QUICK-START TUTORIAL
FOR VMWARE HORIZON
CLOUD ON MICROSOFT
AZURE
VMware Horizon
Table of Contents

VMware Horizon Cloud on Microsoft Azure 2.0
- Introduction
- Purpose
- Audience

Technical Introduction and Features
- About Horizon Cloud Service on Microsoft Azure
- Packaging, Licensing, and Service Models
- Features and Benefits

Components and Architecture
- About System Architecture and Components
- VMware Horizon Cloud Service Components
- Horizon Cloud Service on Microsoft Azure Components

A: Setting Up
- About Setup
- Exercise A1: Reviewing the Workflow
- Exercise A2: Creating the VNet
- Exercise A3: Configuring VNet Peering (Optional)
- Exercise A4: Configuring the DNS Server
- Exercise A5: Creating a Service Principal Authentication Key
- Exercise A6: Assigning the Contributor Role to the Service Principal
– **Exercise A7: Verifying Required Resource Providers**

**B: Deploying a Horizon Cloud Service Pod**

– **About Pod Deployment**
– **Exercise B1: Deploying the Horizon Cloud Service Pod**
– **Exercise B2: Binding to the Active Directory Domain**
– **Exercise B3: Defining VM Types & Sizes**

**C: Creating an Image**

– **About Image Creation**
– **Exercise C1: Importing VMs from Microsoft Azure Marketplace**
– **Exercise C2: Customizing the Windows VM**
– **Exercise C3: Converting the Master VM to an Image**

**D: Deploying a Farm**

– **About Farm Deployment**
– **Exercise D1: Creating a Farm**
– **Exercise D2: Exploring RD Session Host Power Management**
– **Exercise D3: Adding Applications from the Farm**

**E: Assigning Resources**

– **About Assignments**
– **Exercise E1: Checking Desktop Capacity Allocation**
– **Exercise E2: Assigning Applications from the Farm**
– **Exercise E3: Creating RDSH Session Assignments**
– **Exercise E4: Assigning Floating Desktops**
– **Exercise E5: Assigning Dedicated Desktops**
Exploring Reporting and Analytics

– About Monitoring and Analytics

– Exploring Dashboard and Activity

– Exploring Reports and Notifications

Exploring VMware User Environment Manager

– Installing VMware User Environment Manager on Microsoft Azure

– Exploring Deployment Options

– Optimizing VM Performance

– Using the NoAD Mode

Summary and Additional Resources

– Summary

– Terminology Used in This Tutorial

– Additional Resources

– About the Authors

– Feedback
Quick Start Tutorial for VMware Horizon Cloud on Microsoft Azure

VMware Horizon Cloud on Microsoft Azure 2.0

Introduction

This Quick-Start Tutorial introduces you to VMware Horizon® Cloud Service™ on Microsoft Azure. This solution combines the management functionality of the Horizon Cloud Service control plane with the cost-saving capacities of Microsoft Azure. You can take advantage of the Horizon Cloud Service to manage your desktops and remote applications. This includes managing VDI and RDS-hosted applications on Microsoft Azure infrastructure, as well as the flexibility to choose the deployment option that best meets the needs of your organization or use cases.

This Quick-Start Tutorial is relevant for VMware Horizon Cloud Services on Microsoft Azure 2.0, and describes the process of deploying Horizon Cloud Service components into your Microsoft Azure capacity. This process creates an entity called the Horizon Cloud Service pod (previously referred to as a node), which pairs with the control plane. You then use the control plane to create RDSH and session farms, and to manage and deliver virtual RDS-enabled Windows Servers and remote applications to your end users. You can also leverage the automation to perform basic VDI agent updates to floating and dedicated desktops.

Purpose

This Quick-Start Tutorial introduces you to Horizon Cloud Service on Microsoft Azure, and helps you to evaluate this product through a series of practical exercises. The Overview section describes the benefits, features, architecture, and components, and component interoperability. The subsequent sections provide exercises to help you deploy the Horizon Cloud Service pod into your Microsoft Azure capacity, and then to explore and evaluate this product and its core capabilities and key features.

Important: This Tutorial is for evaluation purposes, based on minimum required resources for a basic deployment, and does not explore all possible features. The resulting environment should not be used as a template for deploying a production environment. To deploy a production environment, see the Horizon Cloud Service documentation.

Audience

This guide is intended for security architects, engineers, and administrators who want to familiarize themselves with, or are in the process of implementing, a Horizon Cloud Service on Microsoft Azure infrastructure.

It is assumed that you have familiarity with Windows data center technologies such as Microsoft Azure and Active Directory, and knowledge of VMware Horizon 7 and VMware Unified Access Gateway. You should also be familiar with virtualization technology, cloud computing, network routing, and firewall security architecture. Knowledge of compatibility is also useful when using VMware Horizon Cloud Service on Microsoft Azure (see VMware Product Interoperability Matrices).

Note: Not all sections of this guide are necessarily applicable to your particular deployment. Optional sections are marked as such. If you have questions about the specifics of your order, see Getting Started with Horizon Cloud, or reach out to your VMware sales representative.

Technical Introduction and Features

About Horizon Cloud Service on Microsoft Azure

The VMware Horizon Cloud Service delivers virtual desktops and applications using a cloud platform that is scalable across multiple deployment options. The overall environment consists of the VMware-hosted cloud service, your designated capacity, and the VMware software deployed into that capacity.

The Horizon Cloud Service provides a single cloud control plane from which you can choose multiple deployment options. At any time, you can dynamically switch options to adjust to use cases changes, employee moves, economic shifts, and so on. These options consist of Horizon pods using:
• **Microsoft Azure capacity** - Public cloud infrastructure from Microsoft Azure, an Infrastructure-as-a-Service (IaaS) provider
• **On-premises capacity** - Hyper-converged infrastructure from partners such as Dell EMC, Hitachi, and QTC
• **VMware Cloud on AWS capacity** - Cloud-hosted capacity managed by VMware

The first option, Microsoft Azure, is the focus of this Quick Start Tutorial. You can connect your Microsoft Azure instance to your Horizon Cloud Service control plane for a comprehensive cloud-hosted solution for delivering virtualized Windows apps and desktops.

Setting up the environment involves deploying the required VMware software into your Microsoft Azure capacity. The deployed VMware software creates an appropriately configured entity called a Horizon Cloud Service pod, which pairs with the control plane. After the pod is deployed, you use the control plane to create RDSH farms and entitle remote desktops and applications to your end users, as well as to assign dedicated and floating Windows 10 desktops.

For more information, see the [Horizon Cloud Service on Microsoft Azure datasheet](#).

**Packaging, Licensing, and Service Models**

Horizon Cloud Service delivers virtual desktops and apps using a cloud platform that is scalable across multiple deployment options. Horizon Cloud Service is available in two subscription options:

- **Per named user**: For virtual environments with end users that require dedicated access to virtual machines (VMs) throughout the day
- **Per concurrent connection**: For virtual environments with a high number of users who share machines throughout the day, such as students or shift workers

You can bring your own hyper-converged infrastructure (HCI) or Microsoft Azure infrastructure, or purchase cloud-hosted infrastructure from VMware. For more information, see [How to Buy](#) and [Horizon Universal License](#).

**Features and Benefits**

With the Horizon Cloud Service on Microsoft Azure offering, Microsoft and VMware work together to extend the desktop-as-a-service (DaaS) offering with new cross-cloud capabilities. Key features of Horizon Cloud Service on Microsoft Azure include:

- **Support for VDI desktops**: For desktops that use the Microsoft Windows 10 operating system, you can entitle both VDI dedicated desktops and VDI floating desktops to your end users.
- **Easy deployment**: Depending on the complexity of your configuration, it can take as little as 60 minutes to deploy the service to your own Microsoft Azure instance.
- **Single management plane**: Even if you deploy multiple instances of Horizon Cloud Service to multiple Microsoft Azure regions, you still use the same cloud-based management UI to configure and manage your Horizon Cloud Service environments.
- **Single infrastructure provider**: You can manage virtual applications from the cloud with your existing infrastructure provider.
- **Simple upgrades**: VMware provides a simple blue-green upgrade method that allows you to rev to the next release in minutes.
- **Power management**: Horizon Cloud Service has built-in features that automatically allocate and deallocate RD Session Hosts based on demand, which cuts costs because you pay for use only, not for idle time.
- **Schedule-based power management options for VDI dedicated and floating desktops**: You can schedule powering off an assignment’s VDI desktops for weekends, holidays, and non-working hours, which can optimize cost savings. You can also schedule a higher minimum desktop count to meet high-demand times.
- **Rolling maintenance and image update**: Horizon Cloud Service includes built-in orchestration to allow you to do rolling maintenance of your RD Session Hosts.
- **RD Session Hosted applications**: Horizon Cloud Service supports RD Session Hosted applications and desktops with this initial release.
- **Cloud monitoring**: You do not need a third party or additional tool to monitor or manage your Horizon Cloud Service on Microsoft Azure deployment. Our new cloud-based monitoring feature allows you to keep an eye on your deployment from a single UI.
- **True multi-cloud deployments**: You can choose between cloud capacity managed by VMware, bring your own hyper-converged infrastructure, or bring your own public cloud capacity from Microsoft Azure.
- **User Environment Manager (aka Dynamic Environment Manager)**: With this solution, you get personalization and dynamic policy configuration across any virtual, physical, and cloud-based Windows desktop environment, engineered to deliver workplace productivity while driving down the cost of day-to-day desktop support and operations.
- **Workspace ONE**: This solution integrates with VMware Workspace ONE™ to provide your users with a single workspace to
Leverage Microsoft Azure services and regions: You can host virtual desktops and apps across more data centers and more locations by integrating with Azure, one of the fastest-growing IaaS providers with one of the largest number of global regions.

Expanded geographic reach: You can leverage any region from the many global Microsoft Azure data centers, and configure and deploy desktops in minutes.

Low-cost hourly billing: You benefit from consumption-based pricing for capacity, as well as no upfront costs or termination fees.

For more information, see VMware Horizon Cloud Service and under Release Notes, select Horizon Cloud Service - v2.0 - July 2019.

Components and Architecture

About System Architecture and Components

The Horizon Cloud Service on Microsoft Azure system architecture includes the standard Horizon Cloud Service components, as well as unique components and integrations that provide additional capabilities.

Figure 1 demonstrates the automated provisioning of a Horizon Cloud Service pod on your Microsoft Azure capacity. Note: Deployments into Microsoft Azure were previously referred to as nodes.

1. Your Microsoft Azure infrastructure-as-a-service (IaaS) provides capacity.
2. Your VMware Horizon Cloud Service control plane is granted permission to create and manage resources with the use of a service principal in Microsoft Azure.
3. You provide additional prerequisites such as Active Directory, as well as optional components such as Deployment Engine, Workspace ONE Connector, and RDS license, from either Microsoft Azure or Horizon Cloud on premises.
4. The Horizon Cloud Service control plane initiates the deployment of the Horizon Cloud Service pod, VMware Unified Access Gateway™ appliances for secure remote access, and other infrastructure components that assist with the configuration and management of the Horizon Cloud Service infrastructure.
5. After the Horizon Cloud Service pod is deployed, you can connect the pod to your own corporate AD infrastructure or create a new AD configuration in your Microsoft Azure subscription. You deploy VMs from the Microsoft Azure marketplace, which are sealed into images, and can be used in RD Session Host farms.
With the VDI functionality, you can also create Windows 10 assignments of both dedicated and floating desktops.

**VMware Horizon Cloud Service Components**

Horizon Cloud Service consists of the following major components:

- **Infrastructure**: You can choose Microsoft Azure infrastructure, VMware cloud-hosted infrastructure, or your own hyper-converged infrastructure (HCI). This guide focuses on the Microsoft Azure infrastructure option.
- **Active Directory**: You can choose to deploy AD on premises or in cloud.
- **Image**: Also called image template, a desktop or RDSH server image that can be used in a Horizon Cloud Service tenant to create desktop or application assignments. It is used as the base image from which virtual machines (VMs) are cloned.
- **VMware Horizon Client™**: Software-based client installed on a desktop, thin client, mobile device, or tablet that facilitates connectivity to Horizon Cloud-hosted desktops and applications.
- **Horizon Cloud Service tenant appliance**: A hardened Linux appliance that provides desktop and application brokering, provisioning, and entitlement services. It hosts the end-user and administrative portals.
- **Desktop and services subnets**: Unique IP subnets that you assign to allow for desktop, application, and administrative connectivity. The Desktop Zone uses the desktop subnet for virtual desktops and RDSH servers. The Services Zone uses the services subnet for tenant appliances and other utility services.
- **Horizon Cloud Service Control Plane**: The central location to conduct all administrative functions and policy management. From the cloud-based control plane, you can manage your RDS farms and assign applications to users and groups from any browser on any machine with an Internet connection. The cloud control plane provides access to manage all Horizon Cloud Service pods deployed into your Microsoft Azure infrastructure in a single, centralized user interface, no matter which regional data center you use.
- **Horizon Cloud Service Administration Console**: The web-based portal, a component of the control plane, that you use to provision and manage Horizon Cloud Service desktops and applications, resource entitlements, and images. The Horizon Cloud Service Administration Console provides full life-cycle management of desktops, and Remote Desktop Session Host (RDSH) through a single, easy-to-use web-based console. Organizations can securely provision and manage desktop models and entitlements, as well as native and remote applications, through the centralized Horizon Cloud Service Administration Console. The Horizon Cloud Service Administration Console also provides usage and activity reports for various user, administrative, and capacity-management activities.
- **VMware Unified Access Gateway**: A hardened Linux appliance that allows for secure remote access into the Horizon Cloud Service environment and is part of the Security Zone (for external Horizon Cloud Service access) and the Services Zone (for internal Horizon Cloud Service access).
- **Optional VMware User Environment Manager (aka Dynamic Environment Manager)**: A scalable management solution that provides personalization of Windows and apps; dynamic policy configuration across virtual, physical, and cloud-based Windows desktop environments, for managing a user’s persona across devices and locations; and VMware User Environment Manager.
- **Optional VMware Workspace ONE**: You can choose to deploy a Workspace ONE connector in your data center.
- **Optional True SSO Enrollment server**: You can choose to deploy a True SSO Enrollment server in your data center.
- **NEW! VMware Types & Sizes**: A new feature to configure a subset of virtual machines (VMs) available for images. Microsoft Azure provides a variety of types of virtual machines (VM) and classifies them based on the memory, storage, and compute types. The length of the list of VMs makes it somewhat unwieldy, so this new feature enables you to select a subset to display to your end users as a pop-up list. During deployment, you can configure the list to include a sub-set of all available types and sizes, and you can change it any time after deployment. For more information, see Sizes for Windows Virtual Machines in Azure.

**Horizon Cloud Service on Microsoft Azure Components**

Horizon Cloud Service on Microsoft Azure deploys three appliances from your Microsoft Azure configuration that provide the following capabilities:

- **Horizon Cloud Service Pod**: Manages all infrastructure resources. While all policy definition and management happen in the cloud, all of the real work—creating resources on Microsoft Azure infrastructure and making it available to users—happens in the Horizon Cloud Service pod.
- **Unified Access Gateway Appliances**: Provide secure Internet access to published applications and published desktops. One appliance is used for standard runtime, and an additional appliance is used during upgrade. One appliance is continuously powered on, and the second is on only during upgrade.
- **Jumpbox**: A temporary Linux-based VM used during environment buildout, as well as for subsequent environment updates.
A: Setting Up

About Setup

The prerequisite exercises help you prepare your environment for best use of Horizon Cloud Service on Microsoft Azure. The exercises are sequential and build upon one another, so make sure to complete each exercise in this section before going to the next.

In this section, you first verify that your environment meets the basic prerequisites. Next, you create a new virtual network (VNet), one of the prerequisite Microsoft Azure components. You must provide your own Microsoft Azure IaaS capacity, and configure the Microsoft Azure prerequisites for the Horizon Cloud Service deployment. You then set up network ranges based on previously provided CIDR blocks, select Active Directory options, complete VNet bi-directional peering, DNS configuration, and so on. Subsequent sections describe how to deploy the Horizon Cloud Service pod on Microsoft Azure, and finally how to create a farm where your end users can access applications and shared desktops, and assign dedicated and floating desktops.

Exercise A1: Reviewing the Workflow

Before you start, it is best practice to review the workflow and tasks involved. You can use the navigation tool on the left to jump to each section as outlined below:

1. Verify that your environment meets the prerequisites listed in VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist.

2. See Deploying a Horizon Cloud Service Pod
   - Prepare the Microsoft Azure for pod deployment.
   - Deploy the pod.

3. See Creating an Image
   - Register Active Directory domain.
   - Configure a master image.
   - Install applications in the master image.
   - Convert the master image into an assignable image.

4. See Deploying a Farm
   - Create an RDSH farm to provide session desktops to assign to users.
   - Create another RDSH farm to provide remote desktops to assign to users.
   - Create a CNAME record in your DNS server.

5. See Assigning VDI Desktops
   - Assign a dedicated desktop.
   - Assign a floating desktop.

6. See Explore Horizon Cloud Service Monitoring and Analytics
   - Explore the reports and analytics functionality.

7. See Explore VMware User Environment Manager
   - Explore the integration with User Environment Manager and capabilities.

After you finish reviewing the workflow, verify that your environment meets all prerequisites, and then proceed to the next exercise to configure the VNet.

Exercise A2: Creating the VNet

You can deploy a Horizon Cloud Service pod to an existing virtual network (VNet), or create a new VNet. But before you create a VNet, verify that your environment meets the prerequisites listed in VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist. For more information, see Getting Started with VMware Horizon Cloud Service on Microsoft Azure.

This exercise describes how to create a new VNet where Active Directory services are available. Microsoft Azure automatically creates the necessary subnets in the VNet using CIDR blocks that you provide. Horizon Cloud Service automates machine creation and domain join operations, and requires access to a VNet with AD services. A set of resource groups in your Microsoft Azure capacity is also automatically created. Resource groups organize the assets that the environment needs, such as virtual subnets and VMs for the Unified Access Gateway, RDS-enabled server images, RDSH farms, and so on.
1. Log in to Microsoft Azure

   1. Log in to your existing Microsoft Azure deployment.
   2. Make sure to use a subscription that provides IaaS capacity.

2. Add a New Virtual Network
1. In the navigation bar on the left, select Virtual Networks.
2. Click Add to create a VNet.

3. Provide Data for New VNet
In the Create Virtual Network pane, provide the following information:

1. **Name**: Enter a name to distinguish this VNet from others.
2. **Address space**: Accept the default, or enter an address range.
3. **Subscription**: Select from the drop-down menu.
4. **Resource group**: Select an existing resource group, or create a new one when the virtual network is created.
5. **The value should not be empty**: Create a new resource group or use an existing one.
6. **Location**: From the drop-down menu, select the region where you plan to deploy the Horizon Cloud Service pod.
7. **Subnet Name**: Accept the default. Horizon Cloud Service automates the creation of the necessary subnets using the CIDR blocks previously provided.
8. **Address range**: Accept the default.
9. **Service endpoints**: Accept the default.

2. In the lower right corner, click **Create**.
3. Wait until the creation process is complete, and the VNet is created.

For more information, see [VMware Horizon Cloud Service Deployment Guide](https://example.com), in the search field select **Book**, and search the guide for **Configure the Required Virtual Network in Microsoft Azure**.

After creating the VNET, proceed to the next section to configure bi-directional VNET peering.
Exercise A3: Configuring VNet Peering (Optional)
In this exercise, you use Microsoft Azure to configure bi-directional peering. You should configure VNet-to-VNet peering only if the following is true:

- You created a new VNet that does not have an AD VM inside it
- You are not using Express Route for VNet peering
- You are not using VPN for express route peering

In this tutorial, it is assumed that another VNet is in the same region as the AD/DNS server, to which you are peering for access to those services.

**1. Peering Connects the Horizon Cloud Service VNet on Microsoft Active Directory**

1. Select the Virtual Networks pane and select a network.
2. Click **Peering**.
3. On the right-most pane, verify that the peer is not yet connected.

**2. Add Peering Details**
1. In the **Add peering** pane under **Peer details**, provide the required information:
   - **Name**: Enter a name to distinguish this action from others.
   - **Virtual network deployment model**: Select the **Resource manager** option.
   - **Subscription**: Select your subscription.
   - **Virtual network**: Click **Choose a virtual network**, and select your VNet.

2. Under **Configuration**, provide the following required information: enabled
   - **Allow virtual network access**: Enabled.
   - **Configure forwarded traffic settings**: Enabled.
   - **Configure gateway transit settings**: Check to allow gateway transit.

3. Click **OK**.

### 3. VNet Peering Is Connected
1. Return to the third pane if you are not already there.
2. Verify that VNet peering is now connected.

4. VNet Peering Overview Details

1. In the second pane, click **Overview**.
2. Review the additional details now displayed in the third pane.

For more information, see the [Getting Started with VMware Horizon Cloud Service on Microsoft Azure](#) guide.

After you finish configuring the VNet, proceed to the next exercise to configure the DNS server.
Exercise A4: Configuring the DNS Server

Now that the VNet is configured, your next step is to configure the DNS, which is required during the Horizon Cloud Service pod deployment. Horizon Cloud Service uses the default Microsoft Azure-provided DNS for the deployment for outbound DNS resolution, but requires Active Directory to resolve the Active Directory domain controllers. You must set the virtual network to support both internal and external name resolution.

1. Microsoft Azure DNS Supports Name Resolution

1. In the navigation bar on the left, click Virtual networks.
2. Select the virtual network you want to use for your pod.
3. Click DNS servers to display the DNS server settings.

2. Configure DNS Before Deploying the Horizon Cloud Service Pod
In the upper right, select the **Custom** option.

1. Add the address of the DNS server to use for name resolution.

2. For more information, see [Getting Started with VMware Horizon Cloud Service on Microsoft Azure](#).

After you finish configuring the DNS server, proceed to the next exercise to create an authentication key for the service principal.

**Exercise A5: Creating a Service Principal Authentication Key**

Horizon Cloud Service needs a service principal to access and use your Microsoft Azure subscription capacity. A service principal defines the policy and permissions for use of an application in a specific tenant, and is used to grant Horizon Cloud Service permission to access and modify your Microsoft Azure tenant. When you register a Microsoft Azure AD application, the service principal is also created. For more information, see [Create the Required Service Principal by Creating an Application Registration](#).

In addition to the service principal, you must generate an authentication key and assign the Contributor role to the service principal at the subscription level.

**1. Service Principal Settings**
1. Locate the service principal details window.
2. Click **Settings** to open the Settings menu.

2. **Authentication Key Required to Deploy the Horizon Cloud Service Pod**

1. In the Settings menu, click **Keys**.

3. **Authentication Key Security Policy**
1. In the Keys menu, provide the following information:
   - **Description**: Enter a description of 16 characters or fewer, such as Hzn-Cloud-Key1.
   - **Expires**: Set the duration of the key, based on your security policy. You can set the expiration to **Never expires**, or you can set a specific time frame.
   - **Caution**: If you set a specific time frame, make sure to refresh the key before it expires, and enter the new key into the subscription information in the Horizon Cloud Service Administration Console. If the key expires without doing this, the associated pod stops because Horizon Cloud Service cannot detect it.
   - **Value**: Keep the Keys window open until you have copied and saved the key value.

2. Click **Save**.

### 4. Save the Authentication Key Because Irretrievable Later

1. Copy the unique key value.
2. Save the value securely, because you cannot retrieve it later.

For more information, see [Connect Virtual Networks with Virtual Network Peering using the Azure Portal](#) and [Use Portal to Create an Azure Active Directory Application and Service Principal That Can Access Resources](#).

After you finish creating an authentication key for the service principal, proceed to the next exercise to assign a role to the service principal.

**Exercise A6: Assigning the Contributor Role to the Service Principal**

In this exercise, you assign the contributor role to the service principal at the subscription level.
1. Make Note of the Subscription ID

1. In the navigation bar on the left, select **Subscriptions**.
2. Click the name of the subscription.
3. Copy and save the subscription ID to use when you deploy the pod.

2. Add Permissions

1. Click **Access control (IAM)**.
2. Click **Add** to display the **Add permissions** window.

3. Add Permissions Information
1. In the Add permission window, provide the following information:
   - **Role**: From the drop-down menu of built-in roles, select **Contributor**.
   - **Assign access to**: From the drop-down menu, select **Azure AD user, group, or application**.
   - **Select**: Search for and select the service principal by the name you gave it earlier.

2. Click **Save**.

### 4. Save the Service Principal

1. Click your service principal to select it
2. Click **Save**.
After you finish assigning a role to the service principal, proceed to the next section to verify the required resource providers.

Exercise A7: Verifying Required Resource Providers
In this exercise, you verify that your subscription includes the registered resource providers that the pod requires.

1. **Navigate to Resource Providers**

   ![Image](image_url)

   1. In the navigation bar on the left, select **Virtual machines**, and click the name of the subscription used with this pod.
   2. In the subscription menu, click **Resource providers**.

2. **Verify That Required Resource Providers Are Registered**
In the Status column, verify that the following resource providers have a Registered status, and if they do not, register them:

- Microsoft.Compute
- microsoft.insights
- Microsoft.Network
- Microsoft.Storage

3. Verify Subscription-Based Values Required for Deployment
In the navigation bar on the left, click Azure Active Directory > Manage.

1. In the second pane, click Properties.

2. In the third pane, verify that you have the four subscription-based values required during pod deployment:
   - Subscription ID
   - Azure Active Directory ID
   - Application ID
   - Application key value

For more information, see Getting Started with VMware Horizon Cloud Service on Microsoft Azure.

After you finish creating and configuring the service provider and verified that you have the subscription-related values required for deployment, proceed to the next section to deploy the Horizon Cloud Service pod.

B: Deploying a Horizon Cloud Service Pod

About Pod Deployment
Now that you have set up the Horizon Cloud Service on Microsoft Azure pod, you are ready to begin the initial configuration process of your deployment. In this series of exercises, you deploy a Horizon Cloud Service pod and bind it to an existing Active Directory domain. This grants the Horizon Cloud Service control plane access to create and manage resources in Microsoft Azure. These exercises are sequential and build upon one another, so make sure to complete each exercise in this section before going to the next.

Exercise B1: Deploying the Horizon Cloud Service Pod
Armed with the prerequisite information from your Microsoft Azure tenant, you are now ready to begin deploying the Horizon Cloud Service pod and binding it to an existing Active Directory domain.

1. Use your My VMware credentials, which give you access to the Horizon Cloud Service control plane.
2. Before you deploy the Horizon Cloud Service pod, verify that you have the prerequisite information from your Microsoft Azure tenant, which the Horizon Cloud Service deployment wizard uses during the deployment process:
   - **Service Principal**: Like a certificate, the service principal object defines the policy and permissions for use of an application in a specific tenant, and is used to grant Horizon Cloud Service permission to access and modify your
Microsoft Azure tenant
- **Subscription ID**: Primary Microsoft Azure billing identifier based on your agreement with Microsoft
- **Directory ID**: Your Primary Identifier or Identifiers in Microsoft Azure Active Directory
- **Application ID**: An attribute of the Service Principal that securely ties the Horizon Cloud Service control plane to your Microsoft Azure subscription and is used to authorize Horizon Cloud as an application to use your Microsoft Azure capacity
- **Application Key**: A one-time-use password that is used to encrypt the service principal

For more information, see [Getting Started with VMware Horizon Cloud Service on Microsoft Azure](#).

1. **Log in to VMware Horizon Cloud Service**

![Login to VMware Horizon Cloud Service](image)

- Log in to Horizon Cloud Service, using your My VMware account ID and password.

2. **Add a New Horizon Cloud Service Pod**
In an account with no pods previously deployed, the Getting Started wizard defaults to the Capacity section. In the upper right corner of the Add Cloud Capacity pane, click Add, which starts the Horizon Cloud Service Pod Deployment wizard.

**Note**: To add a new Microsoft Azure pod to an account with pods previously deployed, you can alternatively click Settings > Capacity > New > Pod > Microsoft Azure.

### 3. Add Microsoft Azure Capacity

In the Add Capacity window, select **Microsoft Azure**. Adding capacity is equivalent to deploying a pod in a capacity environment and connecting that pod to your overall Horizon Cloud environment.

### 4. Provide Subscription Details
1. In the Microsoft Azure Subscription tab of the Add Cloud Capacity window, provide the data that you gathered earlier:
   - **Apply Subscription**: Select **Add New** and enter the new subscription information.
   - **Subscription Name**: Enter a recognizable name to distinguish this subscription from others. The name must start with a letter and contain only letters, numbers, and dashes.
   - **Environment**: Select the environment associated with your Microsoft Azure subscription.
   - **Subscription ID**: Enter the subscription ID in UUID form, from the Subscription area of your Microsoft Azure portal.
   - **Directory ID**: Enter the Microsoft Azure AD Directory ID in UUID form, from the Microsoft Azure Active Directory properties in your Microsoft Azure portal.
   - **Application ID**: Enter the application ID in UUID form associated with the service principal you created in the Microsoft Azure portal. Creating an application registration and associated service principal in your Microsoft Azure Active Directory was a prerequisite. The application registration is used to authorize Horizon Cloud as an application to use your Microsoft Azure capacity.
   - **Application Key**: Enter the key value for the authentication key of the service principal that you created in the Microsoft Azure portal. Creating this key was a prerequisite.

2. In the lower right corner, click **Next**.

### 5. Provide Pod Setup Details
In the Details panel of the Pod Setup tab, provide the following information:

1. **Pod Name**: Enter a recognizable name, to be used in the Administration Console to distinguish this pod from other pods.
2. **Location**: Click **Add** to specify a location, which you can use to group pods according to categories that you provide, such as Business Unit A, Business Unit B, and so on.
3. **Microsoft Azure Region**: Select the physical geographic Microsoft Azure region into which you want the pod to be deployed. For best performance, deploy the Horizon Cloud Service pod in a region that is geographically near the end users consuming the service to provide lower latency.
4. **Description**: Enter an optional description for this pod.

Scroll down to the next panel.

### 6. Provide Networking Details

In the Networking panel of the Work Setup tab, provide the following information:

1. **Virtual Network**: Select a virtual network to use for your pods.
2. **Use Existing Subnet**: Enable this option to use an existing subnet.
3. **Management Subnet**: Enter a management subnet for your pods.
4. **Desktop Subnet**: Enter a desktop subnet for your pods.
5. **NTP Servers**: Enter NTP servers for your pods.
6. **Use Proxy**: Enable this option if your pods need to use a proxy for networking.

Identity Management:

- **Identity Manager Tenant**: Select the identity manager tenant for your pods.
Virtual Network: Select a virtual network from the list. Only virtual networks 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: Slide to enable, as in this example.

Management Subnet: Enter a subnet (in CIDR notation) to which the pod and Unified Access Gateway instances get connected, such as 192.168.8.0/28. For the management subnet, a CIDR of at least /28 is required.

Desktop Subnet: Enter the subnet (in CIDR notation) to which all of this pod's RDSH servers for end-user remote desktops and applications get connected, such as 192.168.12.0/22. Minimum: /28. Recommended: /22.

NTP Servers: Enter the list of NTP servers to use for time synchronization, separated by commas (for example 10.11.12.13, time.example.com).

Use Proxy: Slide to enable, or leave disabled as in this example.

2. In the Identity Management panel, accept the default, and click Next.

7. Provide Unified Access Gateway Details

1. In the Unified Access Gateway panel of the Work Setup tab, provide the following information.

- Enable External UAG? Slide to enable, as in this example.

- Internet Enabled Desktops: Select Yes to enable users located outside your corporate network to access desktops and applications. The pod includes a load balancer and Unified Access Gateway instances to enable this access. Selecting Internet-enabled desktops triggers Horizon Cloud Service to automatically deploy two Unified Access Gateway appliances in an availability setting.

- FQDN: Enter the required fully qualified domain name (FQDN), such as ourOrg.example.com, for your end users to use to access the service. You must own that domain name and have a certificate in PEM format that can validate that FQDN.
QUICK-START TUTORIAL FOR VMWARE HORIZON CLOUD ON MICROSOFT AZURE

- **DMZ Subnet**: Enter the subnet in CIDR notation for the demilitarized zone (DMZ) network to be configured to connect the Unified Access Gateway instances to the load balancer.
- **DMZ Addresses**: Accept default.
- **Route**: Leave blank.
- **Certificate**: Upload the certificate in PEM format for Unified Access Gateway to 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. A certificate is automatically applied to the two Unified Access Gateway appliances during deployment.

2. For this exercise, leave the two-factor identification settings disabled, and in the lower right corner, click Validate & Proceed.

### 8. Review Summary

![Image of the Review Summary page]

- Review the summary, verify that the information is correct and complete, and then click Submit.

### 9. Verify That the Pod Is Deployed
• Wait until the green check mark appears, which indicates that the Horizon Cloud Service pod and all supporting infrastructure components are deployed. This process can take awhile to complete.

After you finish deploying the Horizon Cloud Service pod, proceed to the next exercise to perform the domain bind operation.

Exercise B2: Binding to the Active Directory Domain
Machine creation and domain join operations are automated by Horizon Cloud Service. The domain bind operation must be performed on the pod before creating images and farms. You have several Active Directory domain configurations to choose from. For more information about these options, see Getting Started with VMware Horizon Cloud Service on Microsoft Azure.

1. Get Started
To complete the Active Directory configuration, provide information about the domain and accounts used for domain operations.

1. In the Horizon Cloud Service Administration Console, in the navigation pane on the left, click **Settings**.
2. Click **Getting Started**.
3. In the Getting Started wizard, locate the **Microsoft Azure 1 Pod** added.
4. Click **General Setup** to expand the fields.

### 2. Configure Active Directory
1. Under General Setup, locate the Active Directory panel.
2. On the far right, click Add.

3. **Register Active Directory**
1. In the Register Active Directory window, provide information about the domain and accounts used for domain operations.
   - **NETBIOS Name**: Enter the Active Directory domain name.
   - **DNS Domain Name**: Enter the fully qualified Active Directory domain name.
   - **Protocol**: Accept the LDAP default.
   - **Bind Username**: Enter the user account in the domain to use as the primary LDAP bind account.
   - **Bind Password**: Enter the password associated with the Bind Username.
   - **Auxiliary Account #1**: In the Bind Username and Bind Password fields, enter a user account in the domain to use as the auxiliary LDAP bind account and its associated password.
   - For more information, see [VMware Horizon Cloud Service on Microsoft Azure Administration Guide](#).

2. In the lower right corner, click **Domain Bind**.

### 4. Provide Domain Join Details
After configuration is complete, in the Domain Join window, provide the required data.

1. **Primary DNS Server IP**: Enter the IP address of the primary DNS Server.  
   **Note**: This DNS server must be able to resolve machine names inside of your Microsoft Azure cloud as well as resolve external names.
2. **Join Username**: Enter the user account in the Active Directory that has permissions to join systems to that Active Directory domain.
3. **Join Password**: Enter the password associated with the Join Username.
4. **Secondary DNS Server IP (Optional)**: Enter the IP of a secondary DNS Server.

In the lower right corner, click **Save**.

---

5. **Add the Administrator**

In the Add Administrator window, select an Active Directory User Group

1. In the Add Administrator window, select an Active Directory User Group
2. In the lower right corner, click **Save**.
Note: Add the Active Directory group that includes the domain-join account, as described in the prerequisites. This action grants this group permissions to perform management actions in the Administration Console.

6. Notice Change in Login Windows

1. When you finish registering the pod with your Active Directory domain, the system returns you to the login window.
2. In the login window, you must log back in, first with your My VMware account, and then with the Active Directory credentials in the group that you just assigned.

7. Join the VMware Customer Experience Improvement Program

1. With the Horizon Cloud Service pod deployed and the bind operation complete, you can move the Yes/No slider to choose whether or not to join the VMware Customer Experience Improvement Program.
2. In the lower right corner, click Save.

For more information, see VMware Horizon Cloud Service on Microsoft Azure Administration Guide, and search the guide for Register Your First Active Directory Domain.

After deploying the Horizon Cloud Service pod and completing the bind operation, proceed to the next section to create master images.

Exercise B3: Defining VM Types & Sizes

You can optionally select which VM types and sizes to allow, add sizes to favorites, and customize how VM names are displayed.

Microsoft supports a wide variety of VM types and sizes, which you can learn about at Sizes for Windows virtual machines in Azure. Instead of reviewing the entire list of available VM types, you can save time by creating your own sub-set of your favorite types and
sizes. You can create this sub-set during deployment, and you can update it at any time afterward. If you set the option to choose your VM type, your end users can review the sub-set and quickly make their selection.

For more information, see General Purpose virtual machine sizes.

1. Navigate to VM Types & Sizes

1. In Horizon Cloud, navigate to Settings.
2. Under Settings, select VM Types & Sizes.
3. Scroll through the long list of available settings.

2. Expand a VM Type & Size

1. From the list of available VM types, select a type.
In this example, the Dv2 Series is selected, a general purpose type that is good for testing and development, small to medium databases, and low to medium traffic web servers with a balanced CPU-to-memory ratio.

2. Expand and examine the details of this series.

3. Edit the VM Type

![VM Types & Sizes](image)

1. In the upper right, click Edit.
2. From the list, select the VM Type & Size that you want to define.

4. Add a Tag
In the edit window of the VM Type & Size you selected, click the arrow to expand.

1. Under Tags, add a tag.
2. Make sure to use only letters, numbers, and spaces. As you can see, the use of an apostrophe is not allowed.

5. Save the New Tag
1. Enter a well-formed tag.

2. In the lower right, click Save.

6. Verify Success
At the top of the VM Types & Sizes window, look for the banner that verifies success.

For more information, see VMware Horizon Cloud Service on Microsoft Azure Administration Guide, and search the guide for Managing VM Types and Sizes for Farms and Assignments.

After you finish creating and defining the subset of VM types and sizes that you want, you are ready to proceed to create a new image in the next exercise.

**C: Creating an Image**

**About Image Creation**

Microsoft provides a variety of VM templates in the Microsoft Azure Marketplace. Upon import, Horizon Cloud Service joins the VM to the domain, enables the RDS role, automates the Horizon and DaaS installations, and performs a bootstrap process, enabling secure pairing of the DaaS agent to the Horizon Cloud Service pod. All of this is automated, although the process can be performed manually if you want to convert an existing VM to a Horizon Cloud Service image yourself.

After the imported VM is configured with the necessary applications, Horizon Cloud Service converts the VM to an image by automatically running SYSPREP and sealing the OS. You can then use the image to create RDS session host farms and assign dedicated and floating VDI desktops.

**Exercise C1: Importing VMs from Microsoft Azure Marketplace**

In this exercise, you import a VM from the Microsoft Azure Marketplace, configure it with applications, and convert the VM to an image. With this image, you can then create new instances of the VM.

Later in this Tutorial, a set of exercises create an RDS server farm, for which you need an image with a server OS. Another set of exercises create a pool of VDI desktops, for which you need a Windows 10 desktop OS.

This exercise demonstrates deploying a new image using a desktop OS, and the process for deploying a server OS is virtually the same.

1. Navigate to Imported VMs
1. In the navigation panel of the Horizon Cloud Service Administration Console, click **Inventory**.
2. In the Inventory menu, click **Imported VMs**.
3. In the Imported VMs window, click **Import**, which imports a Windows VM from the Microsoft Azure Marketplace.

### 2. Select the Marketplace

In the Import Desktop window under From Marketplace, click **Select**.

### 3. Provide Destination Desktop Details
1. In the Import Desktop Marketplace window under Destination Desktop, provide the following information:
   - **Location**: Select a location from the pop-up menu to get a list of pods available to store the desktop.
   - **Pod**: Select a pod to serve the desktop from.

2. Scroll down to the Desktop Details panel.

### 4. Provide Desktop Details

1. Under Desktop Details, provide the following information:
   - **OS**: Select the operating system to use from the Microsoft Azure Marketplace.
   - **Include GPU**: Select **Yes** to provide GPU-backed hardware. If disabled, your Microsoft Azure subscription in the selected pod region does not support GPU hardware.
   - **Domain**: Select the Active Directory domain that you want configured in the base VM.
   - **Enable Public IP Address**: Select **Yes** to configure a public IP address so you can access the VM through an RDP connection.
   - **Optimize Windows Image**: Select **Yes** to optimize Windows on image import, which improves VM performance and capacity utilization.
   - **Remove Windows Store Apps**: Select **Yes** to remove Windows Store apps, which improves performance.

2. Scroll down to the next panel.
5. Provide Admin Credentials for the Desktop

1. Under Admin Credentials for the Desktop, provide the required information:
   - **Username**: Enter the administration username for the VM account. This username is used for the local administration account to access the OS of the master image VM.
   - **Password**: Enter the password for the administrator account, which must adhere to the Microsoft Azure rules.
   - **Verify Password**: Re-enter the password to verify.
   - **Do you have a Windows Server License**: Select Yes, and select the check box to confirm that you have the proper license.

2. Scroll to the next panel.

6. Provide Properties

1. In the Admin Credentials for the Desktop panel and the Properties panel, provide the required information.
   - **Name**: Enter a unique name for the master image VM.
   - **Description**: You can enter an optional description.

2. Select **Advanced Options** to reveal the Horizon Agent Features panel.
7. Provide Horizon Agent Details

1. Under Horizon Agent Features, accept the default to install all features in the master VM:
   - **Enable Flash MMR**: Redirects Flash multimedia content sent to the client system and plays in a Flash container window using the Flash Player ActiveX version.
   - **3D support in RDSH**: Provides support for vGPU-powered 3D RDS hosts.
   - **MMR for Terminal Services**: Redirects multimedia content directly to the client computer, which plays the media content, offloading the demand on the RDS desktop and improving performance optimization.
   - **Client Drive Redirection**: Allows you to share folders and drives on your local system with remote desktops and applications.
   - **Skype for Business**: Provides the ability to use the RDS desktops to make optimized audio and video calls with Skype for Business inside a virtual desktop without negatively affecting the virtual infrastructure and overloading the network.
   - **Webcam Support (Real Time Audio Video RTAV)**: Allows you to run Skype, Webex, Google Hangouts, and other online conferencing applications on remote desktops with client local webcam and audio devices.
   - **Smart Card**: Lets you redirect smart cards from client to remote sessions for both SSO and in-session leverage.
   - **Thin Print**: Allows you to print to any printer configured for your local computer from a remote desktop or application without installing printer drivers on the remote desktop.
○ **Scanner Redirection**: Redirects scanning and imaging devices that are connected to the client systems so those devices can be used with the desktop or remote application.

○ **USB Redirection**: Enables redirection of USB devices that are connected to your local client system so those devices can be used with the desktop or remote application.

○ **URL Redirection**: Collects performance data from monitored software and hardware objects in your Horizon environment and provides predictive analysis and real-time information about problems in your Horizon infrastructure.

○ **Serial Port Redirection**: Enables devices connected to serial ports on your local client system so those devices can be used with the remote desktop or application.

○ **Geolocation Redirection**: Allows the geolocation information of the client system to be used by Internet Explorer in remote desktops.

2. **Help Desk**: Select Yes to install the Help Desk.

2. In the lower right corner, click Import.

8. **Verify the VM Imported Successfully in Microsoft Azure**

1. When the success banner verifies that the import is complete, you can return to the Microsoft Azure portal.

2. Verify that the VM was successfully completed.

9. **Explore the Details of the Imported VM**
1. Select the imported VM.
2. Explore the details.

10. Verify That the Imported VM Is Active

1. Return to the Horizon Cloud Service Administration Console, where the imported VM is displayed.
2. Horizon Cloud Service automates the customization of the master image VM, the green dot appears under Status, and the status changes to **Active** when the process is complete.

For more information, see [VMware Horizon Cloud Service on Microsoft Azure Administration Guide](#), and search the guide for **Create a Master Virtual Machine Automatically from the Microsoft Azure Marketplace**.

**Note**: It is also recommended that you optimize the image using the [VMware Windows Operating System Optimization Tool](#). This tool includes templates that you can customize to enable and disable Windows system services and features across multiple systems. Many Windows system services are enabled by default. You can disable services or features using the optimization tool, and improve performance by eliminating unnecessary services or features. For instructions, see the [VMware Windows Operating System Optimization Tool Guide](#).

When you finish importing the Windows 10 desktop OS VM, proceed to the next exercise to customize it.
Exercise C2: Customizing the Windows VM

You can customize the Windows operating system of the new master image VM, set wallpapers, and install applications to provide to your end users. If you enabled a public IP address for the master image VM, you can connect to the VM by using the IP address displayed in the Imported VMs window in an RDP client like Microsoft Remote Desktop Connection.

1. RDP to a Public IP

Depending on your configuration, you can use either a private or public IP address to RDP to the new master image VM.

1. Use the IP address of the master image VM to connect to the RDS-enabled Windows Server operating system.
   - **Public IP address**: RDP into it using that IP address.
   - **Private IP address**: RDP into it by one of these two methods:
     - Use another VM in your Microsoft Azure subscription that does have a public IP address, and do an outbound RDP into the master image VM.
     - Use your VPN and RDP into the master image VM over your corporate network.

2. Log in to the RDS-enabled Windows Server operating system using the credentials that you set up when creating the master image VM, and enter the username as \username.

3. Copy the IP address.

2. Log in with a Local Administrator Account
When the login window is displayed, you can log in to Horizon Client.

Once you are connected, you can add end-user applications and video GPU drivers, and any other required configurations to the VM.

Install the third-party applications and drivers that you want available to run in the multi-user RDS desktop environment.

In the Windows Server operating system, right-click the Start button and click Command Prompt (Admin) to open a command prompt as an administrator.

In the command prompt, use the following command to determine the install mode of the server:

```
change user /query
```

The server is in RD-Execute mode if you receive the following response:

```
Application EXECUTE mode is enabled
```

In the command prompt, use the following command to switch the server into RD-Install mode, a special mode to install applications so they can run in a multi-user environment:

```
change user /install
```

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

In the operating system, install any custom drivers you want in the RDS desktops, such as NVIDIA GPUs.

Make any customizations or configurations you want to the RDS desktops, such as adding custom wallpaper, setting default fonts or colors or themes, adjusting the taskbar default settings, and so on.

When you finish, sign out of the operating system. **Note:** Do not shut down the Windows operating system, but instead, use Sign Out.

For more information, see [VMware Horizon Cloud Service on Microsoft Azure Administration Guide](#), and search the guide for **Customize the Guest Windows Operating System of the Master Image Virtual Machine**.

After you finish customizing the master image VM, proceed to the next exercise to convert the master image VM to an assignable image.

**Exercise C3: Converting the Master VM to an Image**

When the master image VM is ready, it is made assignable. For this exercise, you can use any VM with the Agent and bootstrap process already complete.

**1. Start Creating a New Image**
1. In the Horizon Cloud Service Administration Console navigation bar on the left, select **Inventory**.
2. In the Inventory menu, select **Images**.
3. In the Images window, click **New**.

### 2. Provide Desktop-to-Image Details

In the New Image window under **Convert Desktop to Image**, provide the following information:

- **Location**: Select the location to get a list of pods available to store the desktop.
- **Pod**: Select the pod to serve the desktop from.
- **Desktop**: From the list of desktops that can be converted to an image, select the desktop you want.

### 3. Provide OS Properties Details
Under OS Properties, provide the following information:

- **Image Name**: Provide a unique name to the image that will be used as the operating system on your virtual desktops.
- **Company Name**: Enter an identifying name, which is used as the default in desktops that are created with this image.
- **Timezone**: Set the time zone, to be the default time zone for all desktops created with this image.

### 4. Provide Admin Credentials

1. Under **Admin credentials for the desktop**, provide the account credentials for a valid administrator account in the selected image VM. Make sure to follow the complexity standards and other limitations.
   - **Username**: Enter the credentials for the local administrator account that is enabled in the master image VM.
   - **Password**: Enter the password and confirm.
   - **Note**: These credentials are the user name and password that were entered in the wizard when the master VM was created in the Imported VMs window.

2. In the lower right corner, click **Publish**.

### 5. Wait for the Published Status
Wait until the status changes to Published to use the assignable image for creating a farm.

For more information, see VMware Horizon Cloud Service on Microsoft Azure Administration Guide, and search the guide for Convert a Configured Master Virtual Machine to an Assignable Image.

After you finish importing and customizing a master image VM and converting it into an assignable image, proceed to the next section to use the assignable image.

If the master image you created has a Windows 10 OS, proceed to Assigning Resources to create VDI desktop pool.

If the master image you created has a server OS, proceed to Deploying a Farm to create an RDSH farm.

**D: Deploying a Farm**

**About Farm Deployment**

A farm is a collection of Microsoft Remote Desktop Services (RDS servers) on Microsoft Azure that host applications and desktops. Farms simplify RDS host management because you can use farms to serve multiple user subsets where the sizes of the subset vary, or the desktop or application requirements vary. Farms can provide session-based desktops and remote applications.

Ideally, you provide the resources that users need to do their jobs without delays, and at the same time, avoid the cost of unused resources that are powered on but sitting idle. Horizon Cloud Service provides power management capabilities for the Microsoft Azure servers so hosts are automatically powered hosts on and off and deallocated, as needed. The result is that farms can automatically scale out to the maximum size when necessary, and scale down to minimum size when not needed. This reduces cloud capacity costs, as well as computing costs for deallocated servers.

You set up these options in the Horizon Cloud Service farm profile when you first create the farm, and you can also modify the settings at any time afterward.

**Note:** For this set of exercises, you need a server image deployed.

**Exercise D1: Creating a Farm**

When the new image has been published, you can use it to create farms.

1. Create a New Farm
1. In the navigation bar of Horizon Cloud Service Administration Console, select Inventory.
2. Select Farms.
3. In the Farms window, click New.

2. Provide General Settings

1. In the New Farm window, Definition tab, provide the following information, and then scroll down.
   - **Name**: Enter a name to help identify this farm in the system.
   - **Description**: Enter an optional description to help identify the farm in the system.
   - **VM Names**: Enter a name for all server VMs created for this farm to which a number is appended, such as win2016-1, win2016-2, and so on. The name must start with a letter and can contain only letters, dashes, and numbers.
   - **Farm Type**: Specify the type of asset this farm provides to end users. Keep this assignment time in mind when you select the server size, since desktop assignments may require more capacity.
QUICK-START TUTORIAL FOR VMWARE HORIZON CLOUD ON MICROSOFT AZURE

- **Desktops**: Provides session-based desktops
- **Applications**: Provides access to remote applications
  - **Location**: Select the location from the list of pods in the pop-up menu.
  - **Pod**: Select the pod for this farm.

2. Scroll down to provide additional general settings.

### 3. Provide More General Settings

3. Filter Models: You can filter the available VM models by type and favorites, and add filters as well.
4. Model: Select the Azure VM size for the Farm. Some VM sizes are not available in all regions.
5. Image: Select an available RDSH image from the list. Images that do not match the desktop model disk size are not displayed.
6. Preferred Protocol: Select either PCoIP or Blast as the default display protocol that you want the end-user sessions to use.
7. Preferred Client Type: Select the source to use when end users launch assignments from this farm, either a Horizon Client or a browser for HTML Access.
8. Domain: Select the Active Directory domain registered with your environment.
9. Join Domain: Select Yes so that the server instances are automatically joined to the domain when created.
10. Encrypt Disks: For the purposes of this exercise, accept the default No. If you select Yes, the disks for all servers in this farm are encrypted. After the farm is published, encryption cannot be changed.
11. NSX Cloud Managed: For the purposes of this exercise, accept the default No. If you select Yes, NSX Cloud networking and security management is supported for this farm.

2. Scroll to the **Farm Size** section.

### 4. Set Farm Size
1. In the **Farm Size** pane, provide the information to enable the farm to automatically scale up or down on demand:
   - **Min Servers**: Specify the minimum number of usable servers in this farm so not all servers are running at the same time.
   - **Max Servers**: Specify the maximum number of servers that can exist at any one time so not all servers will be running at the same time.
   - **Power Off Protect Time**: Accept the default of 30 minutes that a VM is protected from powering off after powering on due to a headroom error.
   - **Sessions per Server**: Specify the total number of sessions you want to allow per server.
     - **Note**: This number cannot be updated after the farm is created.

2. In the lower left, click **Advanced Properties**.

### 5. Provide Advanced Properties
1. Under **Advanced Properties**, provide the following information:
   - **Computer OU**: Enter the Active Directory Organizational Unit where the server VMs are to be located. For example, `OU=RootOrgName,DC=DomainComponent,DC=eng`, and so on. The entries must be comma-separated with no spaces in between.
   - **Run Once Script** (optional): You can enter the full executable path of a script that you want run after system preparation completes.
   - **Do you have a Windows Server License**: Select **Yes** and check the check box below to verify that you have Windows licenses with active Software Assurance or have an active Windows Server subscription, in order to use Azure Hybrid Benefit to save compute costs.
   - For more information about these settings, see **Exercise D2: Explore RD Session Host Power Management**.

2. In the lower right corner, click **Next**.

6. **Provide Rolling Maintenance Information**

1. In the Management tab, provide the information for Rolling Maintenance.
   - **Rolling Maintenance**: Select the maintenance type, either according to:
QUICK-START TUTORIAL FOR VMWARE HORIZON CLOUD ON MICROSOFT AZURE

- **Scheduled**: Select a time cadence such as daily or weekly.
- **Session**: Specify the number of user sessions at which the farm should begin rolling maintenance.
  - **Recurrence**: Indicate the type of recurrence.
  - **Recurrence Day**: Indicate the day of the week.
  - **Scheduled Hour**: Indicate the hour of the recurrence.
  - **Concurrent Quiessing Servers**: Indicate the number of concurrent quiessing servers.
  - **Server Action**: Select the action that the system should perform on servers that are undergoing maintenance:
    - **Restart**: Restart the sever VMs.
    - **Rebuild**: Delete server VMs and then re-provision them from their RDS desktop image.

2. Scroll to the Power Management panel.

### 7. Provide Power Management Information

1. In the Power Management panel, provide the information used to optimize the farm for your unique business needs. This is where you determine the thresholds at which new capacity is powered up or down, for automatic shutdown or deallocation of unused servers. Set the thresholds at which the system automatically grows and shrinks the number of powered-on server instances as it responds to demand and use:
   - **Optimized Performance**: Keeps more hosts powered on than are needed to service the current end-user workload. As more users log in, Horizon Cloud Service continues to power on hosts in advance, up to the threshold of the maximum farm size. This option increases capacity costs by having the next server ready before requested, but decreases the chance of a delay when users make the request.
   - **Optimized Power**: Waits as long as possible before powering on the next server instance, and more progressively deallocates unused hosts, leaving fewer available resources for end users. This option decreases capacity costs by using the servers longer before powering new ones, but increases the chance of a delay when users try to log in. You can even set the minimum number to 0, so all servers automatically power down when no users need them. However, the next users who log in experience a delay while the server powers back on, which might take several minutes.
   - **Balanced**: Strikes a 50:50 balance between optimizing for performance (time-to-availability for users), and optimizing for power (minimizing between capacity costs).

2. Scroll down to the Timeout Handling section.

### 8. Provide Timeout Handling Information
1. In the Timeout Handling panel, provide the required settings. This is where you configure how you want the system to handle different user session types.
   - **Empty Session Timeout**: Specify how to handle idle user sessions: never timeout idle sessions, or timeout after a specified number of minutes. **Note**: When a session is disconnected, the session is preserved in memory. When a session is logged out, the session is not preserved in memory, and any unsaved documents are lost.
   - **When Timeout Occurs**: Leave blank.
   - **Log Off Disconnected Sessions**: Specify when the system logs the user out of a disconnected session.
   - **Max Session Lifetime**: Specify the maximum number of minutes the system should allow for a single user session.
   - **Session Timeout Retrieval**: Leave blank.

2. Scroll down to Schedule Power Management.

9. Schedule Power Management

1. Under Schedule Power Management, click **Add a row**, and set the power management schedule:
   - **Name**: Provide a recognizable name for this schedule.
   - **Days**: Select the day or days of the week to run the schedule.
   - **Start Time**: Select a time of the day to start the schedule. You might need to scroll to see all options.
   - **End Time**: Select the time of the day to end the schedule.
   - **Timezone**: Set the time zone if it differs from the default.
   - **Min Servers**: Enter the minimum number of servers to include.

2. In the lower right corner, click **Next**.
10. Verify the Summary Information

1. In the Summary tab, review all settings to verify they are correct and complete.
2. In the lower right corner, click Submit.

11. Verify in VMware Horizon Cloud Service

Under Status, verify that the green dot is displayed to indicate that the farm has been created properly.

For more information, see VMware Horizon Cloud Service on Microsoft Azure Administration Guide, and search the guide for Create a
Farm.

After you finish creating farms from the image, proceed to the next exercise to review RDS host power management.

Exercise D2: Exploring RD Session Host Power Management

Horizon Cloud Service provides power management capabilities for the Microsoft Azure servers, automatically powering hosts on and off and deallocating them as needed. You can see the results of setting up the farm that you just created by returning to Microsoft Azure.

1. Verify in Microsoft Azure

1. Return to the Microsoft Azure portal.
2. Review the hosts that the farm automatically creates there.

2. Automatic Shutdown or Deallocation

You can set up automatic shutdown or deallocation of unused servers.

1. From the navigation bar, select Virtual machines.
2. View the status showing each subscription as running or automatically deallocated.
3. Automatic Creation of Resource Groups

Horizon Cloud Service streamlines administration tasks, such as the automatic creation of resource groups, which contain all farm-related components.

1. From the navigation bar, select **Resource groups**.
2. Click **Overview** to view resource group details.

4. Automatic Definition of Network Security Group Rules
Network security group rules are automatically defined.

1. From the navigation bar, select More services.
2. Select Network security groups.
3. Select a group to view the security rules.

For more information, see VMware Horizon Cloud Service on Microsoft Azure Administration Guide, and search the guide for Applications in Your Horizon Cloud Inventory.

After you finish reviewing RDS host power management, proceed to the next exercise to add applications from the farm.

Exercise D3: Adding Applications from the Farm

Horizon Cloud Service can auto-discover applications installed on the farm, or you can manually specify an application. Select the applications to be published, and assign them to end users or groups.

1. Add New Applications
1. In the Horizon Cloud Service Administration Console navigation bar, click **Inventory**.
2. In the Inventory menu, select **Applications**.
3. In the Applications window, click **New**.

### 2. Select Auto-Scan from Farm

In the New Application window, under Auto-Scan from Farm, click **Select**.

### 3. Provide Definition Information
In the New Application window, provide the Definition information:

1. **Location**: Select a location from the pop-up menu.
2. **Pod**: Select the pod containing the farm you want to choose.
3. **Farm**: Select the farm.

Next, click **Next**.

### 4. Select the Applications to Publish

In the Applications tab, select the applications to be published.

1. Check the applications you wish to publish.
2. Click **Next** in the lower right corner.
5. Provide Attributes

1. In the Attributes tab, provide the appropriate attributes.
2. In the lower right corner, click Next.

6. Verify the Summary Information

1. In the Summary tab, review to verify that the selections are correct and complete.
2. In the lower right corner, click Submit.
7. Verify Addition of New Applications

In the Applications window, the green banner verifies that the new applications were added successfully, and the green dots indicate that each application is active.

For more information, see VMware Horizon Cloud Service on Microsoft Azure Administration Guide and search the guide for Importing New Applications from an RDSH Farm Using Auto-Scan from Farm.

After you finish adding applications from the farm, proceed to the next section to explore assigning desktops and applications to users and groups.

E: Assigning Resources

About Assignments

After you finish creating images and farms, you are ready to assign desktops and applications to users. There are three main types of assignments:

- **Desktop Assignments** - You can use automation that is built into the system to perform basic VDI agent updates to floating and dedicated desktops. VDI desktops are powered off and deallocated when not in use, which reduces infrastructure costs. You can also leverage the system to support RDSH session desktops, to be accessed by remote users over a network connection. For more information about floating and dedicated desktop assignments, see VMware Horizon Cloud May 2018 Release Technical What's New Overview.

- **Application Assignments** - You can assign Windows applications to users or groups using remote applications, which can be hosted on the RDS farms you created earlier. This enables you to provide the resources your users need when they need them, and avoids the cost of maintaining idle resources just waiting to be used.

- **Customization** - You can customize your end user environments by making URL redirection assignments. You do this by configuring the client-to-agent URL redirection rules that tell the Horizon Client to redirect URLs from the end user's client machine to a desktop or application within your Horizon Cloud environment. For more information about customization, see Assigning Customizations in Quick-Start Tutorial for VMware Horizon Cloud with Hosted Infrastructure.

Exercise E1: Checking Desktop Capacity Allocation

Before you assign a desktop to a user or group, it is best practice to check the desktop capacity allocation.

1. Navigate to Dashboard
1. In the navigation bar on the left, click Monitor.
2. In the Monitor menu, click Dashboard.

### 2. Examine Utilization Data

1. Scroll down to the Utilization pane, and hover over the diagram. In this example, 7% of the allocated capacity is being used. Utilization is measured as follows:
   - **Horizon 7**: Average CPU, memory, and storage usage from vCenter(s) hosting connected Horizon 7 pods
   - **Microsoft Azure**: Desktop percentage is the number of connected to allocated desktops across Azure pods. Capacity percentage is number of allocated desktops.
2. In the bar graph, you can select and deselect metrics to hide data and enhance focus.
3. Navigate to Capacity Window

1. In the navigation bar on the left, select Settings.
2. In the Settings menu, click Capacity.
3. In the Capacity window, you can adjust your view by location or type.
4. Under Status, click the pod to see a detail summary.

4. View Capacity Allocation Details
Scroll down the Summary window to examine the capacity and utilization data:

1. **Capacity Utilization**: The number of desktops currently in use, divided by the number of desktops possible to use, tells you the capacity percentage by pod.

2. **Desktop & App Utilization**: The number of active sessions, divided by the number of sessions possible, provides you with a measure of user activity in terms of sessions in use, compared to maximum sessions possible.

Note the amount used so that you can compare after assigning the desktop.

For information about the capacity model, see [Service Description: VMware Horizon® Cloud Service™ on IBM Cloud](#).

After verifying that the Desktop Capacity Allocation is sufficient, you can proceed to the next exercise to assign a desktop and see how the capacity allocation is affected.
Exercise E2: Assigning Applications from the Farm

To assign applications to users and groups:

1. **Assign New**

   1. In the navigation bar on the left, click **Settings**.
   2. Under Settings, click **Getting Started**.
   3. Under Desktop Assignment, to the right of Create New Desktop Assignment, click **New**.

2. **Select Applications**

   In the New Assignment window under Applications, click **Select**.

3. **Define Fixed Attributes**
1. In the Definitions tab of the New Application Assignment window, select the **Type**.

2. Under Fixed Attributes, provide the following information:
   - **Location**: From the pop-up list, select the location.
   - **Pod**: From the pop-up list, select the pod containing the farm you want to choose.
   - **Filter Models**: From the pop-up list, select **Type equals VMware Recommended**.
   - **Model**: From the pop-up list, select the model.
   - **Domain**: From the pop-up list, select the domain name.
   - **Join Domain**: Slide right to enable.
   - **Encrypt Disks**: Leave disabled.
   - **NSX Cloud Managed**: Leave disabled.

3. Scroll down to the Flexible Attributes section.

4. **Define Flexible Attributes**
1. In the Flexible Attributes panel, provide the following information:
   - **Images**: Accept the image.
   - **Assignment Name**: Enter a friendly name to identify this assignment. The name must start with a letter, and contains only letters, dashes, and numbers.
   - **VM Names**: All VMs in this assignment inherit the assignment name, and include an appended number, such as Server DTAfloating 1, Server DTAfloating 2, and so on.
   - **Default Protocol**: From the pop-up list, select **Blast Extreme** as the default protocol for end user sessions.
   - **Preferred Client Types**: From the pop-up list, select **Browser**.
   - **Min Desktops**: Enter the minimum number of desktops to be allowed.
   - **Max Desktops**: Enter the maximum number of desktops to be allowed.
   - **Power Off Protect Time**: Enter the number of minutes.

2. In the lower right, click **Next**.

5. **Add Users**
1. In the Users tab, select the users and groups to assign. **Note**: You can click the *Active Directory* search field. If no results are found, click *Search Active Directory*.

2. In the lower right corner, click *Next*.

### 6. Configure Management

1. In the Management tab, accept the defaults.
2. In the lower right, click Next.

7. Verify Summary Information

1. In the Summary tab, review and verify that your settings are correct and complete.
2. In the lower right corner, click Submit.

8. Verify Success
In the Getting Started window, verify that the success banner appears at the top.

9. Verify the Assignment

1. In the left-hand navigation bar, select Assignments.
2. Under Status, verify that the assignment displays a green dot, indicating that the assignment is now active.

For more information, see Create a Remote Application Assignment.

When you finish assigning applications to user and groups, your end users can launch their assigned desktops and remote applications using your FQDN in either the Horizon Client or with HTML Access. You can proceed to the next exercise to create an RDSH session assignment.

Exercise E3: Creating RDSH Session Assignments

To create a session desktop assignment, use the Assignments window after first verifying that your deployment meets the following prerequisites:

- A farm is configured to deliver remote desktops
- The intended farm is in the pod to deliver from
- The intended farm is not already assigned

1. Assign New
1. In the navigation pane on the left, click Assignments.
2. In the Assignments window, click New.

2. Select Applications

In the New Assignment window, select Desktops.

3. Provide Fixed Attributes
1. In the Definition step under the Type pop-up menu, select **Remote**.

2. Under Fixed Attributes, provide the following information:
   - **Location**: Select the location of the pod where the session desktops should be provided.
   - **Pod**: Select the pod.

3. Under **Flexible Attributes**, enter the **Assignment Name**, a memorable name to help end users identify this assignment, using only letters, hyphens, and numbers.

4. In the lower right corner, click **Next**.

4. **Select Applications**
In the Applications tab, select the applications to add.

1. In the lower right, click Next.

2. Select Users and Groups

In the Users tab, search users and groups in your registered Active Directory domains and select the ones for this assignment.

1. In the Users tab, search users and groups in your registered Active Directory domains and select the ones for this assignment.

5. Select Users and Groups
2. In the lower right corner, click Next.

6. Verify the Summary

1. In the Summary tab, review the configuration summary.
2. In the lower right corner, click Submit.

7. Verify in the Assignments Window

1. Verify that the success banner appears at the top.
2. Wait while the system configures the farm's server instances to provide session desktops to the selected users. The green dot indicates that the assignment is active.

For more information, see VMware Horizon Cloud Service on Microsoft Azure Administration Guide.

When you finish assigning session-based desktops to users and groups, this exercise is complete. You can proceed to the next
exercise to assign floating desktops.

Exercise E4: Assigning Floating Desktops

You can choose which type of desktop to assign to a user or group in the Assignments window. You can use the Assignments window to create, edit, and delete an assignment, and update the agent software for any existing assignments. In this exercise, you assign floating desktops. With floating desktops, the user is assigned a desktop upon first login, and the desktop is recreated after the user logs off. Desktops are powered on or off according to the power management policy. For more information, see VMware Horizon Cloud May 2018 Release Technical What’s New Overview.

1. Navigate to New Assignments

1. In the Horizon Cloud Service Administration Console navigation bar, click Assignments.
2. In the Assignments window, click New.

2. Select Desktops

In the New Assignments window, under Desktops, click Select.

3. Define Fixed Attributes

In the New Assignments window, under Desktops, click Select.
1. For **Type**, select **Floating**.

2. In the **Fixed Attributes** panel, provide the following information:
   - **Location**: From the pop-up list, select the location.
   - **Pod**: From the pop-up list, select the pod containing the farm you want to choose.
   - **Filter Models**: From the pop-up list, select the type and equals attributes.
   - **Model**: From the pop-up list, select the model.
   - **Domain**: From the pop-up list, select the domain name.
   - **Join Domain**: Slide to enable.
   - **Encrypt Disks**: Leave disabled.
   - **NSX Cloud Managed**: Leave disabled.

3. Scroll down to the next panel.

4. **Define Flexible Attributes**
1. In the Flexible Attributes panel, provide the following information:
   - **Images**: Accept the image.
   - **Assignment Name**: Enter a friendly name to identify this assignment. The name must start with a letter, and contains only letters, dashes, and numbers.
   - **VM Names**: All VMs in this assignment inherit the assignment name, and include an appended number, such as Server DTAfloating 1, Server DTAfloating 2, and so on.
   - **Default Protocol**: From the pop-up list, select **Blast Extreme** as the default protocol for end user sessions.
   - **Preferred Client Types**: From the pop-up list, select **Browser**.
   - **Min Desktops**: Enter the minimum number of desktops to be allowed.
   - **Max Desktops**: Enter the maximum number of desktops to be allowed.
   - **Power Off Protect Time**: Enter the number of minutes.

2. In the lower right corner, click **Next**.

### 5. Configure Management
1. In the Management tab under Image Updates, enter the number of concurrent quiescing desktops to allow.
2. Under Power Management, select the mode from the pop-up list.
3. Under Timeout Handling, provide the following information:
   - Log Off Disconnected Sessions: Select Never.
   - Max Session Lifetime: Enter the number of minutes.
4. Under Schedule Power Management, provide the following information:
   - Name: Enter the name for this schedule.
   - Day(s): Click the Days field and select one or more days of the week from the drop-down list.
   - Start Time: Select the time of the day to start the schedule from the drop-down list.
   - End Time: Select the time of day to end the schedule from the drop-down list.
   - All Day: Leave unchecked.
   - Timezone: Select your timezone if necessary.
   - Min Desktops: Select the minimum number of desktops to include.
5. In the lower right corner, click Next.

6. Assign to Users or Groups
In the Users tab, select the users and groups to assign desktops to.

Note: In the Users tab, you can click the Active Directory search field. If no results are found, click Search Active Directory.

1. In the lower right, click Next.

2. Verify the Summary Information
1. In the Summary tab, verify that all selections are correct and complete.
2. In the lower right corner, click Submit.

8. Verify Completion

1. Wait until the green banner appears at the top, indicating success.
2. Wait until the green dot appears in the Status column, indicating that the floating desktop assignment is now active.
9. Launch Horizon Client

- Launch Horizon Client.

10. Log in to Horizon Client

1. Enter your login credentials for Horizon Client:
   - **Username**: Enter the username.
   - **Password**: Enter the password.

2. Click **Login**.

11. Launch the Floating Desktop
In Horizon Client, select a virtual desktop.

1. Verify that the virtual floating desktop launches properly.

2. For more information, see VMware Horizon Cloud Service with Microsoft Azure Administration Guide, and search the guide for Create a Floating VDI Desktop Assignment.

Now that you have successfully assigned a floating desktop, you can proceed to the next exercise to assign a VDI-based dedicated desktop. The process is very similar.

**Exercise E5: Assigning Dedicated Desktops**

You use the Assignments window to create, edit, and delete assignments, choose which type of desktops to assign, and update the agent software for any existing assignments.

In this exercise, you assign a dedicated desktop. Your end-users are assigned a virtual desktop upon first login. They continue to get the same desktop whenever they log in subsequently, until or unless you rebuild the desktops. For more information, see VMware Horizon Cloud May 2018 Release Technical What's New Overview.

1. Navigate to New Assignments
1. In the navigation bar on the left, select **Assignments**.
2. In the Assignments window, click **New**.

### 2. Select Desktops

- In the New Assignment window under Desktops, click **Select**.

**Note:** To assign AppStacks or RDSH applications instead of desktops, you would select **Applications**.

### 3. Select a Dedicated Desktop Type
In the Definitions tab of the New Desktop Assignment window, for Type, select **Dedicated**.

1. Under Fixed Attributes, provide the following information:
   - **Location**: From the pop-up menu, select the location.
   - **Pod**: From the pop-up menu, select the pod.
   - **Filter Models**: In the first pop-up menu, select **Type**, and in the second, **VMware Recommended**.
   - **Model**: Select a **Desktop Model** from the pop-up menu.
   - **Domain**: From the pop-up menu, select the domain.
   - **Join Domain**: Slide right to enable.
   - **Encrypt Disks**: Leave disabled.
   - **NSX Cloud Managed**: Leave disabled.

2. Scroll down to the Flexible Attributes section.

4. Set the Flexible Attributes
1. Under Flexible Attributes, provide the following information:
   - **Image**: Select the image from the pop-up menu.
   - **Assignment Name**: Enter a unique name to identify this assignment. The name must start with a letter, and contains only letters, dashes, and numbers.
   - **VM Names**: VMs in this assignment inherit the assignment name, and include an appended number, such as Server DTA1 1, Server DTA1 2, and so on.
   - **Default Protocol**: Choose **Blast Extreme** as the default protocol for end user sessions.
   - **Preferred Client Type**: Accept the browser default with which to launch assignments associated with this pool.
   - **Min Desktops**: Enter the minimum number of desktops to be allowed. In this example, it is 1.
   - **Max Desktops**: Enter the maximum number of desktops to be allowed. In this example, it is 5.

2. In the lower right corner, click **Next**.

**5. Schedule Power Management**
1. In the Management tab under Schedule Power Management, click **Add a row**.

2. Under Schedule Power Management, provide the following information:
   - **Name**: Provide a name for this schedule.
   - **Days**: Select one or more days of the week to schedule.
   - **Start Time**: Select a time of the day to start the schedule.
   - **End Time**: Select the time of the day to end the schedule.
   - **Timezone**: Select the appropriate time zone.
   - **Min Desktops**: Enter the minimum number of desktops to include.

3. In the lower right, click **Next**.

### 6. Select a User or Group
In the Users tab, select a user or group:

1. Click the Active Directory search field, and start entering the name of the user or group.
2. If you do not know the name, click **Search Active Directory** for a list of all names.
3. In the Active Directory hit list, select the name.
4. In the lower right corner, click **Next**.

### 7. Submit

1. In the Summary tab, review the summary.
2. In the lower right corner, click **Submit**.
8. Verify Completion

1. Verify that the success banner appears at the top of the window.
2. Wait until the green dot appears in the Status column, indicating that the new assignment is now active. This might take a few minutes.

9. Launch Horizon Client

- Launch Horizon Client.

10. Log in to Horizon Client
1. Enter your login credentials for Horizon Client:
   - **Username**: Enter the username.
   - **Password**: Enter the password.

2. Click **Login**.

### 11. Launch the Dedicated Desktop

- In Horizon Client, launch the dedicated virtual desktop.
12. Verify Success

- Verify that the virtual dedicated desktop launches properly.

When you finish assigning a dedicated desktop to a user or and group, you have completed the entire workflow. In the next two chapters, you can proceed to explore the Horizon Cloud Service monitoring and analytics features and the VMware User Environment Management capabilities in greater depth.

Exploring Reporting and Analytics

About Monitoring and Analytics

After setting up Horizon Cloud Service on Microsoft Azure, you can explore the monitoring and analytics functionality.

Horizon Cloud Analytics includes dashboard, activity monitoring, and reporting features, which provide the following benefits:

- **Contextual metrics**: Generates in-depth information about user experience and resource usage. We leverage contextual metrics to give you details on user experience, and resource utilization.
- **Historical utilization**: Provides ability to visualize usage with perspective on capacity, concurrency, and uniqueness. The system enables you to go back in time, to visually evaluate differences in how your resources are consumed by your deployment.
- **Endpoint landscape**: Facilitates understanding access patterns by protocol, client type, and location. We also monitor how information is gathered directly from the endpoints that the users are using to access the system.

The result is that you have one place to go to get all the details you need to monitor the health and performance of your Horizon Cloud Service implementation.
Exploring Dashboard and Activity
This section explores the Dashboard and Activity options.

The **Unified Dashboard** puts current information about your deployment at your fingertips, including deployment health, sessions, and issues across all connected pods.

The **Activity** window displays audit logs so you can view the history at any time.

1. **Launch the Dashboard**

   - In the navigation bar on the left, click **Monitor > Dashboard**.
   - You can use the **Dashboard** to keep your eye on deployment health, capacity, sessions, and utilization data of all pods connected to the Horizon Cloud Service. At a glance, you can spot issues across all connected pods, and then drill down to reveal the details.

1.1. **Customize the Display**
1. You can filter the dashboard to display selected metrics to make it easier to focus on what is most important, and hide the rest.
2. You can expand and collapse the side panel revealing issues and sessions related to each location in your system.

1.2. Spot Issues As They Arise

When you hover your cursor over a location icon, the corresponding map tool-tip is displayed.

1. In the tool-tip, click View to highlight the issues in that location.
2. The Issues pane on the right displays five issues at a time. Click View to see more, if any.

1.3. View the Details
In the Global Footprint - Health window, you can examine the details more closely, including a description of the issue, where it occurred, and the type of pod it occurred in.

1.4. Filter by Location or Pod

In the upper right, you can use location options to filter the issues by location, or by pod.

1.5. Filter by Description

You can also filter issues by type, description, pod, pod type, or location.
1.6. View Sessions

1. In the panel on the right, click the Session tab to take a look at the session usage of all pods in a location.
2. Hover your cursor over a location icon to display the session usage for that location.

1.7. View Utilization and Sessions

- Scroll down to see utilization and session data in a visual graph format, and hover your cursor over the diagrams for more details.

2. Monitor Activity
The **Activity** window provides audit logs for your use at any time.

1. In the navigation bar on the left, click **Monitor > Activity**.
2. In the Activity pane, click **Show** to select a time range to see all activity during the indicated range.

When you finish exploring the dashboard and activity monitoring options, proceed to the next exercise to explore reports and notification options.

**Exploring Reports and Notifications**

You can access the built-in reports from the **Reports** window. This makes it easy to review the health of your Horizon Cloud Service and monitor end user experience within your system.

You can access the **Notifications** to review the history of where and when actions were taken and errors occurred.

1. **Explore Reports**
Horizon Cloud Service includes a variety of pre-built reports covering VDI and RDSH desktop usage, VDI applications usage, and user mapping, from Horizon 7 to Horizon Cloud on Microsoft Azure.

- In the left-hand navigation bar under Monitor, click Reports.

1.1. Select a Report to Customize

You can customize the data displayed in each report.

- For example, select Azure Concurrency to see a record of the concurrency status of all pool and farm assignments in Azure.
Click the **Period** arrow and select a time frame from the pop-up menu to ensure that the report is focused and relevant.

### 1.2. Select a Report to Export

When you have the information you want, you can export the data in each report.

- For example, select the **Utilization** report to view consumption trends for deployed capacity and concurrency metrics. Notice that you can hover your cursor over the line graph to reveal additional details.
- To export the report, navigate to the upper left, and click **Export**.

### 1.3. Export Report
2. Examine Notifications

Notifications are a handy way to look at the history of where and when actions were taken and errors occurred.

1. In the left-hand navigation bar, expand Monitor.
2. In the Monitor menu, click Notifications.
3. In Show, you can select a time range from the pop-up menu.

For more detailed information about how to use reports and notifications, see Horizon Cloud Service documentation.

You have now reached the end of the exploration exercises. The next section explores the VMware User Environment Management capabilities in greater depth.

Exploring VMware User Environment Manager

Installing VMware User Environment Manager on Microsoft Azure

VMware User Environment Manager provides a wide range of capabilities such as personalization of Windows and applications, contextual policies for enhanced user experience, and privilege elevation to aid in your privilege management strategy. VMware User Environment Manager has the flexibility to run on physical, virtual, and cloud-hosted machines.

If you are already using VMware User Environment Manager on physical or virtual desktops or RD Session Host servers, your knowledge transfers immediately to Horizon Cloud Service on Microsoft Azure.

You provide your own Microsoft Azure IaaS capacity, on which you deploy Horizon Cloud Service and VMware User Environment Manager, and which is included in Horizon Cloud Service.

The infrastructure requirements are minimal, comprised primarily of SMB file shares. VMware User Environment Manager uses one share for configuration data, and another for profile archive data. You can deploy one or more Windows Server VMs on Microsoft Azure, and configure file sharing. For comprehensive share requirements, see Installing and Configuring VMware User Environment Manager. While there are several server models available in the Microsoft Azure Marketplace, consider using Dv2, Dv3, or Ev3 series.
VMs to create file servers for the requisite SMB file shares. Additional disks can be added to accommodate increased performance demand (IOPS) as needed.

![Figure F1: VMware User Environment Manager Process Flow](image)

**Note:** For Horizon 7, the default installation directory for the FlexEngine.exe is `C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe`. But because the UEM agent is installed alongside the Horizon DaaS agent when importing a VM from the Azure Marketplace, the FlexEngine.exe lands in the default installation directory `C:\Program Files\VMware\Horizon Agents\User Environment Manager\FlexEngine.exe`. For more information, see **Updating the Agent-Related Software Used by Horizon Cloud**. See also: **Installing and Configuring VMware User Environment Manager** and **VMware Horizon Cloud on Microsoft Azure 2.0 > Installing VMware User Environment Manager on Microsoft Azure**.

### Exploring Deployment Options

You can use Microsoft Azure to extend your existing data centers in a hybrid-cloud model, or treat Microsoft Azure as a stand-alone, public-cloud capacity. Horizon Cloud Service and VMware User Environment Manager support both configurations.

- **Stand-alone:** For the stand-alone or single-site deployment model, see **Installing and Configuring VMware User Environment Manager** for everything you need to know to deploy. VMware User Environment Manager is installed and managed the same way, whether deployed on premises or in a public cloud.

- **Hybrid-cloud:** For the hybrid-cloud or multi-site model, Microsoft Azure capacity is essentially a remote customer data center. See **VMware Workspace ONE and VMware Horizon Reference Architecture** for detailed information to configure VMware User Environment Manager for a consistent user experience as end users roam from site to site.

### Optimizing VM Performance

A common question for multi-site VMware User Environment Manager deployments is whether users from multiple sites can access a single SMB file share instance at the primary data center. While this is possible, there are design considerations to ensure the best experience.

DirectFlex is a feature of VMware User Environment Manager that reads and writes personalization data as applications are opened and closed. DirectFlex improves the efficiency of the VMware User Environment Manager agent by only fetching configuration data that is needed, when it is needed, rather than reading it all during login. By design, DirectFlex makes frequent requests to the SMB file servers hosting the VMware User Environment Manager configuration and user shares. The latency of these requests directly affects the end-user experience. Typically, anything less than 20 milliseconds has no noticeable impact. As latency gets worse, the chance and severity of impact to the end-user experience increases.

Even a high-performing ExpressRoute may have latency greater than 20 milliseconds, so it is recommended to deploy VMware User Environment Manager in the same Azure region as your Horizon Cloud Service pod. If your design goal is to have a single VMware User Environment Manager deployment for both on-premises and cloud-hosted VMs, Distributed File System (DFS) replication is
recommended. This model provides IT with a single point of administration, while keeping configuration and user data geographically near the VMs accessing the data.

Figure F2: VMware User Environment Manager Deployment Options

For more information about configuring DFS for multi-site VMware User Environment Manager deployments, see VMware Workspace ONE and VMware Horizon Reference Architecture.

Using the NoAD Mode

VMware User Environment Manager has traditionally been configured and enabled using ADMX templates with Group Policy, and logon or logoff scripts. Version 9.1 introduced an alternative, XML-based option called NoAD Mode.

NoAD Mode simplifies administration by eliminating the need to create and manage GPOs, and can be used for on-premises, hybrid-cloud, and public-cloud deployments of VMware User Environment Manager.

When deploying VMware User Environment Manager in a hybrid-cloud or multi-site model, NoAD Mode has the added benefit of not being dependent on Domain Controllers and GPO replication. While not a requirement, NoAD Mode is an alternative that may suit the needs of your organization, especially for hybrid-cloud and public-cloud deployments.
VMware User Environment Manager seamlessly integrates with Horizon Cloud Service, and provides a consistent user experience across physical, virtual, and cloud-hosted PCs and RD Session Host servers.

For more information about the deployment process, see Deploying and Using VMware Horizon Cloud on Microsoft Azure. For more information about VMware User Environment Manager, see User Environment Manager: Technical Overview and Quick-Start Tutorial for User Environment Manager.

Summary and Additional Resources

Summary

Upon completion of the exercises of this tutorial, you now have a basic deployment of Horizon Cloud Services with at least one pod using capacity from Microsoft Azure. You created a master image, set up a farm from that image, and provisioned virtual desktops and remote applications that your end users can securely access from any device. You used the Horizon Cloud Administration Console for unified health monitoring and reporting, and you explored the integration with VMware User Environment Manager.
Although the basic environment you just set up is for evaluation purposes only, you are now in a position to explore further on your own as you evaluate this offering. When you are ready to deploy a production environment, see the Horizon Cloud Service documentation.

### Terminology Used in This Tutorial

The following terms are used in this tutorial:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base image</td>
<td>A VM, also referred to as a desktop image, a golden image, or a master image, that is an RDS-enabled Microsoft Windows Server operating system VM configured with the Horizon Agent and DaaS Agents, and is created and configured for desktop deployment.</td>
</tr>
<tr>
<td>Cloud</td>
<td>A set of securely accessed Internet-hosted services</td>
</tr>
<tr>
<td>DaaS agent</td>
<td>Desks as a service agent</td>
</tr>
<tr>
<td>Disk IOPS</td>
<td>Input and output operations per second (IOPS, pronounced eye-ops) is an input and output performance measurement used to characterize computer storage devices like hard disk drives (HDD), solid state drives (SSD), and storage area networks (SAN).</td>
</tr>
<tr>
<td>IaaS capacity</td>
<td>Capacity provided through infrastructure as a service</td>
</tr>
<tr>
<td>RDSH farm</td>
<td>RDS session host farm VMs are the server instances that provide session-based desktops and remote applications to your end users.</td>
</tr>
<tr>
<td>Virtual desktop</td>
<td>The user interface of a virtual machine that has been made available to an end user</td>
</tr>
<tr>
<td>Virtual machine</td>
<td>A software computer running an operating system or application environment that is backed by the physical resources of a host</td>
</tr>
<tr>
<td>VMware Horizon Cloud Service control plane</td>
<td>VMware hosts the Horizon Cloud Service control plane in the cloud and provides ongoing feature updates and enhancements. This service enables the central orchestration and management of virtual desktops, desktop applications, remote desktop sessions, and remote applications for your users. The cloud service also manages your pods (previously called nodes), which are physically located in your provided capacity environments. When you log in to the cloud service, you see all your pods and perform management activities across them, regardless of where they are physically located. The VMware Horizon Cloud Service control plane also hosts the Horizon Cloud Service Administration Console, which is accessible from anywhere at any time, providing maximum flexibility.</td>
</tr>
<tr>
<td>VMware Horizon Cloud Service Administration Console</td>
<td>The common management user interface hosted by the cloud control plane. The Horizon Cloud Service Administration Console runs in industry-standard browsers and provides a single location for management tasks involving user assignments and the virtual desktops, remote desktop sessions, and applications.</td>
</tr>
<tr>
<td>VNet peering</td>
<td>Virtual network which is used to connect Horizon Cloud Service VNet with Microsoft Active Directory. Virtual network peering enables you to seamlessly connect two Microsoft Azure virtual networks. Once peered, the virtual networks appear as one, for connectivity purposes.</td>
</tr>
</tbody>
</table>

**Note:** For additional VMware terms and concepts, see the VMware Technical Publications Glossary or VMware Technical Publications Glossary Online. For information about Microsoft Azure-specific terms, see the Microsoft Azure Glossary.

### Additional Resources

For more information about Horizon Cloud Service on Microsoft Azure, you can explore the following resources:

- Application and service principal objects in Azure Active Directory
- Blog post: Deploying and Using VMware Horizon Cloud on Microsoft Azure: New Video Series
QUICK-START TUTORIAL FOR VMWARE HORIZON CLOUD ON MICROSOFT AZURE

- Blog post: Get Ready for VMware Horizon Cloud on Microsoft Azure
- Blog post: Here Comes Horizon Cloud
- Blog post: Horizon Cloud on Microsoft Azure—It Keeps Getting Better
- Blog post: VMware Horizon Cloud on Microsoft Azure: Learn More at VMworld 2017 U.S.
- Blog post: User Environment Manager: Technical Overview
- Blog post: Quick-Start Tutorial for User Environment Manager
- Getting Started with VMware Horizon Cloud Service on Microsoft Azure
- Horizon Cloud on Microsoft Azure Datasheet
- Horizon Cloud Service on Microsoft Azure documentation
- Horizon Cloud Support for Microsoft Azure - FAQ
- Installing and Configuring VMware User Environment Manager
- Installing and Configuring User Environment Manager in NoAD Mode
- Microsoft SMB Protocol and CIFS Protocol Overview
- Video: Create an Image and Deploy a Farm
- Video: VMware Horizon Cloud Demo
- Video: Previewing Horizon Cloud Service on Microsoft Azure
- Video: VMware Horizon Cloud on Microsoft Azure – Getting Started
- Video: VMware User Environment Manager 9.2 - Privilege Elevation Demo
- Video: VMware User Environment Manager 9.4: Argument-Based Privilege Elevation - Feature Walk-through
- Video: VMware User Environment Manager 9.2: Publisher-Based Application Blocking & Privilege Elevation - Feature Walk-through
- VMware and Microsoft
- VMware Horizon 7 Enterprise Edition Multi-Site Reference Architecture
- VMware Horizon Cloud
- VMware Horizon Cloud Service on Microsoft Azure Cheeksheet

About the Authors
This guide was originally written and recently updated by:

- Rick Terlep, End-User-Computing Architect, End-User-Computing Technical Marketing, VMware
- Cindy Heyer Carroll, Technical Writer in End-User-Computing Technical Marketing, VMware
- Josh Spencer, End-User-Computing Architect, End-User-Computing Technical Marketing, VMware
- Jerrid Cunniff, End-User-Computing Cloud Services Senior Architect, VMware

Feedback
The purpose of this guide is to assist you, and your feedback about this is valuable. To comment on this guide, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.