wizard, you provide the Microsoft Azure subscription information that you want to use for this pod.

Prerequisites

- Verify that you have met the prerequisites described in Using the Horizon Cloud Administration Console to Perform an Automated Deployment of a Pod into Microsoft Azure.
- For this wizard step, verify that you have the subscription-related information as described in Subscription-Related Information for the Horizon Cloud Pod Deployment Wizard.
- Complete the steps in Start the Pod Deployment Wizard for Deploying a Pod-Manager-Based Pod.
### Procedure

1. 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.

**Note** You might wonder why there would be previously entered subscription information when you are deploying a pod from the initial Getting Started page. Previously entered subscription information is possible in situations such as the following examples:

- You start the wizard, enter subscription information in this first wizard step, and click Add to submit the subscription information to the system and progress forward in the wizard. Then on a subsequent step, you cancel out of the wizard before completing all of the steps. In this situation, the system has saved the subscription information you entered in this first wizard step after you clicked **Add**. Even though you cancel out of the wizard in a subsequent step, the system retains that previously entered subscription information.

- You used this Horizon Cloud customer account record before, deploying first and subsequent pods for that account record, and then at some point in time, deleted those pods. When you log back in with the credentials that are associated with your Horizon Cloud customer account record, subscription information that was previously entered is still associated with that customer record, and previous subscription names are displayed in the drop-down list.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply Subscription</strong></td>
<td>Select the name of a previously entered subscription or select Add New to enter new subscription information.</td>
</tr>
<tr>
<td><strong>Subscription Name</strong></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>
</tbody>
</table>
| **Environment**       | Select the cloud environment associated with your subscription, for example:  
- **Azure - Commercial**, for the standard global Microsoft Azure cloud regions  
- **Azure - China**, for the Microsoft Azure in China cloud  
<p>| <strong>Subscription ID</strong>   | 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. |
| <strong>Directory ID</strong>      | 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. |
| <strong>Application ID</strong>    | 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. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Key</strong></td>
<td>Enter the key value for the service principal's authentication key that you created in the Microsoft Azure portal. Creating this key is a prerequisite.</td>
</tr>
</tbody>
</table>
| **Use a Different Subscription for External Gateway** | Enable this toggle when you want to deploy an external Unified Access Gateway configuration into its own subscription, separate from the pod's subscription. Using separate subscriptions for the external gateway gives your organization the flexibility to assign separate teams control over those subscriptions, depending on their area of expertise. It allows for more granular access control for which people in your organization can access the pod's assets in its subscription's resource groups and which people can access the gateway's assets.  
When this toggle is turned on, the fields for entering the gateway's subscription information are displayed. Specify the information in those fields as you did for the pod's subscription. |

**Important** In this screen, you cannot delete previously entered subscription values associated with a particular **Subscription Name**. Even though this occurrence is rare, you might imagine a situation where you:

a. Set up the subscription-related pieces in Microsoft Azure.

b. Start the Add Cloud Capacity wizard, enter those subscription values in the first step, and progress on to the next wizard step.

c. However, upon reading the networking values requested in the next wizard step, you cancel out of this wizard and open a new browser tab to go into the Microsoft Azure portal and adjust your networking configuration to meet the prerequisites.

d. While in the Microsoft Azure portal, you then also decide to make a new application registration to have a service provider with a different name.

e. You return to the browser that has the Getting Started page and restart the Add Cloud Capacity wizard.

At this point, your previously entered subscription name is still in the **Apply Subscription** drop-down list. However, if you select that name, all of the fields are prepopulated with the previous values, including the old application ID, and there is not a way to change the values in the screen or edit or delete that subscription name to start over with it. If this happens to you, cancel out of the wizard, restart the wizard, and on this first step, create a brand new subscription name by selecting **Add New**, enter the current values you want to use, and proceed forward.

The following screenshot is an example with the main subscription details completed.
Choose the Microsoft Azure subscription you want to apply or add a new one.

**Pod Subscription**

- **Apply Subscription:** Add New
- **Subscription Name:** mysub1
- **Environment:** Azure - Commercial
- **Subscription ID:**
- **Directory ID:**
- **Application ID:**
- **Application Key:**

2 Proceed to the next wizard step.

When you click the button to proceed to the next step, 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 application's service principal for the specified application ID assigned a role that permits all of the operations that the deployment process requires for the type of deployment you are doing. For a description of the service principal and its role requirements, see the topic [Create the Required Service Principal by Creating an Application Registration](#) and [Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions](#).

If you see an error message about correcting 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. Here is a list of some, though not necessarily all, situations that can result in that error message:

- If you specified a **Directory ID** that is in your subscription but you specified an **Application ID** value that is in a different directory.
If the specified service principal's assigned role does not permit the operations that the pod deployer requires.

**Important** More than one piece might be invalid when 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.

3 Specify pod details and networking information by following the steps in Specify Pod Configuration Information for the Horizon Cloud Pod You Are Deploying Into Microsoft Azure Using the Deployment Wizard.

**Specify Pod Configuration Information for the Horizon Cloud Pod You Are Deploying Into Microsoft Azure Using the Deployment Wizard**

In the Pod Setup step of the pod deployment wizard, you specify details such as the name of the pod, as well as networking information.

**Remember** This wizard deploys the pod-manager-based type of pod. The console currently does not provide a deployment wizard to deploy a Horizon pod in Azure VMware Solution (AVS). For information about deploying an Horizon pod in AVS, see Tech Zone’s Horizon on Azure VMware Solution Architecture.

**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.

**Prerequisites**

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

If you are going to have the deployment process automatically create the required subnets, verify that the CIDR address ranges that you plan to specify in the wizard fields for those subnets are not already being used by existing subnets on your VNet in Microsoft Azure.

If you have created subnets in advance for use with this pod, verify that those subnets have no resources attached to them and verify that the subnet you created to use for the management subnet has the Microsoft.SQL service configured as a service endpoint for that subnet. The pod deployment wizard will validate that the Microsoft.SQL service is configured as a service endpoint on the management subnet.

**Caution** These subnets you create on your VNet for a pod deployment must be empty. You can create the subnets prior to deploying the pod, but do not put any resources on those 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.
**Procedure**

1. In this step of the wizard, provide details about the pod and the required networking information.

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

### Add Microsoft Azure Capacity

<table>
<thead>
<tr>
<th>Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod Name:*</td>
<td></td>
</tr>
<tr>
<td>Location:*</td>
<td>Add New</td>
</tr>
<tr>
<td>Microsoft Azure Region:*</td>
<td>Select</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
</tr>
<tr>
<td>Azure Resource Tags:</td>
<td>Name</td>
</tr>
</tbody>
</table>

### High Availability

<table>
<thead>
<tr>
<th>Enabled:</th>
<th></th>
</tr>
</thead>
</table>

### Networking

<p>| Virtual Network:* |   |
| Use Existing Subnet: |   |
| Management Subnet (CIDR):* |   |
| VM Subnet (CIDR) - Primary:* |   |
| NTP Servers:* |   |
| Use Proxy: |   |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pod Name</strong></td>
<td>Enter a friendly name for this pod. This name is used in the administrative console to identify this pod from your other pods.</td>
</tr>
</tbody>
</table>
| **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 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. Currently, due to a known issue, the location names are not localized.                                                                 |
| **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/ for details. |
| **Description**        | Optional: Enter a description for this pod.                                                                                                                                                                                                                                                                                                                      |
| **Azure Resource Tags** | Optional: Create custom tags to be applied to Azure resource groups. Azure resource tags are only applied to the resource groups, and are not inherited by the resources in the groups. To create the first tag, enter information in the Name and Value fields. To create an additional tag, click + and then enter information in the Name and Value fields that appear below the existing ones.  
- You can create a maximum of 10 tags.  
- The tag name is limited to 512 characters, and the tag value is limited to 256 characters. For storage accounts, the tag name is limited to 128 characters, and the tag value is limited to 256 characters.  
- Tag names cannot contain the following characters: < > % & \ ? /  
- Tag names cannot contain these case-insensitive strings: 'azure', 'windows', 'microsoft'  
- Tag names and tag values can only contain ASCII characters. Blank spaces and characters outside the standard 128-character ASCII set (also known as high ASCII or extended ASCII characters) are not allowed. |
**Option** | **Description**
--- | ---
**High Availability** | This toggle determines whether the deployed pod has two pod manager VMs. In the deployed pod, one pod manager VM is the active one and the other is ready to handle failover if the active one goes offline, which provides high availability for the pod. For details about high availability and the pod, see *High Availability and Your Horizon Cloud Pod in Microsoft Azure*. If you switch off this toggle, the pod is deployed with a single pod manager VM. If that pod manager VM goes offline, there is no second one ready to handle the failover.

*Note* Even when this toggle is switched off, the pod still deploys with the pod architecture that has the memory-optimized, Gen 5, Microsoft Azure Database for PostgreSQL server and a Microsoft Azure load balancer in front of the pod manager VM. When you see this toggle displayed in the pod deployment wizard, its presence indicates that the pod deployer will deploy a pod using the pod architecture that has those items. A pod deployed with this toggle turned on will have a second pod manager VM, while a pod deployed with this toggle turned off will have a single pod manager VM.

**Virtual Network** | Select a virtual network from the list.
Only virtual networks (VNet) that exist in the region selected in the *Microsoft Azure Region* field are shown here. You must have already created the VNet you want to use in that region in your Microsoft Azure subscription.

**Use Existing Subnet** | Enable this toggle if you have created subnets in advance to meet the pod's subnet requirements. When this toggle is set to *Yes*, the wizard’s fields for specifying subnets change to drop-down selection menus.

*Important* The wizard does not support using an existing subnet for one of the required subnets and also entering CIDR addresses for the other required subnets. When this toggle is set to *Yes*, you must select from existing subnets for all the pod’s required subnets.

**Management Subnet** | When *Use Existing Subnet* is enabled, this menu 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 a subnet that has the Microsoft .SQL service configured as a service endpoint for that subnet. This service endpoint supports the required communication between the pod manager VMs and the pod's Azure Postgres database over the management subnet.
- 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 switched off, enter a subnet address range (in CIDR notation) for the deployer to create a subnet to which the pod and Unified Access Gateway instances will get connected, such as 192.168.8.0/27. For the management subnet, a CIDR of at least /27 is required.

*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.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Subnet - Primary</td>
<td>This field relates to the subnet used for those VMs that the pod provisions to provide your end-user desktops and applications. Such VMs include the golden image VMs, the farms' RDSH-capable VMs, and the VDI desktop VMs.</td>
</tr>
<tr>
<td>VM Subnet (CIDR) - Primary</td>
<td>When <strong>Use Existing Subnet</strong> is enabled, this menu lists the subnets available on the VNet selected for <strong>Virtual Network</strong>. Select the existing subnet that you want used for those VMs.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>Select an empty subnet, one that has no other resources attached to it. If the subnet is not empty, unexpected results might occur during the deployment process or pod operations.</td>
</tr>
<tr>
<td></td>
<td>When <strong>Use Existing Subnet</strong> is switched off, enter a subnet address range (in CIDR notation) for the deployer to create this subnet as the pod is deployed, such as 192.168.12.0/22. For the desktop subnet, a CIDR of at least /27 is required, and a CIDR of /22 is recommended.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>Ensure the range that you enter is large enough to allow for accommodating the number of VMs you anticipate you will want this pod to provision to provide your farms' RDSH-capable VMs and the VDI desktop VMs for your end users. This desktop subnet cannot be extended after the pod is deployed.</td>
</tr>
<tr>
<td><strong>Caution</strong></td>
<td>When you do not select the wizard option to use existing subnets, the subnet must not already exist in your Microsoft Azure environment. If it already exists, you will get an error when you try to proceed to the next wizard step.</td>
</tr>
</tbody>
</table>
### NTP Servers

Enter the list of NTP servers you want to use for time synchronization, separated by commas. An NTP server you enter here can be a public NTP server or your own NTP server that you set up for providing time synchronization. The NTP servers you specify here must be reachable from the virtual network you selected in the **Virtual Network** field for the pod to use. In this field, you can specify each NTP server either by its numeric IP address or its domain name. When you provide a domain name in this field instead of a numeric IP address, you must ensure that the DNS configured for your virtual network can resolve the specified name.

Examples of public NTP server domain names are `time.windows.com`, `us.pool.ntp.org`, `time.google.com`.

### Use Proxy

If you require a proxy for outbound Internet connectivity, enable this toggle and complete the associated displayed fields.

The pod deployer requires outbound access to the Internet to securely download software into the Microsoft Azure cloud environment and connect back to the Horizon Cloud cloud control plane. To enable the pod to use your proxy configuration, you must provide the following information after enabling the toggle.

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

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

The following screenshot is an example with this step completed when having the deployment process automatically create the subnets and with **High Availability** enabled. In this example, a proxy was not needed to meet the outbound Internet connectivity requirement.
2 Proceed to the next step by clicking **Next**.
Specify details for the pod to have a Unified Access Gateway configuration by following the steps in Specify the Horizon Cloud Pod's Gateway Configuration. For the ability to have your end users access their desktops and remote applications over the Internet, an external Unified Access Gateway configuration is required.

Specify the Horizon Cloud Pod's Gateway Configuration

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

**Remember** This wizard deploys the pod-manager-based type of pod. The console currently does not provide a deployment wizard to automate a Horizon pod in Azure VMware Solution (AVS), which uses the Horizon Connection Server technology. For information about deploying an Horizon pod in AVS, see Tech Zone's Horizon on Azure VMware Solution Architecture and Deploying Horizon with Azure VMware Solution.

External gateway configuration

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

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

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

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

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

### Set up external and internal Unified Access Gateways for this pod

<table>
<thead>
<tr>
<th>External Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable External Gateway?</td>
</tr>
<tr>
<td>FQDN:*</td>
</tr>
<tr>
<td>DNS Addresses:</td>
</tr>
<tr>
<td>Routes:</td>
</tr>
<tr>
<td>VM Model:*</td>
</tr>
<tr>
<td>Certificate:*</td>
</tr>
</tbody>
</table>

### Load Balancer

| Enable Public IP? | ![Image](image) |

### Networking

| Use a Different Virtual Network | ![Image](image) |
| Virtual Network:* | ![Image](image) |

| Use Existing Subnet: | ![Image](image) |
| Management Subnet (CIDR):* | ![Image](image) |
| Back End Subnet (CIDR):* | ![Image](image) |
| DMZ Subnet (CIDR):* | ![Image](image) |

### 2 Factor Authentication Settings

| Enable 2 Factor Authentication? | ![Image](image) |

### Deployment

| Use Existing Resource Group? | ![Image](image) |

<table>
<thead>
<tr>
<th>Internal Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Internal Gateway?</td>
</tr>
</tbody>
</table>
Prerequisites

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

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

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

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

Procedure

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable External Gateway?</td>
<td>Controls whether the pod has an external gateway configuration. The external configuration allows access to desktops and applications for users located outside of your corporate network. The pod includes a Microsoft Azure load balancer resource and Unified Access Gateway instances to provide this access.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  Leaving the default enabled setting is recommended.</td>
</tr>
<tr>
<td></td>
<td>When this toggle is switched off, clients must either connect through Workspace ONE Access integrated with the pod or directly to the pod managers' load balancer, or they connect through an internal gateway configuration. In the case of clients connecting through Workspace ONE Access integrated with the pod or directly, some post-deployment steps are required. In this case, after the pod is deployed, see the information in the Horizon Cloud Administration Guide about uploading SSL certificates to the pod.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Enter the required fully qualified domain name (FQDN), such as our0rg.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></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>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. 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>
</tbody>
</table>
Option | Description
--- | ---
**Routes** | Optionally specify custom routes to additional gateways that you want the deployed Unified Access Gateway instances to use to resolve network routing for the end user access. The specified routes are used to allow Unified Access Gateway to resolve network routing such as to RADIUS servers for two-factor authentication.

When configuring this pod to use two-factor authentication with an on-premises RADIUS server, you must enter the correct route the Unified Access Gateway instances can use to reach the RADIUS server. For example, if your on-premises RADIUS server uses 10.10.60.20 as its IP address, you would enter 10.10.60.0/24 and your default route gateway address as a custom route. You obtain your default route gateway address from the Express Route or VPN configuration you are using for this environment.

Specify the custom routes as a comma-separated list in the form ipv4-network-address/bits ipv4-gateway-address, for example: 192.168.1.0/24 192.168.0.1, 192.168.2.0/24 192.168.0.2.

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

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

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

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

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

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

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Internal Gateway?</td>
<td>Controls whether the pod has an internal gateway configuration. The internal configuration provides trusted access to desktops and applications for HTML Access (Blast) connections for users located inside of your corporate network. The pod includes an Azure load balancer resource and Unified Access Gateway instances to provide this access. By default, this gateway's load balancing type is private. The load balancer is configured with a private IP address.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Enter the required fully qualified domain name (FQDN), such as 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.</td>
</tr>
<tr>
<td>DNS Addresses</td>
<td>Optionally enter addresses for additional DNS servers that Unified Access Gateway can use for name resolution, separated by commas. When configuring this internal gateway configuration to use two-factor authentication with your on-premises RADIUS server, you would specify the address of a DNS server that can resolve the name of your on-premises RADIUS server. As described in the 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>
</tbody>
</table>
Option | Description
--- | ---
**VM Model** | Select a model to use for the Unified Access Gateway instances. You must ensure that the Microsoft Azure subscription you specified for this pod can provide the capacity for two VMs of the selected model.

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

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

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

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

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

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

**Results**

When you have provided the required information associated with your selected options, you can click **Validate & Proceed** to continue to the wizard's final step. See **Validate and Proceed**, and then Start the Pod Deployment Process.

**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.

When two-factor authentication details are specified in the wizard for a gateway configuration, then during the pod deployment process, the pod deployer configures the gateway configuration's corresponding deployed Unified Access Gateway appliances with the specified two-factor authentication details. As described in the Unified Access Gateway documentation, when the Unified Access Gateway appliances are configured for two-factor authentication, the Unified Access Gateway appliances authenticate the incoming user sessions according to your specified two-factor authentication policies. After Unified Access Gateway authenticates a user session according to your specified authentication policy, then Unified Access Gateway forwards that end-user client request for a desktop or application launch to the deployed pod manager to establish a connection session between the client and an available desktop or application.

**Important** After the pod is deployed, when you plan to configure your tenant to use Universal Broker, you have deployed the pod with an external gateway configuration with two-factor authentication settings, and you also deployed the pod with an internal gateway configuration, additional post-deployment steps might be required to ensure Universal Broker can distinguish between an external end user and an internal end user for the purposes of appropriately applying your two-factor authentication settings. For details, see [Best Practices When Implementing Two-Factor Authentication in a Universal Broker Environment](#).

**Prerequisites**

Verify that you have met the prerequisites described in [Prerequisites for Running the Pod Deployment Wizard](#).

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

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

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

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

**Procedure**

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

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

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

   ![Add Microsoft Azure Capacity](image)

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 Enter your &lt;i&gt;DisplayHint&lt;/i&gt; user name and passcode, where &lt;i&gt;DisplayHint&lt;/i&gt; is the text you specify in this field. This hint can help guide users to enter the correct RADIUS passcode. As an example, specifying a phrase like Example Company user name and domain password below for would result in a prompt to the end user that says Enter your Example Company user name and domain password below for user name and passcode.</td>
</tr>
<tr>
<td><strong>Name ID Suffix</strong></td>
<td>This setting is used in SAML scenarios, where your pod is configured to use TrueSSO for single sign-on. Optionally provide a string which will be appended to the SAML assertion user name that is sent in the request to the pod manager. For example, if the user name is entered as user1 on the login screen and a name ID suffix <a href="mailto:of@example.com">of@example.com</a> was specified here, a SAML assertion user name of <a href="mailto:user1@example.com">user1@example.com</a> is sent in the request.</td>
</tr>
<tr>
<td><strong>Number of Iterations</strong></td>
<td>Enter the maximum number of failed authentication attempts that a user is allowed when attempting to log in using this RADIUS system.</td>
</tr>
</tbody>
</table>
| **Maintain Username** | Enable this toggle to maintain the user’s RADIUS username during authentication to Horizon Cloud. When enabled:  
  - The user must have the same username credentials for RADIUS as for their Active Directory authentication to Horizon Cloud.  
  - The user cannot change the username in the login screen.  
  If this toggle is switched off, the user is able to type a different user name in the login screen.  
  
  **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><strong>Host Name / IP Address</strong></td>
<td>Enter the DNS name or the IP address of the authentication server.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></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><strong>Authentication Port</strong></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><strong>Accounting Port</strong></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><strong>Mechanism</strong></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>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Server Timeout</strong></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><strong>Max Number of Retries</strong></td>
<td>Specify the maximum number of times the pod should retry failed requests to the authentication server.</td>
</tr>
<tr>
<td><strong>Realm Prefix</strong></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.</td>
</tr>
<tr>
<td></td>
<td>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><strong>Realm Suffix</strong></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 <a href="mailto:of@example.com">of@example.com</a> was specified here, the system sends <a href="mailto:user1@example.com">user1@example.com</a> to the authentication server.</td>
</tr>
</tbody>
</table>

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

You can configure a secondary authentication server to provide for high availability. Enable the **Auxiliary Server** toggle and complete the fields as described in **Step Primary Server section**.

**Validate and Proceed, and then Start the Pod Deployment Process**

After you click **Validate & Proceed**, the system verifies your specified values. If everything validates, the wizard displays a summary of the information for your review. Then you start the deployment process.

**Procedure**

1 Click **Validate & Proceed**.

The system validates your specified values, such as:

- Are the specified address ranges for the to-be-created subnets valid and non-overlapping with other addresses 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.
- Are any uploaded certificate files in the correct PEM format.
If you selected to use an existing management subnet, does it have the Microsoft.SQL service endpoint enabled on that subnet?

**Important** Starting with the September 2019 service release, new pod deployments require the Microsoft.SQL service endpoint enabled on the management subnet to support use of the pod's Microsoft Azure PostgreSQL database. If you see a validation error similar to the following screenshot that lists your selected subnet, it means the pre-existing management subnet that you selected in the wizard is missing that Microsoft.SQL service endpoint configured on it. At this point, you can log in to the Microsoft Azure portal and enable the Microsoft.SQL service endpoint on the subnet. Then you can resubmit the wizard to deploy the pod. For some details on how to enable that endpoint, see In Advance of Pod Deployment, Create the Horizon Cloud Pod's Required Subnets on your VNet in Microsoft Azure.

If everything validates, the summary page displays.

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

2 On the final wizard step, review the summarized information and click **Submit**.

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

Deploying your first pod can take up to an hour. Until the pod is successfully deployed, a progress icon is displayed in the console's Getting Started screen. You might need to refresh the screen in your browser to see the progress. The browser-based user interface can time out after approximately 30 minutes and ask you to log back in.

**Important**  The pod's pending stage typically lasts up to ten minutes. However, when deploying a pod in Microsoft Azure China cloud, the overall deployment process can take up to seven (7) 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 pod has not moved from Pending to Downloading state after 20 minutes, and you are not deploying into Microsoft Azure China, the system automatically puts the pod into Error state and displays a message that states the pod cannot connect to the cloud services and to check the networking connectivity in your Microsoft Azure environment.

If the display shows the pod is in Error state because the deployed jump box VM could not download the binaries it needs from the cloud service, there is likely an issue with your environment's network configuration. For example, the VNet's configured DNS might not be resolving internal or external names or the required outbound ports are not open or are blocked by your firewall. Sometimes there is a temporary loss of connectivity to packages.microsoft.com site used to download the Microsoft Azure Command Line Interface software. You can run some tests to verify if your environment's networking is configured properly for the pod's requirements. See [Troubleshooting If You Encounter Pod Deployment or First-Time Domain Bind Issues](#).

Throughout the pod deployment process, the Getting Started page's Capacity section indicates the various stages the process goes through (pending, downloading, building, connecting, and so on).

![Building pod: Connecting](image)

The following table gives some approximate sample durations for the stages in building the pod.

**Important**  The actual durations you experience in your deployment's progress will vary depending on the network latencies that exist at the time.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Sample duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Downloading</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Building</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Connecting</td>
<td>10 minutes</td>
</tr>
</tbody>
</table>
When the pod is successfully deployed:

- Horizon Cloud sends a notification email to the account owner that is identified in the corresponding Horizon Cloud customer account record. The email states the pod onboarding is complete.

- A green checkmark is displayed in the Getting Started screen.

At this point, because your Active Directory domain is not yet registered with the pod, a **Delete Pod** option is available in the **Manage** menu. If the deployment process fails for some reason or if you dislike the values you used and want to start over before registering your Active Directory domain, you can click **Manage > Delete Pod** to delete the artifacts that were deployed. When the screen indicates the pod is successfully deleted, you can start the process over by clicking **Manage > Add Pod** again. The following screenshot illustrates the location of the **Manage > Delete Pod** option.

If you choose to delete the pod from this point, due to network latency, the Getting Started page might indicate the pod is fully deleted before all of the pod-related artifacts are completely deleted from your Microsoft Azure environment. Before running the pod deployment wizard again after deleting the new pod, take the following steps:

1. Log out of the Horizon Cloud user interface.
2. Log in to the Microsoft Azure portal.
3. Navigate to your VNet.
4. If you had the deployer automatically create the pod’s subnets, verify that no pod-created subnets exist and that the address ranges that you specified for the pod’s subnets have been removed from the VNet's address space.

Then you can log back in to Horizon Cloud to run the pod deployment wizard again.
What to do next

Expand the General Setup section of the Getting Started screen and complete the required task of registering an Active Directory domain. Registering Active Directory is the next required step. After registering the domain and setting the Super Administrator role for a domain group, the system makes all of the console accessible to you. Then you continue management of this pod in the console. See the Getting Started chapter of the Horizon Cloud Administration Guide. After registering the Active Directory domain, follow the Getting Started wizard to see which task to complete next.

You must set up the appropriate CNAME records in your DNS server according to the type of gateway you specified.

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

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

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

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

When both the external and internal gateway configurations use the same FQDN, after the pod is deployed you must configure the routing of the incoming end-user client traffic to the appropriate load balancer resource in the gateways' resource groups. The goal is to set up the routing so that client traffic from the Internet is routed to the external gateway's Microsoft Azure Public Load Balancer and client traffic from your intranet is routed to the internal gateway's Microsoft Azure Internal Load Balancer. When both gateways have the same FQDN, you configure Split DNS (Split Domain Name System) to resolve the gateway address either to the external gateway or internal gateway depending on the origin network of the end-user client's DNS query.

See the Horizon Cloud Administration Guide for the steps to locate the load balancer information in the pod's details page.
If you specified RADIUS two-factor authentication for the pod's gateway configurations, you must complete the following tasks.

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

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

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

Troubleshooting If You Encounter Pod Deployment or First-Time Domain Bind Issues

If your environment’s networking is not configured properly for use with the Horizon Cloud pod in Microsoft Azure, the process to build out the pod can get stuck in PENDING state or the post-deployment action to domain bind to your Active Directory environment might fail. The two most common network-related causes are failing to open the required outbound ports and failing to enable the DNS to resolve both internal and external addresses. By following the troubleshooting steps here, you can run some tests to verify the required outbound ports are open and the DNS can resolve both internal and external addresses.

The overall networking requirements for successfully deploying a pod are stated in the prerequisites checklist document, located at this PDF link and described in Configure the DNS Server Settings Needed by the VNet Topology You Will Use for Your Horizon Cloud Pods in Microsoft Azure and DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features. If your environment’s networking does not meet those requirements, you will encounter one or both of these two issues:
## Issues
- The Getting Started page shows the pod in pending state and it never proceeds to connecting state. Usually a pod is in pending state for about 10 minutes (except when deploying a pod into Microsoft Azure China cloud, which takes longer).
- Even when the pod has successfully deployed, when you attempt to register your Active Directory, the domain-bind step fails with the error `Unable to register Active Directory`

<table>
<thead>
<tr>
<th>Common causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required outbound ports are not open, or are blocked by your firewall environment. If the required outbound ports are not open or are blocked by a firewall, it prevents the pod software from securely downloading into the Microsoft Azure cloud environment and connecting back to the Horizon Cloud cloud control plane. As a result, the pending state issue occurs.</td>
</tr>
<tr>
<td>The VNet DNS server is not properly configured to point to a valid DNS server that can resolve both internal and external machine names.</td>
</tr>
<tr>
<td>Though the VNet DNS server is properly pointing to a DNS server, that DNS server cannot resolve both internal and external machine names.</td>
</tr>
</tbody>
</table>

If no DNS resolution for external machine names is provided to the VNet, the pending state issue and domain-bind issue can occur. For example, if the DNS cannot resolve to the Active Directory on the Domain Controllers, the domain-bind step fails. For details about the VNet DNS configuration, see [Configure the DNS Server Settings Needed by the VNet Topology You Will Use for Your Horizon Cloud Pods in Microsoft Azure](#).

To run some tests that will check that the DNS configuration can resolve internal and external names and check that the required outbound ports are open, you deploy a small test virtual machine (VM) into your Microsoft Azure subscription and then use that VM to run these networking tests. The high-level sequence of troubleshooting steps is:

1. Create an SSH key pair.
2. Create the test VM in your Microsoft Azure subscription.
3. Connect to that test VM.
4. Run the networking tests.
5. When the testing is done, delete the test VM and all the test-related artifacts that were created in your Microsoft Azure environment for doing this troubleshooting.

**Note** If you do not delete the test-related artifacts and you later use the console's **Delete** action to delete the pod, unexpected results might occur. When deleting a pod, the system checks the pod's subnets to verify that everything connected to the subnets belongs to the pod itself (according to the pod's ID). If the system determines additional VMs, VM disks, IPs, or other artifacts are connected to the pod's subnets, the system cannot cleanly delete the pod.
For details about running the troubleshooting tests, see the following sections.

**Important** If you are directing all traffic out through your on-premises network and only allowing authenticated traffic to pass, but you did not provide values for using a proxy in the pod deployment wizard, even though all of these manual tests will succeed, the traffic sent by an unauthenticated source, the jump box, will fail. The symptom of this situation is the pod deployment is stuck in pending state. If you are in this situation, you must delete the pod from the Getting Started page, re-run the pod deployment wizard, and specify the required proxy information.

**Procedure**

1. **Create an SSH Key Pair**
   You need an SSH key pair to authenticate to the test Linux VM that you will be deploying into your Microsoft Azure subscription. You create the key pair on the system you will use to SSH connect to the test VM. This step is optional if you already have a key pair on that system.

2. **Create the Test Virtual Machine in Your Microsoft Azure Subscription**
   You will use a test Linux virtual machine (VM) in your Microsoft Azure environment to run the tests that check the network connectivity that is configured for your Horizon Cloud pod.

3. **Use SSH to Connect to the Test VM**
   Make a SSH (Secure Shell) connection to the test VM so that you can run the network connectivity tests in your Microsoft Azure environment.

4. **Run the Tests to Check Networking in Your Microsoft Azure Environment**
   You run these tests to verify these two network-related areas are configured properly: that the DNS can resolve both internal and external addresses and that the required outbound ports are open. You run these tests using your test VM.

5. **Delete the Test VM After You Complete the Tests**
   When you have finished the tests to check your Microsoft Azure network configuration and no longer need the test VM, you should delete it and all of its related artifacts from your Microsoft Azure environment.

### Create an SSH Key Pair

You need an SSH key pair to authenticate to the test Linux VM that you will be deploying into your Microsoft Azure subscription. You create the key pair on the system you will use to SSH connect to the test VM. This step is optional if you already have a key pair on that system.

You can use either a Microsoft Windows or a Linux system to create this SSH key pair. The steps for both types of systems are described here. Choose the steps most suitable for your situation.

#### Create an SSH Key Pair on a Microsoft Windows System

Use these steps when you will be using a Microsoft Windows system to SSH connect to the test Linux VM that you will be deploying into your Microsoft Azure subscription.
When you create the test VM in Microsoft Azure, you will use the contents of the generated public key file. If you already have an existing SSH key pair on the Microsoft Windows system that you will use to connect with the test VM, then you can skip this step and proceed with creating the test VM, as described in Create the Test Virtual Machine in Your Microsoft Azure Subscription.

By following these steps, you generate the SSH key pair, copy the public key file’s contents so you can use it when creating the test VM, and load the private key into the PuTTY Pageant tool. Pageant is an SSH authentication agent that can hold your private keys in memory. By holding the private key in memory, the private key is automatically applied against any SSH session from that Microsoft Windows system, making it easier to use.

Prerequisites

A Microsoft Windows system does not have SSH key-pair software installed on it by default. Verify that SSH key-pair generating software is installed on the system you are planning to use. You can use any SSH key-pair generating software. The steps below describe using the PuTTY software on Microsoft Windows to create the SSH key pair. You can obtain the PuTTY software from www.putty.org. After the installation, the PuTTY suite of tools is available. The following screenshot shows an example of the PuTTY tools in the Start menu.

Procedure

1. On your Microsoft Windows system, launch PuTTYgen (the PuTTY key generator).

   On Microsoft Windows 10, the PuTTYgen choice in the Start menu looks like

   ![PuTTYgen](image)

   The PuTTY Key Generator window displays. As highlighted in the following screenshot, the goal is to generate a public-private key pair, of type SSH-2 RSA, and having 2048 bits.
2 Verify that **SSH-2RSA** is selected, **2048** is set for the number of bits, and then click **Generate**. The window changes to the Key window that displays a progress bar.

3 Move your cursor around randomly in the blank area underneath the progress bar. Moving your cursor around in the area adds required randomness into the process.
4 Save the private key to the system by entering a key passphrase and click **Save private key**.

**Note** Using a key passphrase is an optional best practice. However, if you click **Save private key** without entering a key passphrase, a pop-up window asks you to confirm whether you want to save the private key without a key passphrase.

The private key is saved as a PPK file. After you click **Save private key**, you can browse to a directory in the local system, type a file name, and save the file.

5 Use the **Save public key** button to save the public key to a location where you can copy it from when you create the test VM.

6 Launch Pageant, the PuTTY SSH authentication agent.

On Microsoft Windows 10, the Pageant choice in the Start menu looks like ![Pageant](image). When you click it, the Pageant icon of a computer wearing a hat is loaded into the system tray.
The following screenshot shows the Pageant icon loaded into a Microsoft Windows 10 system tray.

7 Add your private key to Pageant by right-clicking that system tray icon, clicking Add Key, and using the file selection window to navigate to and select your saved private key (PPK) file.

Note If you specified a key passphrase when you saved the private key file earlier, a box is displayed for you to type that passphrase.

Results
At this point, the private key is loaded into Pageant. You can use the View Keys choice on the action menu to see the key in the list of loaded keys. When you start an SSH session using PuTTY, PuTTY will retrieve the key automatically from Pageant and use the key to authenticate without you having to type your passphrase. Later, when you are finished running SSH sessions and want to shut down Pageant, use the Exit choice from the Pageant system tray icon’s right-click menu.

What to do next
Create the test VM by following the steps in Create the Test Virtual Machine in Your Microsoft Azure Subscription.

Create an SSH Key Pair on a Linux System
Use these steps when you will be using a Linux system to SSH connect to the test Linux VM that you will be deploying into your Microsoft Azure subscription.

In the steps to create the test VM in Microsoft Azure, you will use the contents of the generated public key file. If you already have an existing SSH key pair on the Linux system that you will use to connect with the test VM, then you can skip this step and proceed with creating the test VM, as described in Create the Test Virtual Machine in Your Microsoft Azure Subscription.
Prerequisites

Before performing these steps, ensure that you will not overwrite an existing SSH key pair that you want to keep for other purposes. On a Linux system, the SSH public and private key files are created in the Linux ~/.ssh/id_rsa directory by default. If an SSH key pair exists in that directory and you use the same file name when running this command, or if you specify a different location in the command and an SSH key pair already exists in that location, that existing one is overwritten.

Procedure

1. On your Linux system, open a bash shell.
2. In the bash shell, type the following command:

   ```bash
   ssh-keygen -t rsa -b 2048
   ```
3. Follow the on-screen instructions about entering a file in which to save the key, entering a passphrase, and confirming the passphrase.

   Here is a sample of the on-screen instructions, where mykey was entered as the file in which to save the key.

   ```bash
   -bash-4.1$ ssh-keygen -t rsa -b 2048
   Generating public/private rsa key pair.
   Enter file in which to save the key (/mts-cm/home/user1/.ssh/id_rsa): mykey
   Enter passphrase (empty for no passphrase): 
   Enter same passphrase again: 
   ```

   **Note** Using a key passphrase is an optional best practice.

   The private key is saved in the file that you specify and the public key is saved to a file with that same name and a .pub extension. Using the example above of entering mykey as the file, the sample output would be:

   ```bash
   Your identification has been saved in mykey.
   Your public key has been saved in mykey.pub.
   ```

What to do next

Create the test VM by following the steps in Create the Test Virtual Machine in Your Microsoft Azure Subscription.

Create the Test Virtual Machine in Your Microsoft Azure Subscription

You will use a test Linux virtual machine (VM) in your Microsoft Azure environment to run the tests that check the network connectivity that is configured for your Horizon Cloud pod.
Prerequisites

Verify that you have the SSH public key that you created as described in Create an SSH Key Pair. You will provide that public key in the VM creation wizard so that the VM will trust SSH connections coming from the system that has the corresponding private key.

Verify you have the name of the virtual network (VNet) that is the same one that you are using to deploy your pod, as described in Configure the Required Virtual Network in Microsoft Azure.

If you tried to deploy a pod and the deployment process failed at some point, the process might already have created the pod’s management subnet in the VNet.

- If so, it is recommended you deploy the test VM on to that subnet. To identify if the pod’s management subnet exists on the VNet, log in to the Microsoft Azure portal, navigate to that VNet, and examine the list of subnets it has. You can navigate to the VNet using the Virtual networks choice in the left navigation bar. The pod’s management subnet will have a name in the pattern `vmw-hcs-podID-net-management`, where podID is the pod’s UUID.

- If the pod deployment process did not create the pod’s management subnet on the VNet, you can choose any available subnet on the VNet or create a new subnet for the test VM to use.

Procedure

1. Log in to the Microsoft Azure portal.

2. From the portal’s left navigation bar, click Virtual machines and then click + Add.


4. Select Resource Manager as the deployment model and click Create.

The Create Virtual Machine wizard opens to the steps for configuring basic settings.
5  Provide the VM’s basic settings and then click **OK** to move to the next wizard step.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the VM.</td>
</tr>
<tr>
<td>VM disk type</td>
<td>Keep the default SSD setting.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter a user name that meets the Microsoft Azure user name requirements, as described in the Microsoft documentation <a href="#">here</a>.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> Make a note of this name because you will need to use it later.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>Select <strong>SSH public key</strong>.</td>
</tr>
<tr>
<td>SSH public key</td>
<td>In this field, paste your SSH public key that you created when you created the SSH key pair. The pasted-in contents must start with the line <code>--- BEGIN SSH2 PUBLIC KEY -----</code> and end with the line <code>--- END SSH2 PUBLIC KEY -----</code> from your public key.</td>
</tr>
<tr>
<td>Subscription</td>
<td>Select the same subscription that you are using for your pod.</td>
</tr>
<tr>
<td>Resource group</td>
<td>The recommended choice is to create a new resource group for the test VM and its related artifacts like its disk. Select <strong>Create new</strong> and enter a name for the new resource group. Even though you can use an existing resource group with this test VM, a resource group specific for the test VM is recommended because it is easier to delete the VM and its related artifacts simply by deleting the whole resource group when you are finished running the tests.</td>
</tr>
<tr>
<td>Location</td>
<td>Select the same physical geographic region that you are using for your pod.</td>
</tr>
</tbody>
</table>
6 In the wizard's size step, click a VM size click and then Select to move to the next wizard step.

Because this is expected to be a short-lived VM, used only to complete the verification tests, you can pick any size. However, because smaller sizes usually have lower associated costs in Microsoft Azure, choosing a small size for the test VM is typical. The following screenshot illustrates the example of choosing the D2S_V3 Standard size.
In the wizard's settings step, specify the key networking choices for the test VM.

You make three important choices in this wizard step. The following screenshot illustrates these three key items. After setting the three key network options, you can retain all of the other default values.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual network</strong></td>
<td>You must select the same VNet that you are using to deploy your pod. This VNet should be the one that you configured according to the details in the prerequisites checklist and as described in Configure the Required Virtual Network in Microsoft Azure.</td>
</tr>
</tbody>
</table>
| **Subnet**   | If you already tried to deploy the pod and the process failed, the pod's management subnet might have been created in the virtual network. If the subnet is there, it is recommended to select that subnet for this test VM. Click the Subnet choice to navigate to the subnets that exist on the selected virtual network. You might have to hover over the subnet to see its full name in the tooltip. This screenshot illustrates hovering over a subnet to see the naming pattern of a pod's management subnet, in the pattern vmw-hcs-podID-net-management. If the pod deployment process did not create the pod's management subnet on the VNet, select the subnet on your VNet that you identified to use for the test VM (as described in the prerequisites above).  
**Note** If the pod was successfully deployed, but you are troubleshooting domain-join issues, you might select the pod's desktop subnet for the test VM instead of the management subnet, because domain-join operations are used with the desktop images that get connected to that desktop subnet. |
| **Public IP address** | Select this choice so that the created test VM will have a public IP address assigned to it. Having a public IP address enables you to connect to it over the wide area network (WAN).  
**Note** Using a public IP might not be technically feasible in your networking configuration. If you cannot create the test VM with a public IP, you will need to have network connectivity from your local system to the subnet you selected in the Subnet field or will need to connect to some other machine on your network and then inbound connect to the test VM. |

8. Click **OK** to move to the wizard's summary step.

9. In the summary step, verify that the key pieces of information (subscription, location, virtual network, and subnet) match the ones that you are using for your pod, and then click **Create**.
Results

Creation of the test VM starts running. Typically, you can see the process running on your Microsoft Azure dashboard, as illustrated in the following screenshot.

Deploying the VM usually takes around five to ten minutes. When the VM is fully deployed, it is in Running state. The following screenshot illustrates the details of a sample test VM.

When you see the test VM is up and running, connect to it. Follow the steps in Use SSH to Connect to the Test VM.

Use SSH to Connect to the Test VM

Make a SSH (Secure Shell) connection to the test VM so that you can run the network connectivity tests in your Microsoft Azure environment.

SSH Connect to the Test VM from a Microsoft Windows System

You make this connection from the Microsoft Windows system that has the private key that corresponds to the public key you specified when you created the test VM.

Prerequisites

Verify you have the test VM's IP address and the user name you specified when you created the VM.
On a Microsoft Windows system, PuTTY is typically used. To make it easy for PuTTY to load your private key when you start the SSH session, before starting PuTTY, start Pageant as described in Create an SSH Key Pair on a Microsoft Windows System and add the SSH private key to the Pageant key list. The SSH private key must match the public key you specified when creating the test VM. When the private key is loaded into Pageant, the PuTTY SSH session will use that private key automatically.

**Procedure**

1. Launch PuTTY.
   
   The PuTTY Configuration window opens.

2. In the PuTTY Configuration window, specify the host name, select SSH, and then click Open.

   In the PuTTY Configuration window's Host Name field, type a string in the pattern

   `testvm_username@testvmip`

   substituting the test VM's user name and IP address for `testvm_username` and `testvmip` in the string.

   **Important** After you click Open, when this is the first time you connect to the test VM, a PuTTY security message displays stating that the server's host key is not cached and displays the server's rsa2 key fingerprint. You can continue to make the connection by either clicking Yes to add the server's host key into PuTTY's cache or No to connect without adding the key to PuTTY's cache. If you suspect the connection might not be going to your test VM, click Cancel to abandon the connection and return to the PuTTY Configuration window to verify your host name entry.

   The following screenshot is an illustration of the window using the sample

   `testvmadmin@40.121.180.132`
Results

When the SSH connection is established, a command-line window displays that looks similar to the following screenshot.
What to do next

Now that you are connected to the test VM, you can run the tests to check network connectivity within your Microsoft Azure environment. Follow the steps described in Run the Tests to Check Networking in Your Microsoft Azure Environment.

SSH Connect to the Test VM from a Linux System

You make this connection from the Linux system that has the private key that corresponds to the public key you specified when you created the test VM.

Prerequisites

Verify you have the test VM's IP address and the user name you specified when you created the VM.

Procedure

1. Open a bash shell.
2. At the bash shell $ prompt, enter the ssh command as below, substituting the test VM's IP address and the user name for testvmip and testvm_username in the command:

   ```bash
   ssh testvm_username@testvmip
   ```

   For example, using the test VM details from the examples in Create the Test Virtual Machine in Your Microsoft Azure Subscription, the sample command would look like:

   ```bash
   ssh testvmadmin@40.121.180.132
   ```

Results

When the SSH connection is established, a command-line window displays that looks similar to the following screenshot.
What to do next

Now that you are connected to the test VM, you can run the tests to check network connectivity within your Microsoft Azure environment. Follow the steps described in Run the Tests to Check Networking in Your Microsoft Azure Environment.

Run the Tests to Check Networking in Your Microsoft Azure Environment

You run these tests to verify these two network-related areas are configured properly: that the DNS can resolve both internal and external addresses and that the required outbound ports are open. You run these tests using your test VM.

The pod relies on DNS to resolve both internal and external addresses. The first two tests here check whether the DNS configured in your network environment can resolve known FQDNs for internal and external addresses.

**Important** If you are directing all traffic out through your on-premises network and only allowing authenticated traffic to pass, but you did not provide values for using a proxy in the pod deployment wizard, even though all of these manual tests will succeed, the traffic sent by an unauthenticated source, the jump box, will fail. The symptom of this situation is the pod deployment is stuck in pending state. If you are in this situation, you must delete the pod from the Getting Started page, re-run the pod deployment wizard, and specify the required proxy information.

**Prerequisites**

Before running these tests, verify that you created a test VM in your Microsoft Azure subscription and have an SSH connection to it, as described in Create the Test Virtual Machine in Your Microsoft Azure Subscription and Use SSH to Connect to the Test VM.
Obtain the IP addresses and fully qualified domain names (FQDNs) for servers that are internal to your network that you expect to be reachable from the VNet, such as your Active Directory Domain Controller. You will use this information in the DNS verification test.

**Procedure**

1. **Check that DNS is working in your environment to resolve internal FQDNs by using the `dig` command to query a known domain name that is internal to your VNet in Microsoft Azure.**

   In the SSH connection window, issue the `dig` command to query the domain name of a server that you know is internal to your network, such as your Active Directory Domain Controller.

   ```
   dig internal-domain-name
   ```

   Where `internal-domain-name` is the fully qualified domain name of a server that you know is internal to your network.

   `dig` (Domain Information Groper) is a command-line tool for network troubleshooting. By running this command using an internal host name, the result verifies that your DNS configuration can resolve internal addresses properly. If your DNS configuration can resolve the `internal-domain-name` used in the command, the command output will return the correct IP address associated with that domain name.

   For example, assume the VNet is configured with an internal Active Directory server having Active Directory Domain Controller with a DNS entry of `skylo.local` and an IP address of `192.168.0.15`. Issuing `dig skylo.local` would check whether the VNet's DNS configuration can resolve that internal `skylo.local` server name:

   ```
   testvmadmin@HCS-testingVM:~$ dig skylo.local
   ; <<>> DiG 9.10.3-P4-Ubuntu <<>> skylo.local
   ;; global options: +cmd
   ;; Got answer:
   ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64899
   ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
   
   ;; OPT PSEUDOSECTION:
   ;; EDNS: version: 0, flags:; udp: 4000
   ;; QUESTION SECTION:
   ;skylo.local.                   IN      A
   
   ;; ANSWER SECTION:
   skylo.local.            600     IN      A       192.168.0.15
   
   ;; Query time: 1 msec
   ;; SERVER: 192.168.0.15#53(192.168.0.15)
   ;; WHEN: Mon Mar 26 20:58:01 UTC 2018
   ;; MSG SIZE  rcvd: 56
   testvmadmin@HCS-testingVM:~$
   ```
The test is successful when the ANSWER SECTION indicates the provided host name was resolved to the IP address that you expect for that host name.

**Note** Sometimes DNS is not 100% reliable, and some requests resolve fine while others fail. If issuing the command fails the first time, run the command for ten to twenty iterations and see whether you get reliable responses each time.

2 Check that DNS is working in your environment to resolve external FQDNs by using the `dig` command to query a known external domain name.

In the SSH connection window, issue the `dig` command to query an external industry-standard domain name, such as `vmware.com` or `microsoft.com`.

```
dig external-domain-name
```

Where `external-domain-name` is a fully qualified domain name that is external to your VNet. For example, issuing `dig vmware.com` would check whether the VNet’s DNS configuration could resolve that external name:

```
testvmadmin@HCS-testingVM:~$ dig vmware.com
;; <<>> DiG 9.10.3-P4-Ubuntu <<>> vmware.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38655
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;vmware.com.                    IN      A

;; ANSWER SECTION:
vmware.com.             150     IN      A       107.154.105.19
vmware.com.             150     IN      A       107.154.106.19

;; Query time: 28 msec
;; SERVER: 192.168.0.15#53(192.168.0.15)
;; WHEN: Mon Mar 26 21:14:29 UTC 2018
;; MSG SIZE  rcvd: 71

testvmadmin@HCS-testingVM:~$
```

In the above example, the ANSWER SECTION indicates the external domain name `vmware.com` was properly resolved to two IP addresses.

**Note** You can repeat this test using various external domain names, such as `azure.com` or `microsoft.com`, to verify that your DNS can resolve different external names.
If the DNS tests do not work, verify your network configurations and your DNS server. Check that you added your DNS server to your VNet.

**Important** If you find that you need to add your DNS server to your VNet or you have to change the VNet’s DNS server configuration, you must restart all VMs that are connected to that VNet for them to pick up the change. If you change the VNet’s DNS server configuration and do not restart all of the VMs connected to that VNet, the changes will not propagate correctly on the VNet.

3. Check that the required outbound ports are available by using the `netcat` command.

Horizon Cloud requires some outbound ports to be opened, so that the pod software can be securely downloaded into your Microsoft Azure environment and so that the pod can connect back to the Horizon Cloud control plane. As described in DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features, the following outbound TCP ports are required to be open from the pod’s management subnet: port 80, 443, and 11371. By running the `netcat` command as indicated in the command below, you can verify that those outbound ports are open as required.

In the SSH connection window, issue the following commands (one per port).

**Note** The command below to test port 11371 specifies `packages.microsoft.com` to test that connection, while the other two lines test the outbound connection to the Horizon Cloud control plane.

```
Connection to cloud.horizon.vmware.com 80 port [tcp/http] succeeded!
```

```
Connection to cloud.horizon.vmware.com 443 port [tcp/https] succeeded!
```

```
Connection to packages.microsoft.com 11371 port [tcp/hkp] succeeded!
```

When a port is properly open, the `netcat` command returns the `succeeded!` line for its test.

If the `netcat` commands return failures, check your Microsoft Azure network connections, your Network Security Groups in your subscription, and any firewalls you might have in place. Ensure your network configuration meets the DNS, ports, and protocol requirements that the pod needs for deployment, as described in DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features.

**Results**

If the above tests succeed, you will be able to successfully deploy your pod.

**Note** If you will be configuring optional features for use with your pod, such as Radius two-factor authentication or True SSO, additional ports might be needed for those purposes. You can use the above outbound port testing techniques to verify such ports are properly open.
What to do next

When you have completed the test, you should delete the test VM and all of its related artifacts, such as its VM disk, IP address, NIC, from your Microsoft Azure environment. Ideally you would have created a resource group for the test VM and can simply delete that resource group to delete all of the VM's artifacts. Follow the steps in Delete the Test VM After You Complete the Tests.

Important  If you do not delete all of the test VM's artifacts from your Microsoft Azure environment and you connected the VM to one of the pod's subnets, if you later try to delete the pod from your Horizon Cloud environment using the Delete action on the pod, the system might not be able to fully delete the pod due to those remaining connected artifacts. By default, when you use the Delete action to delete a pod, Horizon Cloud deletes those resource groups and subnets that it created for the pod. Microsoft Azure will prevent deletion of subnets that are still in use. If your test VM's artifacts are connected to the pod's subnets, then those subnets cannot be deleted and the pod deletion will be incomplete. To prevent this situation, ensure all of the test VM's artifacts are deleted after you have successfully deployed your pod.

Delete the Test VM After You Complete the Tests

When you have finished the tests to check your Microsoft Azure network configuration and no longer need the test VM, you should delete it and all of its related artifacts from your Microsoft Azure environment.

Important  If you do not delete all of the test VM's artifacts from your Microsoft Azure environment and you connected the VM to one of the pod's subnets, if you later try to delete the pod from your Horizon Cloud environment using the Delete action on the pod, the system might not be able to fully delete the pod due to those remaining connected artifacts. By default, when you use the Delete action to delete a pod, Horizon Cloud deletes those resource groups and subnets that it created for the pod. Microsoft Azure will prevent deletion of subnets that are still in use. If your test VM's artifacts are connected to the pod's subnets, then those subnets cannot be deleted and the pod deletion will be incomplete. To prevent this situation, ensure all of the test VM's artifacts are deleted after you have successfully deployed your pod.

Procedure

1  Log in to the Microsoft Azure portal.
2 Use one of the following methods to delete the test VM, depending on how you deployed it.

- If you deployed the test VM into its own resource group and you are not using that group for any other purpose, you can delete the entire resource group.

  **Caution** To avoid inadvertently deleting other items, make sure that the resource group contains only your test VM and its associated objects such as its disk and network adapters before deleting the resource group.

  a In the portal’s left hand navigation, click **Resource groups** and search for the test VM’s resource group.

  b Click the resource group’s name to see the items in that resource group.

  c Click **Delete resource group**. In the confirmation message, type in the resource group’s name and then click **Delete**.
If you need to delete the test VM without deleting an entire resource group, you can use the portal's search box to search for the test VM's name. The results of this search will list the VM and all of its associated objects (disk, network interfaces, public IP address, and so on). Then delete each object individually.
Now That Your Very First Pod Is Completely Deployed and Connected to Horizon Cloud

Congratulations on deploying your first ever Horizon Cloud pod!

The console’s Getting Started page indicates when you have successfully created a cloud-connected pod.

The following screenshot illustrates what the page looks like when your very first pod is one deployed into Microsoft Azure.

At this point, you must perform the steps to register Horizon Cloud with the Active Directory domain that you want to use with this pod. The Horizon Cloud Administration Guide provides those detailed steps. See the topic named Getting Started Using Your Horizon Cloud Environment and its subtopics.
Revision History — Changelog — Onboarding to Horizon Cloud for Microsoft Azure and Horizon Pods

This documentation topic provides the history of substantive changes to Onboarding to Horizon Cloud for Microsoft Azure and Horizon Pods — Deployment Guide.

**Note** Only substantive and significant changes made to the guide's topics starting from September 17, 2019 are provided. Details about revisions prior to that date are not available. Also, minor content revisions such as fixing typos, format changes such as turning lists into tables, and other such insignificant changes are not provided.

**March 9, 2021**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 MAR 2021</td>
<td>Updates for the new features corresponding to the March 9, 2021 What's New in the Horizon Cloud Release Notes.</td>
</tr>
</tbody>
</table>

**March 1, 2021**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 MAR 2021</td>
<td>Updates related to the removal of the requirement that the domain join account must be in an Active Directory group that has the Super Administrator role. This requirement is only when your pod fleet has Horizon Cloud pods in Microsoft Azure that are running a manifest older than 1600.0. For additional details, see Service Accounts That Horizon Cloud Requires for Its Operations.</td>
</tr>
</tbody>
</table>

**January 7, 2021**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
</table>

**December 15, 2020**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
</table>
### December 2, 2020

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
</table>

### November 24, 2020

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
</table>

### November 4, 2020

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
</table>

### October 8, 2020

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 OCT 2020</td>
<td>Updates for the new features corresponding to the October 8, 2020 What's New in the Horizon Cloud Release Notes.</td>
</tr>
</tbody>
</table>

### July 9, 2020 — October 7, 2020

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 Sep 2020</td>
<td>Updates made to the screenshots in this guide to align with the availability of the Manage menu on the Getting Started page. Also an update to Horizon Cloud Connector Known Considerations.</td>
</tr>
<tr>
<td>18 AUG 2020</td>
<td>Updates made to align this guide with the Horizon documentation to adopt the terms base image and golden image, as appropriate for each topic's context.</td>
</tr>
<tr>
<td>5 AUG 2020</td>
<td>Updates made to align this guide with the availability of the new regional cloud control plane in Japan. The following documentation topics are updated for that regional control plane's DNS names: DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features and DNS, Ports, and Protocols Requirements When Using Horizon Cloud Connector and a Horizon Pod.</td>
</tr>
<tr>
<td>13 JUL 2020</td>
<td>Pods that can have the high availability (HA) feature are now supported for Microsoft Azure Government (US Gov Virginia, US Gov Arizona, US Gov Texas).</td>
</tr>
<tr>
<td>9 JUL 2020</td>
<td>Updates for the new features corresponding to the July 9, 2020 What's New in the Horizon Cloud Release Notes.</td>
</tr>
</tbody>
</table>
# March 17, 2020 — July 8, 2020

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 JUN 2020</td>
<td>Updates made to align this guide with the June 9, 2020 What's New in the Horizon Cloud Release Notes. The regional names that appear in the Welcome email have been updated to use human-friendly names. The following doc topic is also updated to align with that change: DNS Requirements for a Horizon Cloud Pod in Microsoft and Related Service Features</td>
</tr>
<tr>
<td>27 MAY 2020</td>
<td>Updates made to align this guide with the May 27, 2020 What's New in the Horizon Cloud Release Notes.</td>
</tr>
<tr>
<td>14 APR 2020</td>
<td>Updates made to align this guide with the April 13, 2020 What's New in the Horizon Cloud Release Notes.</td>
</tr>
<tr>
<td>17 MAR 2020</td>
<td>Updates for the new features corresponding to the March 17, 2020 What's New in the Horizon Cloud Release Notes.</td>
</tr>
</tbody>
</table>

# December 13, 2019 — March 16, 2020

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 FEB 2020</td>
<td>Updated the following topics for the stated changes:</td>
</tr>
<tr>
<td></td>
<td>- Added Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read to the list in Operations Required by Horizon Cloud in Your Microsoft Azure Subscriptions.</td>
</tr>
<tr>
<td></td>
<td>- Added resource provider Microsoft.Sql to the list in Create the Required Service Principal Needed by the Horizon Cloud Pod Deployer by Creating an Application Registration.</td>
</tr>
<tr>
<td></td>
<td>- Added a row for the jumpbox VM and pod manager VM to reach the Unified Access Gateway VMs using port 9443/TCP to Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later. This port is required to configure settings in the Unified Access Gateway during pod deployment and whenever editing the pod to change its Unified Access Gateway settings.</td>
</tr>
<tr>
<td></td>
<td>- Corrected port 443 to 8433 as the port requirement for traffic from the pod's Unified Access Gateway VMs to the pod's Microsoft Azure load balancer for login authentication traffic, in Ports and Protocols Requirements for a Horizon Cloud Pod at the September 2019 Release's Manifest or Later.</td>
</tr>
<tr>
<td>13 JAN 2020</td>
<td>Updated proxy-related information for the Horizon 7 Cloud Connector. Updated topics include High-Level Workflow When You are Onboarding an Existing Horizon Pod That Is Deployed in a VMware SDDC as Your First Pod to Your Horizon Cloud Tenant Environment and Preparing to Run the Onboarding Wizard to Pair a Horizon Pod with Horizon Cloud Using Horizon Cloud Connector.</td>
</tr>
<tr>
<td>6 JAN 2020</td>
<td>New information added to topics about Enable SSH Access to the Horizon Cloud Connector Before Pairing It with Your Horizon Connection Server, VMware Horizon Pods with Horizon Cloud - Requirements Checklist - Updated as Appropriate for Connecting Pods Starting from the January 2021 Service Release.</td>
</tr>
</tbody>
</table>
### September 17, 2019 — December 12, 2019

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21 NOV 2019</td>
<td>Updated the resource providers list with additional ones needed for a subscription in Microsoft Azure related to the latest pod architecture, in Step 8 of documentation topic <a href="https://example.com">Create the Required Service Principal Needed by the Horizon Cloud Pod Deployer by Creating an Application Registration</a>.</td>
</tr>
<tr>
<td>17 SEP 2019</td>
<td>Updates for the new features corresponding to the September 17, 2020 What's New in the <a href="https://example.com">Horizon Cloud Release Notes</a>.</td>
</tr>
</tbody>
</table>