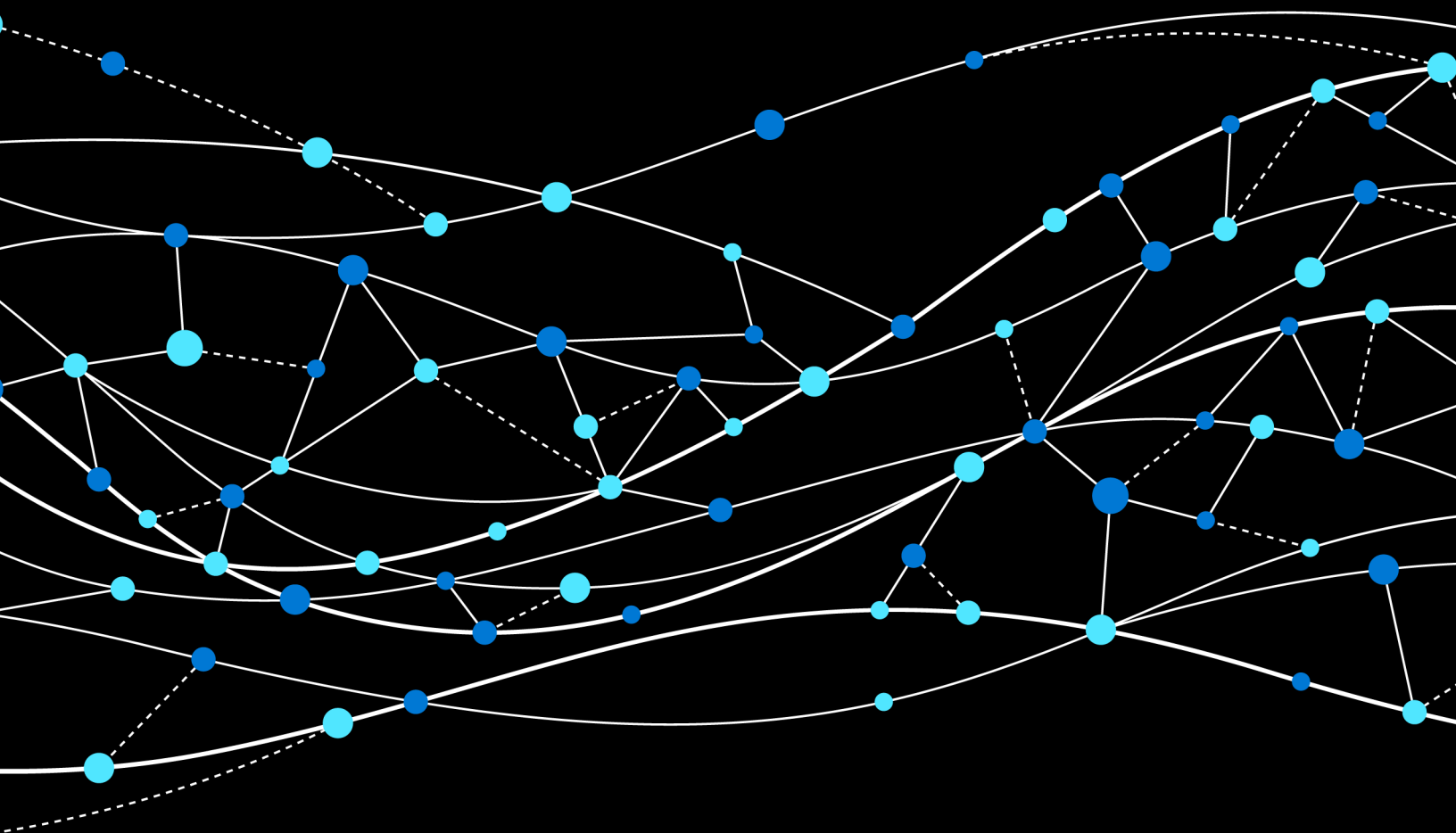


# Migration Guide: VMware Horizon Cloud and Azure Virtual Desktop



# Table of contents

## 03 /

### Introduction

- 03 Why consider a cloud VDI on Azure?
- 04 Why migrate to VMware Horizon Cloud Service on Azure?
- 05 VMware Horizon Cloud on Azure and Azure Virtual Desktop reference architecture

## 08 /

### Preparing for your migration

- 08 Step 1: Prerequisites
- 09 Step 2: Azure Migrate
- 10 Step 3: Discovering VMs
- 11 Step 4: Review assessment

## 13 /

### Preparing for your VMware Horizon Cloud environment with Azure Virtual Desktop

- 13 Azure Virtual Desktop prerequisites
- 16 VMware Horizon Cloud on Azure prerequisites
- 18 Profile management guidelines
- 19 Conditional access
- 20 Dynamic Environment Manager

## 21 /

### Creating your first Horizon Cloud Service pod with Azure Virtual Desktop

- 22 Deployment of Horizon Cloud Pod with Azure Virtual Desktop

## 28 /

### Post-deployment guidance

- 28 Testing the VMware Horizon deployment
- 29 Optimizing costs
- 30 VMware Horizon Cloud on Azure health and usage

## 33 /

### Guidance on additional capabilities

- 33 VMware App Volumes for Horizon Cloud on Azure
- 34 Microsoft Teams
- 35 Power management
- 36 Monitoring and analytics

## 38 /

### Conclusion and resources

# Introduction

Today, many companies are considering new ways of working and assessing how to bring resilience to their organization, including the capability of providing a secure, remote desktop experience for employees, accessible from virtually anywhere.

## Why consider a cloud VDI on Azure?

**Virtual desktop infrastructure (VDI)** is often used to deliver a remote desktop experience to employees internal and external to a company. However, on-premises solutions do not realize the full value of the benefits and modernization that cloud desktop virtualization offers.

Azure Virtual Desktop is a flexible cloud VDI platform for the hybrid workspace. Azure Virtual Desktop is designed to deliver virtual desktops and apps hosted on Microsoft Azure, giving you the full benefits of the cloud, such as scalability and reduced infrastructure cost. In addition, you will receive the benefits of Azure, including integrated Microsoft security features and the unique Windows 10 Enterprise multi-session experience, which combines the Windows 10 experience with the ability to run multiple concurrent user sessions, which was only previously available on Windows Server operating systems.

Your users may already have a desktop virtualization hosted on **Remote Desktop Services (RDS)** and managed through VMware. VMware Horizon is a desktop virtualization platform from VMware that works both on-premises and in Microsoft Azure, and is integrated with Azure Virtual Desktop through VMware Horizon Cloud Service on Microsoft Azure. If you choose to migrate, VMware Horizon Cloud will provide you with a single control plane that allows you to manage on-premises and cloud-based environments, allowing you to use your existing investments. Horizon Cloud on Azure supports the features of Azure Virtual Desktop, which means you can deliver the same Horizon capabilities, including the Blast Extreme protocol, cost- and time-saving management tools, security, and broad endpoint support to your on-premises and Azure-based virtual desktop and app environments. This helps simplify migration and allows you to migrate at your own pace.

This e-book is a guide to assist organizations in moving on-premises VDIs hosted on RDS and VMware Horizon Enterprise to Horizon Cloud on Azure so you can run your VDI on Azure Virtual Desktop.

## Why migrate to VMware Horizon Cloud Service on Azure?

There can be many reasons for migrating, and your company's needs can determine the pace at which you do so. A typical scenario that would benefit from migration is when there is aging hardware that needs to be replaced. In this situation, rather than replacing the on-premises hardware, the customer can take full advantage of the economics of Azure Virtual Desktop, including built-in licensing, discounted consumption costs, and flexibility of deployment in terms of geographic region, shifting from a capital expenditure to an operating expenditure.

Besides the need to replace hardware, companies often migrate so they can realize the benefits of modernization, which helps enable secure remote work, simplify management, and reduce operating costs through an always up-to-date software as a service model from VMware, with the consumption-based infrastructure pricing and extensive global footprint of Azure. Horizon Cloud on Azure allows you to bring your Azure infrastructure capacity and pair it with the Horizon Cloud service without the need for third-party tools. It also provides additional capabilities, such as Power Management, image management, an advanced protocol that adapts to changing network conditions, AD integration, and hybridity, which help enhance and further simplify management. Some additional benefits of migrating are detailed as follows.

### Centralizing management to optimize costs

You can reduce management and infrastructure costs with advanced, centralized management capabilities, and a pricing model that allows you to pay only for what you use. Choose what's suitable for your organization with the single flexible licensing model from VMware, enabling on-premises, cloud, and hybrid environments. Windows 10 multi-session provides additional scale and cost savings with the ability to run concurrent user sessions, thereby maximizing your VMs.

### Offering a familiar experience to your users and IT

Manage your Azure and Azure Virtual Desktop deployment from your Horizon Cloud console with customizations and tooling that support your business needs. Extend and offer a streamlined digital workspace to all apps and use cases, with a full-featured client and advanced remote protocols on Windows, macOS, iOS, Android, Linux, and Thin clients.

## Helping to improve your security posture

Built-in and integrated security features help keep your data safe in the cloud instead of local desktops. You can also use Azure Security Center for enhanced security from the endpoint to the applications, and you can provide additional protection by enabling **role-based access control (RBAC)**.

In the next section, we will be discussing the reference architecture for both Azure Virtual Desktop and Horizon Cloud on Azure.

## VMware Horizon Cloud on Azure and Azure Virtual Desktop reference architecture

This section looks at the combined technologies of Azure Virtual Desktop and Horizon Cloud on Azure. *Figure 1* shows the responsibilities between Microsoft, VMware, and the customer:

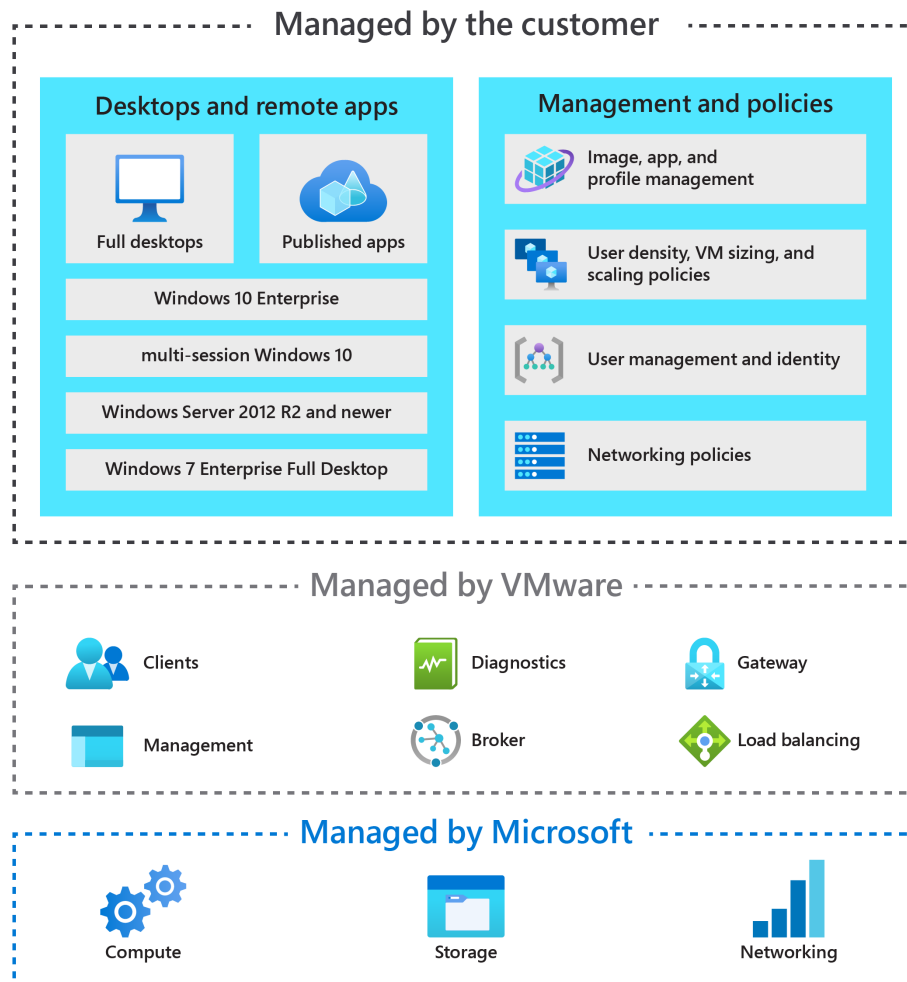
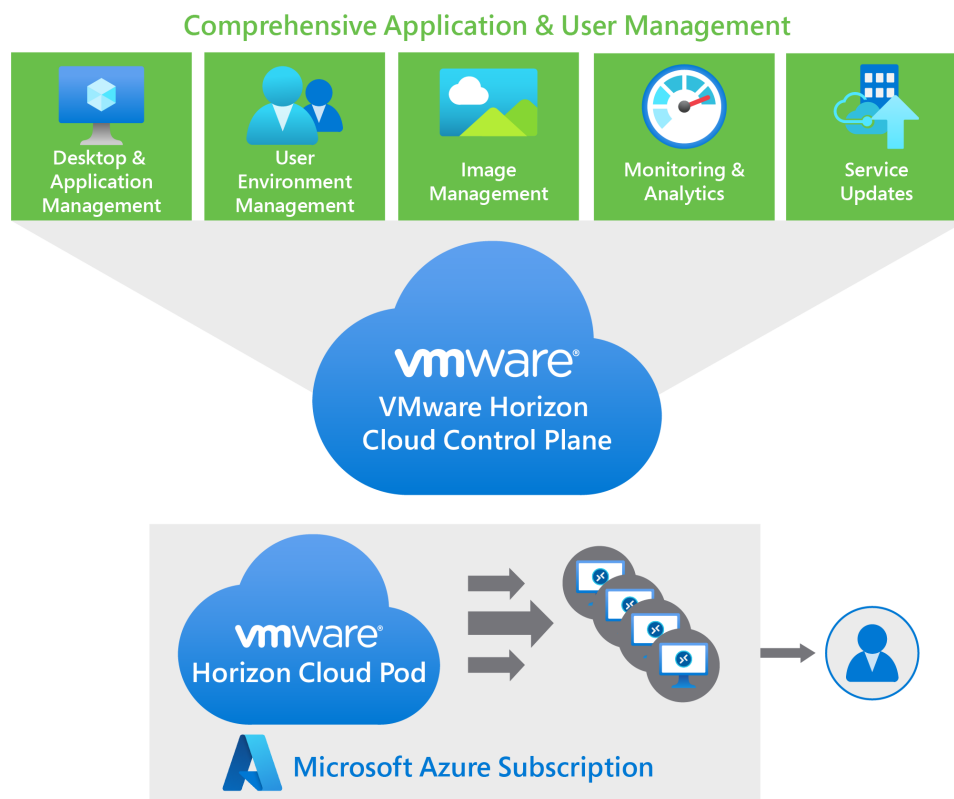


Figure 1: Responsibility distribution between Microsoft, VMware, and the customer

Microsoft provides the underlying infrastructure, including compute, storage, and network within Azure. VMware adds a management layer (Horizon Control Plane) to Azure and feature enhancements within the Horizon Cloud platform. It is important to note that VMware is responsible for core desktop virtualization infrastructure management, including the broker, gateway, management, diagnostics, load balancing, and the client. Like a native Azure Virtual Desktop deployment, the customer is responsible for the desktop and remote apps and management and policies.

As mentioned earlier, VMware is responsible for hosting the Horizon Control Plane and providing feature updates and enhancements for a software-as-a-service experience. Horizon Cloud on Azure is a service that runs and scales across multiple Microsoft Azure regions. This service allows you to deploy Horizon Cloud pods into your Azure tenants, as shown in the illustration in *Figure 2*:



**Figure 2:** Using VMware Horizon Cloud pods for deploying to a customer Azure subscription

The cloud control plane also hosts a familiar management user interface called the Horizon Universal Console. The Horizon Universal Console runs in all industry-standard browsers. This console provides you with a single location for management tasks involving user assignments, virtual desktops, RDSH-published desktop sessions, and applications.

Figure 3 shows a high-level architecture of the hybrid cloud model of VMware Horizon Cloud on Microsoft Azure:

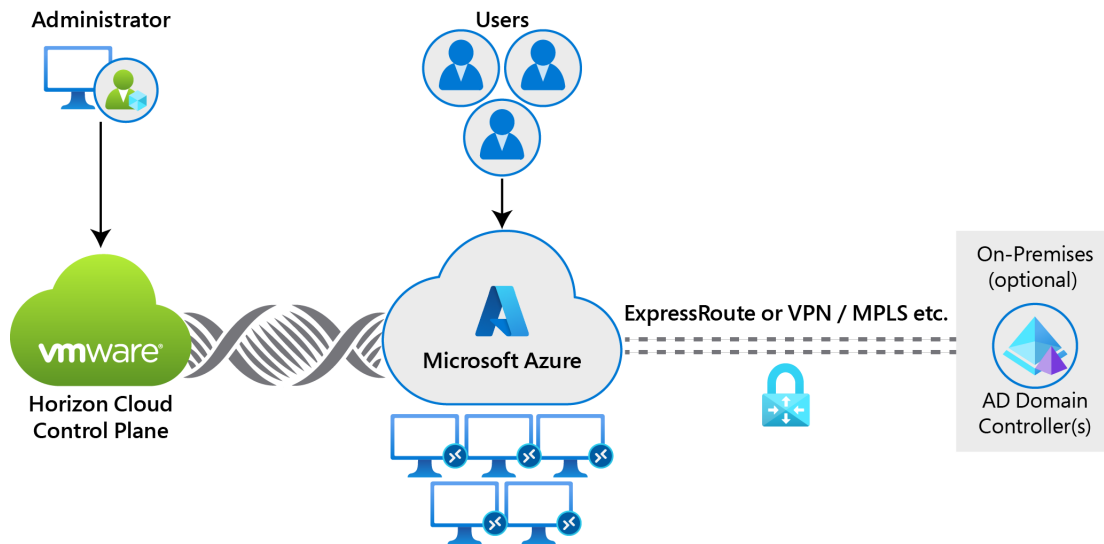


Figure 3: VMware Horizon Cloud Service on Microsoft Azure overview

Now that you know more about Azure Virtual Desktop and the core benefits of migrating your on-premises VDI to Horizon Cloud on Azure, the following sections will outline key steps and practices that will help you in your migration planning. They will break the migration process down into three sections: *Preparing for your migration*; *Preparing for your VMware Horizon Cloud environment with Azure Virtual Desktop*; and *Creating your first Horizon Cloud Service pod with Azure Virtual Desktop*.

## Key benefits

By migrating your VDI, you can realize the benefits of modernization, including:

- Improved security posture through built-in and integrated security features with Azure Virtual Desktop
- Reduced hardware and infrastructure costs, thereby lowering overall capital expenditure
- Simplified management that allows you to deploy and scale within minutes to meet your business needs
- A seamless experience optimized for Windows 10 and Microsoft 365 Apps, including Microsoft Teams

Since Azure Virtual Desktop runs alongside the Citrix Virtual Apps and Desktops service, you'll also be able to take advantage of unified management across your entire hybrid environment.

# Preparing for your migration

This section provides guidance to help migrate existing resources and assess your current environment state, including the sizing requirements of your environment when using Horizon Cloud on Azure. The steps for assessing your environment are broken down into four steps. This phase will help set you up for preparing your VMware Horizon Cloud environment, which we'll cover in the next section.

## Step 1: Prerequisites

To begin with, we'll briefly look at how to connect to Azure and configure Active Directory before moving on to the migration and VM discovery steps.

First, an [Azure subscription](#) is required. If your organization already has one, make sure you have the correct level of permissions. During this migration, you need permission to work with storage and networking components and VMs. Ensure that domain services, either Active Directory or Azure Active Directory Domain Services, are synchronized with **Azure Active Directory (Azure AD)**. Ensure that the domain service is accessible from the Azure subscription and connected virtual network where Horizon Cloud will be deployed. Follow the [Azure AD Connect](#) guide for synchronizing Active Directory on-premises with Azure AD.

**Note:** *For the latest guidance on setting up Azure AD based on the newest product capabilities, please refer to Azure Virtual Desktop documentation [here](#).*



## Step 2: Azure Migrate

There is a dedicated wizard within the Azure portal that allows you to set up Azure Migrate for desktop virtualization. This can be found in the section entitled VDI, as shown in *Figure 4*:

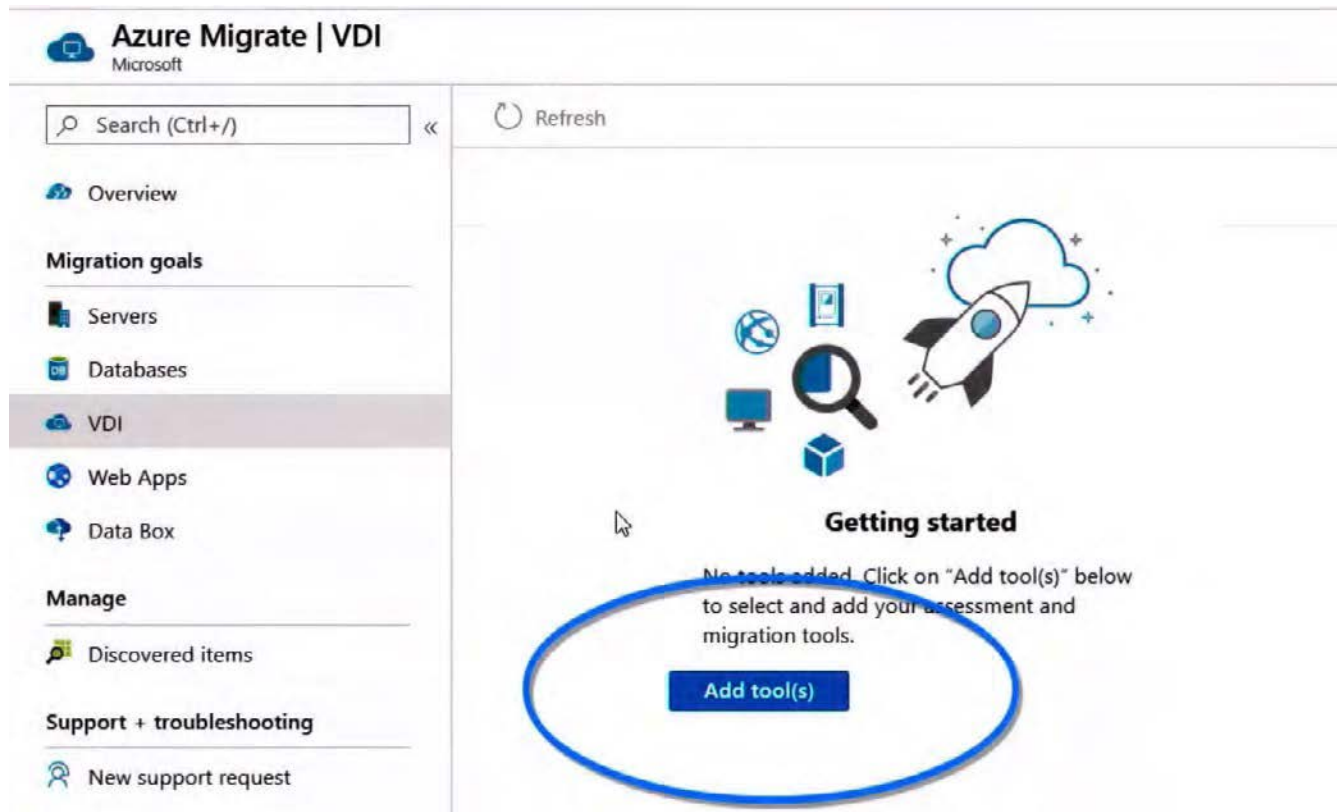


Figure 4: The Azure Migrate wizard

In this wizard, you set your subscription, resource group, project name, and region. You can then start the assessment of the current desktop virtualization environment by selecting **Register**. You can create a new Azure Migrate project in the destination Azure subscription. Select the option to assess and migrate servers, select **VDI**, and then add a tool. After configuring basic parameters, such as the subscription, resource group, and location, make sure you choose **Azure Migrate: Server Migration** as the migration tool. The setup wizard also allows you to select optional ecosystem partner tools that provide additional benefits on top of the server migration. As per the example, you can choose [Lakeside SysTrack](#) as your assessment tool on top of Azure Migrate as your migration tool.

Lakeside is an ecosystem partner that specializes in assessing desktop virtualization environments. Lakeside SysTrack provides in-depth knowledge about your current workload to help you determine sizing and usage. Lakeside SysTrack does support VMware environments to help you assess your environment for migration to Azure. After connecting Azure Migrate and optional ecosystem partner tools and accepting any requested permissions, the discovery process starts.

## Step 3: Discovering VMs

During this step, the virtual desktops of your current environment are discovered and assessed. During this step, we are going to gather a large amount of information about your existing infrastructure. If you selected Lakeside SysTrack as your assessment tool in the previous step, this will help you to collect even more information about your current desktop virtualization workload. Lakeside SysTrack requires an agent that you can easily install using your existing deployment tools. *Figure 5* shows the Lakeside SysTrack visualizer, which makes current usage, consumption, and application inventories easy to digest and helps you to determine the sizing of your Horizon Cloud VMs and much more:

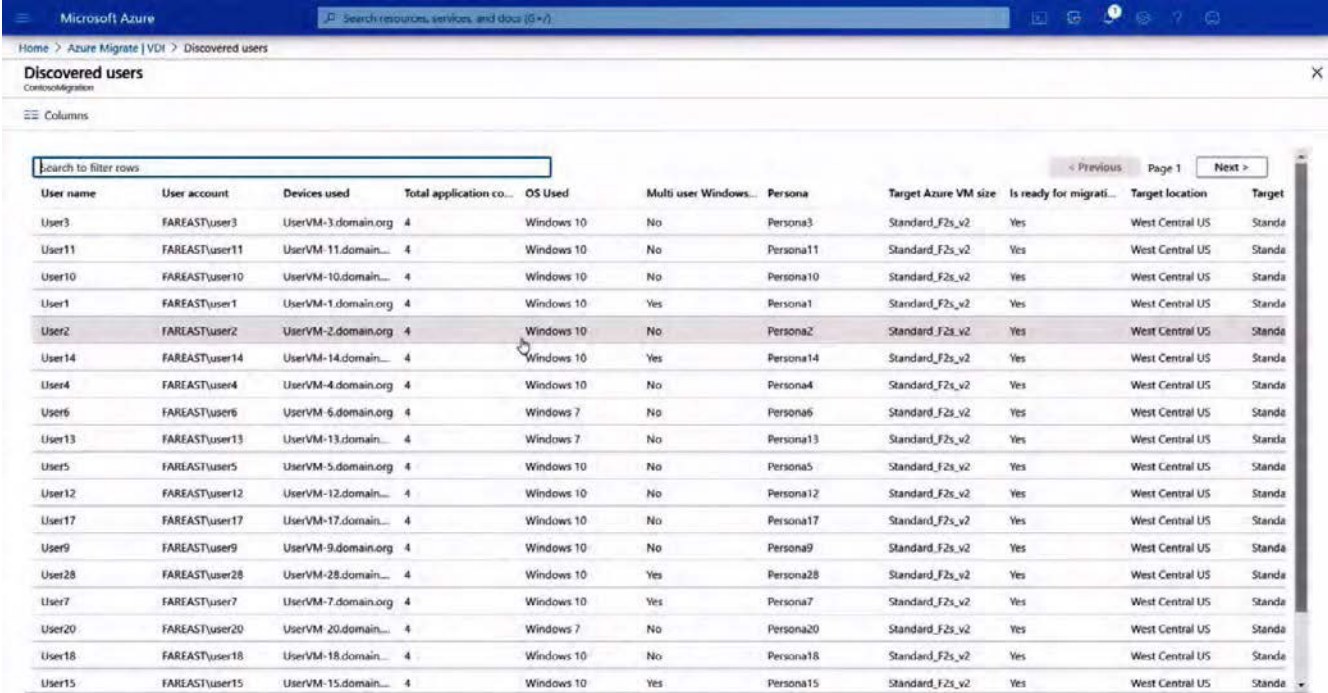


Figure 5: The Lakeside SysTrack visualizer

As part of this step, you also gather insights on any application back-end workloads you may or may not want to move to Azure as well. Typically, moving those applications' back ends to Azure ensures the best performance. In that scenario, the client side of the application running in Horizon Cloud on Azure is closer to the application's back end. Azure Migrate can also assist you with moving these workloads to Azure as well. If you decide not to move some of these back-end resources, ensure that you configure connectivity with your on-premises environment using either ExpressRoute or a site-to-site VPN. Detailed steps relating to discovery can be found here.

## Step 4: Review assessment

When an adequate amount of data is captured, you can review the assessment data to determine the best migration path for you. This assessment data includes the raw assessment data from the desktop and the data broken down into different user personas. As you analyze the data, you can determine the most viable and cost-effective use of both pooled and personal Virtual Desktop resources. The information gathered as part of step three is visible in your Azure portal. *Figure 6* shows an example containing information that is collected.



User name	User account	Devices used	Total application co...	OS Used	Multi user Windows...	Persona	Target Azure VM size	Is ready for migrati...	Target location	Target
User3	FAREAST\user3	UserVM-3.domain.org	4	Windows 10	No	Persona3	Standard_F2s_v2	Yes	West Central US	Standa
User11	FAREAST\user11	UserVM-11.domain...	4	Windows 10	No	Persona11	Standard_F2s_v2	Yes	West Central US	Standa
User10	FAREAST\user10	UserVM-10.domain...	4	Windows 10	No	Persona10	Standard_F2s_v2	Yes	West Central US	Standa
User1	FAREAST\user1	UserVM-1.domain.org	4	Windows 10	Yes	Persona1	Standard_F2s_v2	Yes	West Central US	Standa
User2	FAREAST\user2	UserVM-2.domain.org	4	Windows 10	No	Persona2	Standard_F2s_v2	Yes	West Central US	Standa
User14	FAREAST\user14	UserVM-14.domain...	4	Windows 10	Yes	Persona14	Standard_F2s_v2	Yes	West Central US	Standa
User4	FAREAST\user4	UserVM-4.domain.org	4	Windows 10	No	Persona4	Standard_F2s_v2	Yes	West Central US	Standa
User6	FAREAST\user6	UserVM-6.domain.org	4	Windows 7	No	Persona6	Standard_F2s_v2	Yes	West Central US	Standa
User13	FAREAST\user13	UserVM-13.domain...	4	Windows 7	No	Persona13	Standard_F2s_v2	Yes	West Central US	Standa
User5	FAREAST\user5	UserVM-5.domain.org	4	Windows 10	No	Persona5	Standard_F2s_v2	Yes	West Central US	Standa
User12	FAREAST\user12	UserVM-12.domain...	4	Windows 10	No	Persona12	Standard_F2s_v2	Yes	West Central US	Standa
User17	FAREAST\user17	UserVM-17.domain...	4	Windows 10	No	Persona17	Standard_F2s_v2	Yes	West Central US	Standa
User9	FAREAST\user9	UserVM-9.domain.org	4	Windows 10	No	Persona9	Standard_F2s_v2	Yes	West Central US	Standa
User28	FAREAST\user28	UserVM-28.domain...	4	Windows 10	Yes	Persona28	Standard_F2s_v2	Yes	West Central US	Standa
User7	FAREAST\user7	UserVM-7.domain.org	4	Windows 10	Yes	Persona7	Standard_F2s_v2	Yes	West Central US	Standa
User20	FAREAST\user20	UserVM-20.domain...	4	Windows 7	No	Persona20	Standard_F2s_v2	Yes	West Central US	Standa
User18	FAREAST\user18	UserVM-18.domain...	4	Windows 10	No	Persona18	Standard_F2s_v2	Yes	West Central US	Standa
User15	FAREAST\user15	UserVM-15.domain...	4	Windows 10	Yes	Persona15	Standard_F2s_v2	Yes	West Central US	Standa

Figure 6: The review assessment data

This includes information such as the following:

- The number of users in each persona
- Applications in use by users
- Resource consumption by a user
- Resource utilization averages by user persona
- VDI server performance data
- Concurrent user reports
- Top software packages in use

Detailed steps regarding the assessment can be found [here](#).

Depending on the results you analyzed as part of the assessment and considering the benefits, such as using Windows 10 multi-session, you can choose the operating system image you will deploy using Horizon Cloud on Azure. This could mean continuing to use Windows Server, Windows 10 Enterprise, or Windows 10 multi-session post deployment.

## Recommended next steps:

The typical approach for most organizations would be to create a new template image based on Windows 10 multi-session to use all the operating system benefits. To create a put this in one line, Windows 10 Enterprise multi-session is available in the Azure image gallery. To create a template image using Horizon Cloud on Azure, consult [this guide](#).

For a complete step-by-step guide on preparing, creating, and deploying custom template images for Horizon Cloud on Azure, consult [this guide](#).

**Important:** *Once uploaded to Azure, you need to import your custom template into Horizon Cloud on Azure, and you need to ensure that the Horizon agent is installed.*

Now that you've assessed your environment, you can proceed with preparing for Horizon Cloud with Azure Virtual Desktop. In this step, you deploy the required components for Horizon Cloud on Azure to your Azure subscription.

# Preparing for your VMware Horizon Cloud environment with Azure Virtual Desktop

In the previous chapter, we looked at the preparation steps for the migration to Horizon Cloud on Azure and the associated requirements for assessing your environment's current state. The following section discusses the requirements, including licensing and infrastructure, before you start migrating to Horizon Cloud on Azure with Azure Virtual Desktop.

## Azure Virtual Desktop prerequisites

Let's look at the three key areas of Microsoft Azure before deploying Horizon Cloud on Azure with Azure Virtual Desktop.

Depending on the operating system you select, appropriate licenses for users connecting to the desktops and applications are also required. Ensure that all users who are allowed access to any Horizon Cloud resource on Microsoft Azure have the required licensing. Table 1 shows the required licenses per operating system. You can read more about the licenses required [here](#).

Operating system	Required license
Windows Server 2012 R2, 2016, 2019	RDS Client Access Licence (CAL) with Software Assurance
Windows 7 Enterprise	Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows 10 Enterprise multi-session or Windows 10 Enterprise	Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5

Table 1: The different operating system versions and required MS licensing

Furthermore, your core infrastructure needs the following to be able to support a Horizon Cloud on Azure deployment:

- An Azure AD instance needs to be in place.
- A Windows Server AD instance that is in sync with Azure AD. You can choose to implement this based on Azure AD Connect (ideal for hybrid organizations) or based on Azure AD Domain Services (ideal for hybrid or cloud organizations). In terms of identifying sources and domain membership of the Horizon Cloud session desktops/ host servers, you can select from the following options:
  - You can use Windows Server AD in sync with Azure AD and the user accounts are sourced from Windows Server AD. The Virtual Desktop/session host VM is joined to the Windows Server AD domain.
  - You can use Windows Server AD in sync with Azure AD and the user accounts are sourced from Windows Server AD. The Virtual Desktop/session host VM is joined to Azure AD Domain Services.
  - An Azure subscription is required, which needs to be parented to the same Azure AD tenant that contains the virtual network. The virtual network needs to have access to the Windows Server AD or Azure AD Domain Services instance.

The user connecting to Horizon Cloud on Azure must also meet the following requirements:

- The Virtual Desktop/session host VMs you create as part of your pod must be [Standard domain-joined](#) or [Hybrid AD-joined](#). At the time of writing, VMs cannot be Azure AD-joined only. You must be running one of the following supported operating systems:
  - Windows 10 Enterprise multi-session, version 1809 or later
  - Windows 10 Enterprise, version 1809 or later
  - Windows 7 Enterprise
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2

Azure Virtual Desktop does not support x86 (32-bit), Windows 10 Enterprise N, or Windows 10 Enterprise KN operating system images. Windows 7 also does not support any **virtual hard disk (VHD)** or VHDX-based profile solutions hosted on managed Azure Storage. The available automation and deployment options depend on which operating system and version you choose, as outlined in this article on [supported operating systems](#).

## Considerations

Before getting started, there are a couple of key elements to consider. These are detailed as follows.

### Limitations

When deploying Azure Virtual Desktop, you need to be aware of a couple of technical limitations. Consider and review these limitations before deploying Azure Virtual Desktop in your environment. An up-to-date list of these limitations can be found [here](#).

For more information on supported operating systems with Horizon Cloud on Azure, check [here](#).

### Naming conventions

With an Azure subscription, it is crucial to have a reliable naming convention. The following list contains considerations regarding naming conventions:

- A useful naming convention assembles resource names using important resource information as part of a resource's name. When you construct your naming convention, identify the critical pieces of information you want to reflect in a resource name.
- Each workload can consist of many unique resources and services. Incorporating resource type prefixes into your resource names makes it easier to identify application or service components visually.
- When you apply metadata tags to your cloud resources, you can include information about those assets that couldn't be included in the resource name. If you do not have an existing naming convention for your subscription, please follow the guidance at this [link](#) to maintain a consistent naming convention across your resources.

The following section discusses the prerequisites and considerations that it is important to become familiar with before creating your Horizon Cloud environment. The next section elaborates on deployment options and guides you through the overall deployment process.



## VMware Horizon Cloud on Azure prerequisites

This section summarizes the key requirements needed to deploy Horizon Cloud on Microsoft Azure. The requirement is split into two sections, the first being "**Requirements for pod deployment**" and the second "**Requirements for a productive environment after pod deployment**."

Figure 7 illustrates the internal components of the Horizon Cloud Pod. Please note that the following diagram only shows an external-facing Unified Access Gateway:

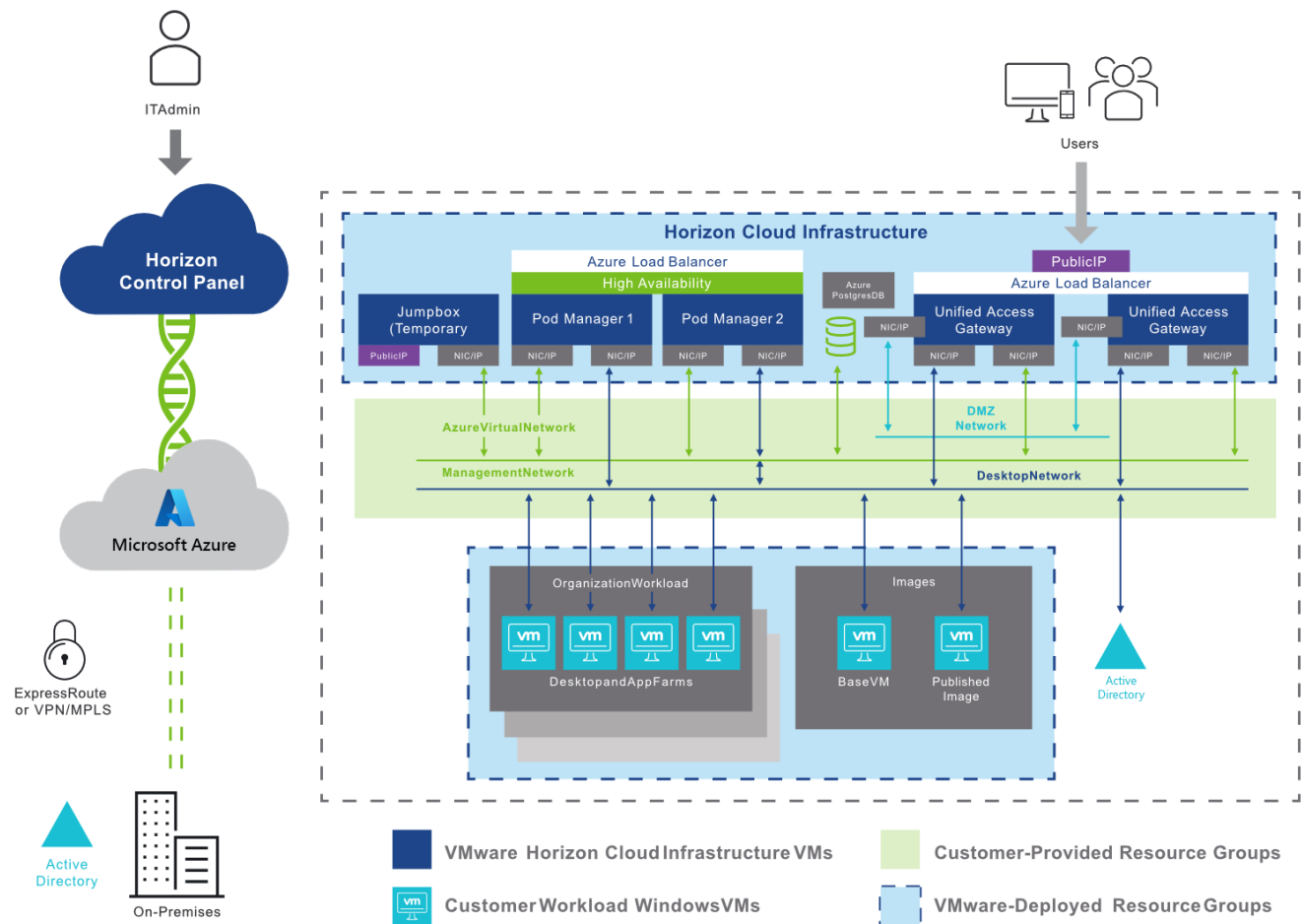


Figure 7: The internal components of the Horizon Cloud Pod



## Requirements for pod deployment

These requirements are specified for pod deployment, detailing the control plane requirements, Microsoft Azure, and network communication:

- [Horizon Control Plane Requirements](#)
- [Microsoft Azure Subscription Requirements](#)
- [Network Requirements](#)
- [Ports and Protocols Requirements](#)
- [Pod Deployment Workflow](#)

## Requirements for a productive environment after pod deployment

The following requirements relate to post pod deployment, including Active Directory, universal broker, images, desktops, and farms:

- [Active Directory Requirements](#)
- [Universal Broker Requirements](#)
- [DNS Record Requirements](#)
- [Horizon Cloud Golden Images, Desktops, and Farms](#)
- [Licensing for the Microsoft Windows Operating Systems](#)

Each requirement is linked to the VMware requirements checklist; you can find it [here](#). For onboarding information, please refer to this [document](#).

This [quickstart guide](#) outlines what you need to configure in Microsoft Azure before you progress with the next steps.

## Selecting an operating system image

Suppose you have an on-premises session-based VDI deployment today that you want to migrate to Horizon Cloud on Azure. You may also use the Windows Server version as your desktop operating system for the pooled Session desktops. This is because Windows 10 multi-session is not supported outside of Microsoft Azure.

It's important to note that Windows Server 2012 R2 and any later version is supported in Horizon Cloud on Azure and Azure Virtual Desktop.

However, for multiple reasons, as outlined in the *Introduction*, leveraging Windows 10 multi-session provides several additional benefits, including a cost saving, as the traditional RDS CALs are no longer required. To fully optimize Azure Virtual Desktop and the Azure cloud, we advise rebuilding your images to Windows 10 multi-session.

This [article](#) provides guidance on preparing a custom master image **virtual hard disk (VHD)** to upload to Azure. Custom images can be created offline, giving you the ability to customize a template to your organization's requirements before uploading the final template to Azure. You can create custom images for all supported versions of the Windows Server and client operating system, including Windows 10 multi-session.

For more information on creating images with Horizon Cloud on Azure, please refer to this [link](#).

## Profile management guidelines

VMware has been providing VDI technology for well over a decade. As the product portfolio has matured, and as companies continue to adopt these technologies for new and innovative uses, a number of desktop and application models have emerged. [Managing User Experience with VMware Horizon](#) illustrates several commonly used models and is meant to help you determine the best model or models needed for your business's requirements.

Some of these models can be built using legacy Horizon technologies such as View Composer and Persona Management. You can use the preferred modern alternatives, such as Dynamic Environment Manager.

- [VMware Dynamic Environment Manager™](#) (DEM) persists user configuration data across virtual, physical, and cloud PCs. Like Persona Management, DEM persists user configuration data between sessions while adding numerous capabilities, from drive and printer mappings to privilege elevation to integration with Horizon through Smart Policies. DEM relies on folder redirection or alternatives such as FSLogix Office Containers or App Volumes user-writable volumes to abstract and persist user data between user sessions. You can read more on [Modernizing VDI for a New Horizon](#) and [Integrating FSLogix Profile Containers with VMware Horizon](#).

## Conditional access

In most production environments, we advise configuring conditional access for Horizon Cloud on Azure. This allows you to define additional security requirements that a user's session needs to meet before accessing the published desktops and applications.

A typical conditional access example is Azure MFA. After configuring Azure MFA, when a user signs in, the client asks for your username and password, followed by an Azure MFA prompt. When you select **Remember me**, your users can sign in after restarting the client without needing to re-enter their credentials. These credentials are stored on the local credentials manager. While remembering credentials is convenient, it can also make deployments for Enterprise scenarios or personal devices less secure. To protect your users, you'll need to make sure the client always asks for Azure MFA credentials.

The following two steps enable SSO integration and conditional access for Horizon Cloud on Azure:

- **Step 1.** More information on setting up and configuring Azure MFA for Horizon Cloud on Azure is provided [here](#). You can also use [Universal Broker to provide MFA](#) with RADIUS and RSA directly.
- **Step 2.** For single sign-on and how to configure your IDP to work with cloud App security, take a look [here](#).

## Dynamic Environment Manager

The inclusion of FSLogix in Azure Virtual Desktop solves many problems related to profile management. Horizon Cloud on Azure integrates with the FSLogix features, either building on top or providing users with alternatives. For example, VMware Dynamic Environment Manager™ (formerly User Environment Manager) can add user environment management features to FSLogix Profile or Office 365 Container. Read more [here](#).

Figure 8 shows Horizon Cloud on Azure with an FSLogix profile container:

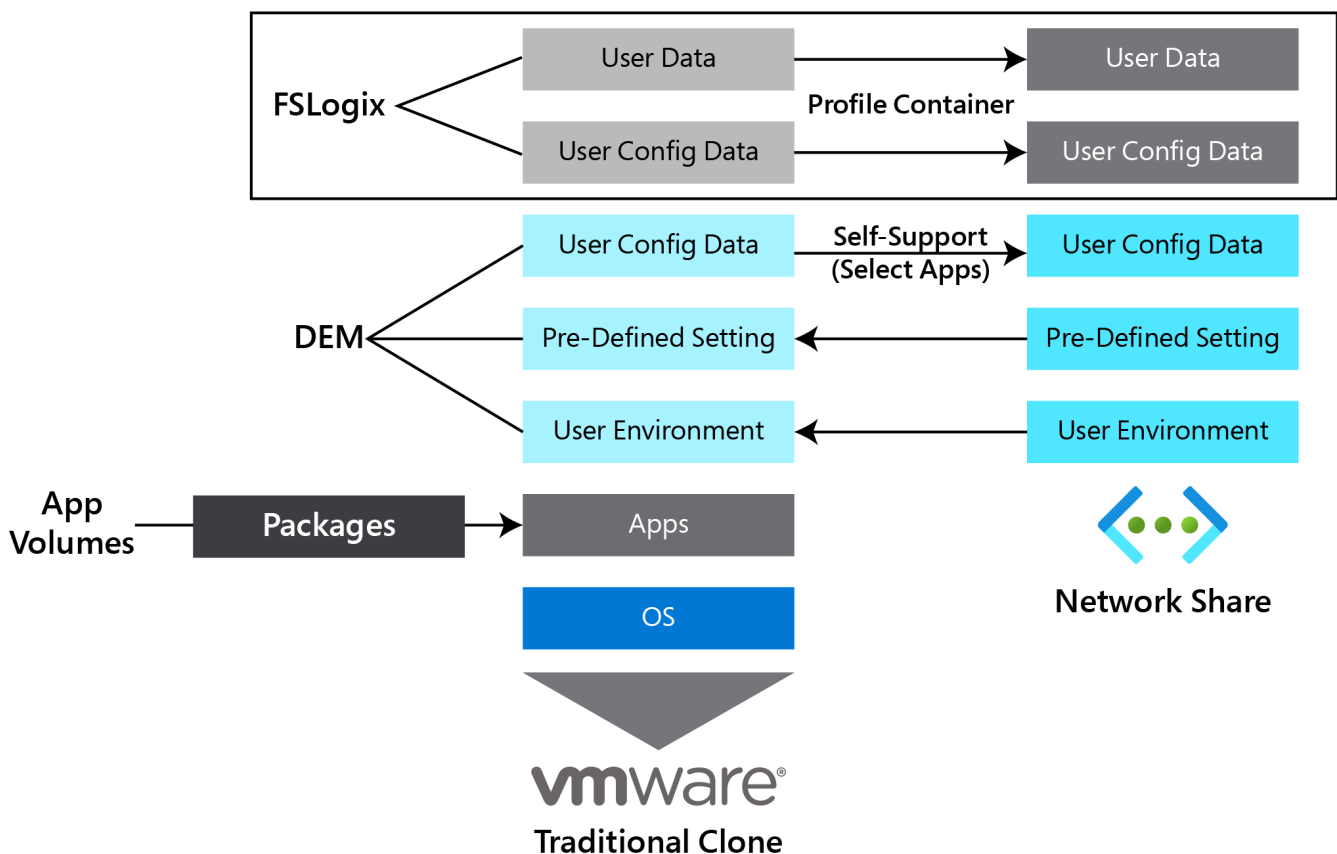


Figure 8: Horizon Cloud on Azure with an FSLogix profile container

In this section, we covered the prerequisites for getting started with Horizon Cloud on Azure with Azure Virtual Desktop. This included profile guidelines, conditional access, and dynamic environment manager.

Next, we'll look at setting up your first Horizon Cloud service pod with Azure Virtual Desktop so that you can start migrating workloads.

# Creating your first Horizon Cloud Service pod with Azure Virtual Desktop

The following steps provide a high-level description of the process for deploying a Horizon Cloud tenant environment. Before we can start deploying a pod, you need to make sure you have met all the requirements as set out in the previous section, VMware Horizon Cloud on Azure prerequisites. This [link](#) details things you need to know before and during the use of Horizon Cloud.

*Table 2* details the high-level steps required to deploy your first pod and configure Horizon Cloud on Azure. Please note that this section provides guidance for *step 1*. You can review all the steps in detail at this [link](#).

Step	Description
1. Capacity	Deploy your first pod.
2. General setup	Configure VMware accounts, Active Directory, Roles and permissions, broker, and the Cloud Monitoring Service.
3. Desktop assignment	Import a VM, create an image, create a new desktop assignment.
4. Application assignment	Create a VM image, application farm, and an application inventory.

Table 2: High-level steps for deploying your first pod and configuring Horizon Cloud on Azure

## Deployment of Horizon Cloud Pod with Azure Virtual Desktop

In this section, we'll look at the deployment of Horizon Cloud with Azure Virtual Desktop. The deployment is where we create the Horizon pod in preparation to migrate from on-premises to Horizon Cloud with Azure Virtual Desktop. We will then progress to the testing of the deployment and cost optimization.

The first step is to add a pod to Microsoft Azure through the VMware Horizon Cloud portal. For an in-depth overview of actions before adding a pod, refer to the [Horizon Service Overview](#) documentation.

### Adding Microsoft Azure Capacity

Figure 9 shows the login page for your Horizon Cloud Tenant:

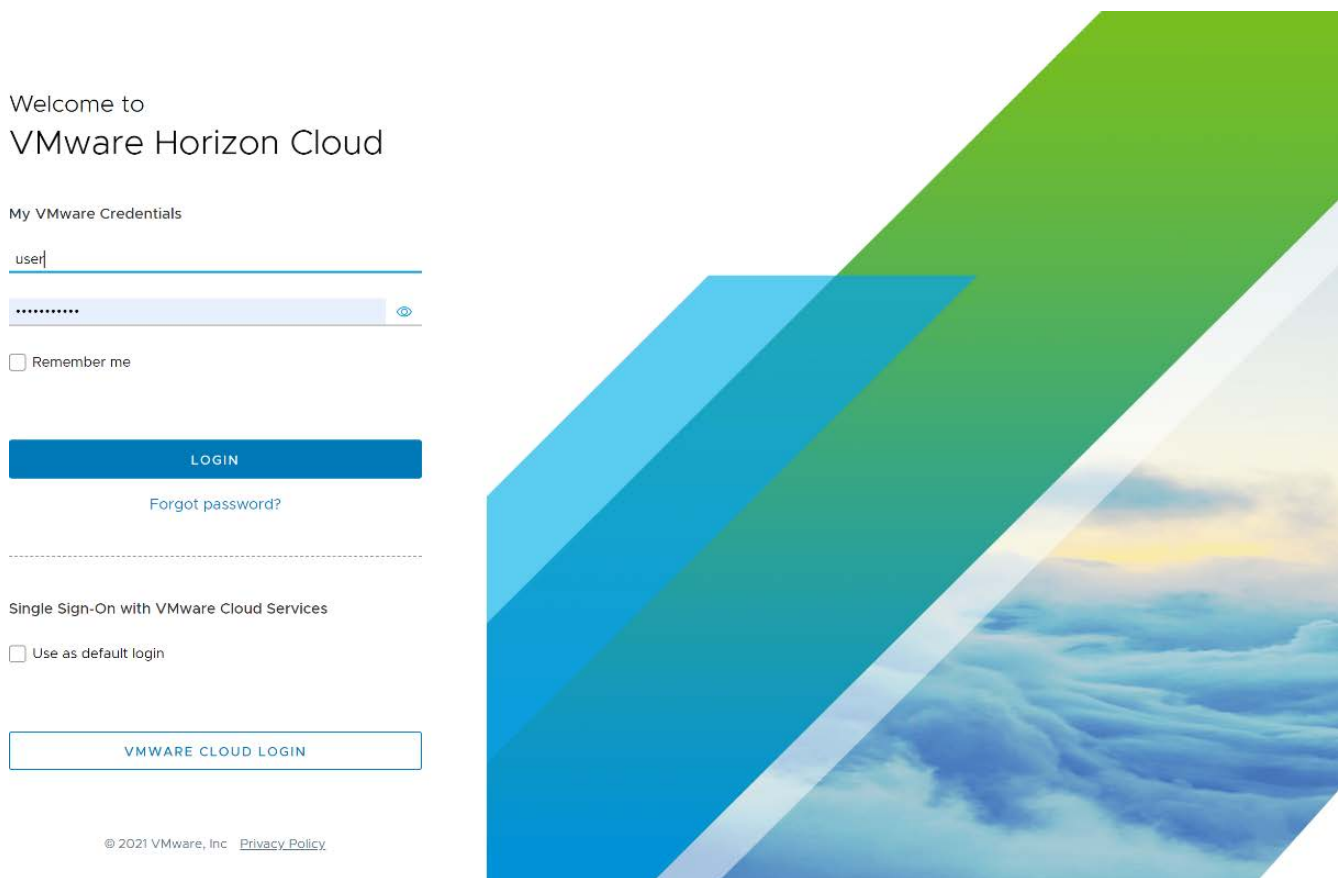


Figure 9: The login page for Horizon Cloud Tenant

Go to the [login page](#) of VMware Horizon Cloud. Once logged in, you will be presented with the **Getting Started** screen, with four tabs labeled **Capacity**, **General Setup**, **Desktop assignment**, and **Application Assignment**. Under the first tab, **Capacity**, click the **MANAGE** box and select **Add Pod**:

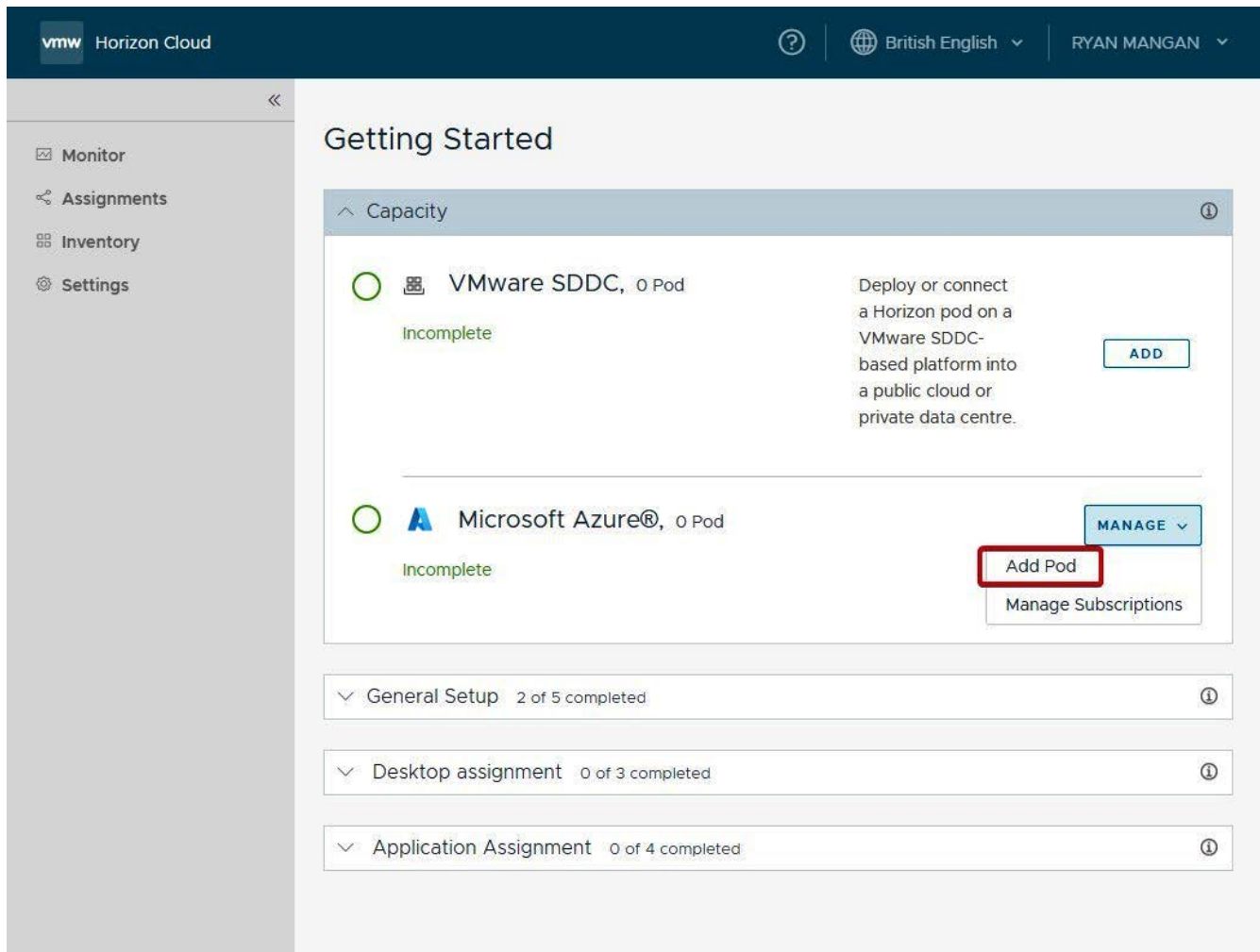


Figure 10: Adding a pod

After you have clicked **Add Pod** from the drop-down menu, you will then be presented with the **Pod Subscription** web form, as shown in *Figure 11*. For more information on this section, please refer to [this documentation](#):

vmware Horizon Cloud

British English

RYAN MANGAN

## Add Microsoft Azure Capacity

Choose the Microsoft Azure subscription you want to apply or add a new one.

### Pod Subscription

**1. Subscription**

2. Pod Setup

3. Gateway Settings

4. Summary

**Apply Subscription:** Add New ⓘ

**Subscription Name:** ⓘ

**Environment:** Azure - Commercial ⓘ

**Subscription ID:** ⓘ

**Directory ID:** ⓘ

**Application ID:** ⓘ

This field is required.

**Application Key:** ⓘ

Use a Different Subscription for External Gateway: ☐ ⓘ

CANCEL ADD

Figure 11: The Pod Subscription form



Complete the web form with the required Microsoft Azure tenant information, as detailed in the *Prerequisites* section. For more information on the pod subscription, visit [this page](#):

vmw Horizon Cloud

?

British English

RYAN MANGAN

Add Microsoft Azure Capacity

1. Subscription

2. Pod Setup

3. Gateway Settings

4. Summary

Enter details to configure and connect the pod.

Details

Pod Name:

rm-vmware-test

?

Location:

London, United Kingdom

?

Edit

Microsoft Azure Region:

UK South

?

Description:

Azure Resource Tags:

Name

Value

+

?

High Availability

Enabled:

☐

?

Networking

Virtual Network:

WVD\_test01 [Test01\_vNet]

?

Use Existing Subnet:

☐

?

Management Subnet (CIDR):

10.0.6.0/24

?

(256 addresses)

VM Subnet (CIDR) - Primary:

10.0.5.0/24

?

(256 addresses)

NTP Servers:

8.8.8.8

?

Use Proxy:

☐

?

CANCEL

BACK

NEXT

Broker

Set up the broker to enable

Figure 12: Configuring and connecting the pod

After you navigate to the **Pod Setup** tab, complete the **Pod Name**, **Location**, **Microsoft Azure Region**, and **Networking** fields. More information on this section can be found [here](#):

vmw Horizon Cloud
British English
RYAN MANGAN

Add Microsoft Azure Capacity

1. Subscription  
2. Pod Setup  
3. Gateway Settings  
4. Summary

Set up external and internal Unified Access Gateways for this pod.

### External Gateway

Enable External Gateway? ☒ ⓘ

FQDN:\* test.vmware.ryanmangansitblog.com ⓘ

DNS Addresses: ⓘ

Routes: ⓘ

VM Model: \* Standard\_A4\_v2 (4 CPUs, 8 GiB Me... ⓘ

Certificate:\* 123.cer Change ⓘ ☒

### Load Balancer

Enable Public IP? ☒ ⓘ

### Networking

Use a Different Virtual Network: ☐ ⓘ

DMZ Subnet (CIDR):\* 10.0.7.0/24 ⓘ (256 addresses)

### Two-Factor Authentication

Enable two-Factor Authentication? ☐ ⓘ

### Internal Gateway

Enable Internal Gateway? ☐ ⓘ

### Azure Resource Tags ⓘ

Inherit Pod Tags: ☒ ⓘ

CANCEL BACK VALIDATE & PROCEED

Broker
Set up the broker to enable

Figure 13: Setting up external and internal Unified Access Gateways

Complete the required gateway settings and select **VALIDATE & PROCEED**. Check your configuration and then, when you're happy, select **Submit**.

For more information on Horizon Cloud Pod's gateway configuration, check [this documentation](#).

You can also check [this resource](#) for more information on **Validate & Proceed**. If you encounter any issues, you can use [this guide](#) to troubleshoot.

Once the building process starts, you see the progress bar start to populate:

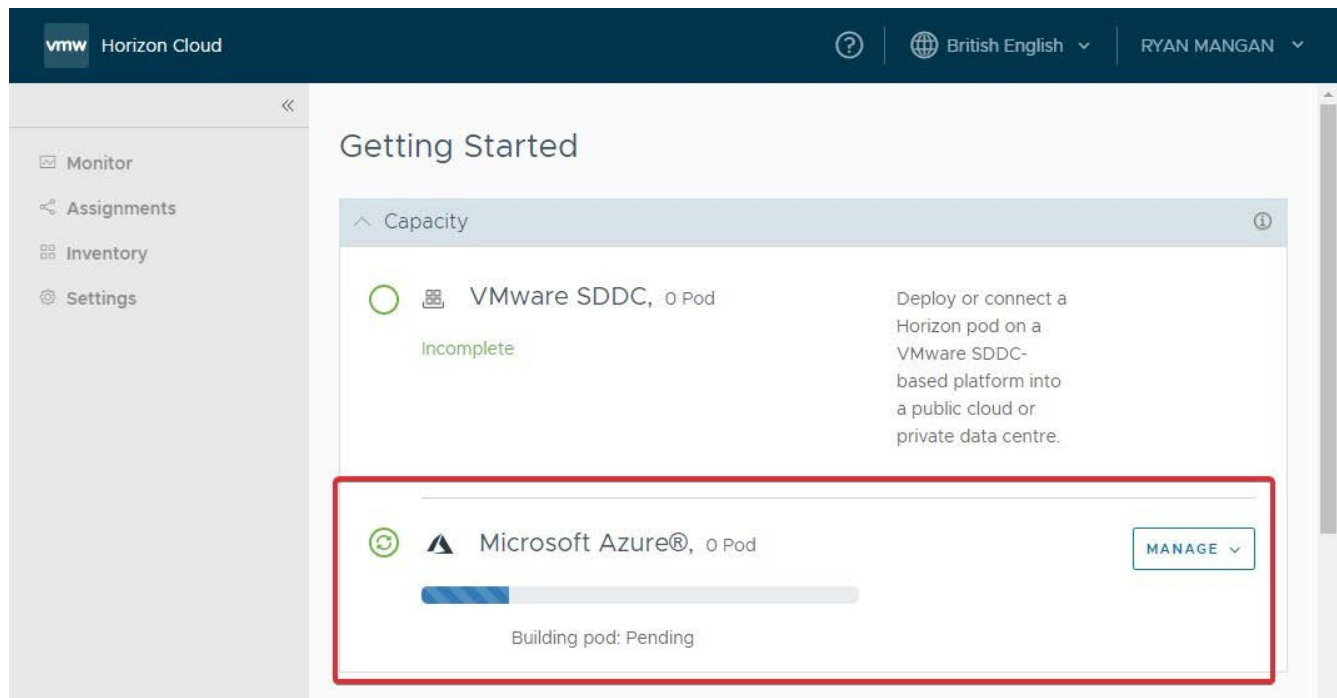


Figure 14: The pod building process in progress

**Note:** For guidance on steps 2 (General setup), 3 (Desktop assignment), and 4 (Application assignment), please refer to [this link](#).

In the next chapter, we'll examine and connect to your deployed Horizon Cloud environment.

# Post-deployment guidance

Once you have migrated to Horizon Cloud with Azure Virtual Desktop, you can then move on to the post-deployment stage. Here, we'll look at testing, cost optimization, and health monitoring.

## Testing the VMware Horizon deployment

Upon completing all of the pod deployment steps, you need to confirm your Horizon Cloud environment's health. Once you are happy, you can then proceed with testing the deployment.

For more information on Horizon Cloud's dashboard page, [click here](#).

You can access Horizon Cloud resources on Windows 7, Windows 10, and Windows 10 IoT Enterprise using the Windows Desktop client. Besides the Windows platform, you can also use Android, iOS, macOS, Chrome, and web clients. The following list contains links to the various clients and guides on installing, configuring, and using the client: [Download VMware Horizon Clients](#).

For a full list of supported VMware Horizon Clients, visit [this page](#).

Figure 15 shows an example of the VMware Horizon Client, which contains published desktops and applications:

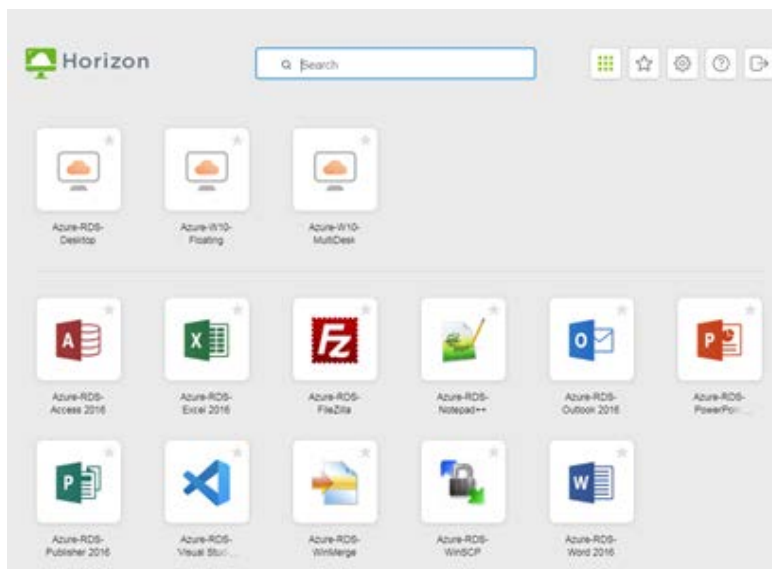


Figure 15: An example of the VMware Horizon Client

**Note:** To find out more about the VMware Horizon Client, please refer to this [link](#).

We can now take the advantage of the features offered by Horizon Cloud with Azure Virtual Desktop to optimize cost as well as monitor health and usage.

## Optimizing costs

To optimize costs and make full use of Horizon Cloud on Azure, there are a variety of considerations that will help you realize cost savings. The following list contains six ways to save costs on your Horizon Cloud on Azure deployment:

- **Make use of Windows 10 multi-session** as the operating system of your Horizon Cloud session host desktops. By leveraging a multi-session desktop experience for users with identical compute requirements, you can let more users sign in to a single VM at once. This results in considerable Azure consumption cost savings for the VMs that are running. If you want additional guidance, the Windows 10 Enterprise multi-session FAQ contains more detailed information.
- **Use Azure Hybrid Benefit.** If your organization has Microsoft Software Assurance, you can use Azure Hybrid Benefit for Windows Server to save on your Azure infrastructure cost. For more information, visit this [link](#).
- **Azure VM Reserved Instances (Azure RI)** can significantly reduce costs by up to about 72% compared to pay-as-you-go prices, with a one-year or three-year commitment on Windows and Linux VMs. With RIs, you prepay for your VM usage. Optimally, combine Azure RI with Azure Hybrid Benefit (as outlined previously) to save up to 80% on list prices. Read more about Azure RI [here](#).
- **Use [Power Management](#)** to reduce your total Horizon Cloud on Azure deployment cost by scaling your VMs using rules to shut down and deallocate session host VMs during off-peak usage hours. Then, turn them back on and reallocate them during peak hours. Read more on Horizon Cloud scaling [here](#).
- **VMware App Volumes** offers Azure consumption cost savings due to the reduced base image size and centralized management, including the integration of MSIX.

Once you have deployed and tested your Horizon Cloud environment, the final step is to monitor health and usage.

## VMware Horizon Cloud on Azure health and usage

During the preparation phase, we determined which VM sizes to use for the session host VMs and investigated the use of the environment by collecting telemetry data regarding the resources that are consumed.

Now that you have migrated to Horizon Cloud on Azure, you can investigate your environment's usage and health. The **Cloud Monitoring Service (CMS)** is one of the central services provided in Horizon Control Plane, providing you with the ability to monitor capacity, usage, and health within and across your cloud-connected pods:



Figure 16: Dashboard displaying the utilization of pods and global health

You can also use Azure Advisor to provide you with information about your Virtual Desktop environment and guide you to best practices you might have missed during your deployment. Closely investigate the recommendations that Azure Advisor contains and implement the suggested best practices shown there.

Figure 17 shows an example of Azure Advisor:

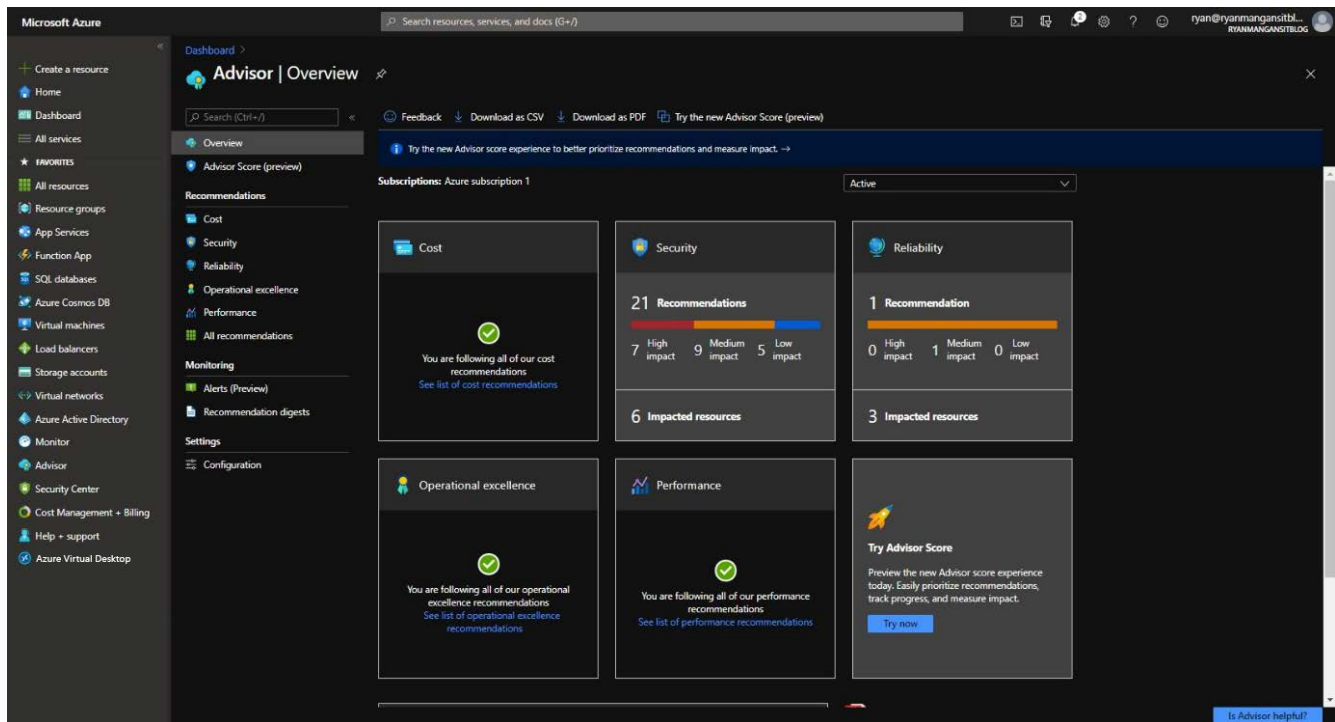


Figure 17: Azure Advisor

We'll now look at the environment clean-up tasks that may be required if you are planning to remove an old on-premises environment.

## Environment cleanup

Once you have successfully migrated your desktop virtualization deployment to Horizon Cloud on Azure, it is also advised to clean up your VDI deployment. It's important to thoroughly investigate, plan, and execute this clean-up to ensure that no components or configurations are left behind. There are a few key areas where clean-up of the VDI environment is advised:

- The VMs of your VDI deployment can be removed. The VMs running your VDI infrastructure roles, such as Connection Brokers, Web Access, and Gateways, are no longer required. The RD Session Host VMs have been migrated to Azure as part of the migration to Horizon Cloud on Azure and can also be removed. It might also be a good idea to snapshot/back up one of your RD Session Host servers in case you experience unexpected behavior with applications or settings inside the session host servers as part of Horizon Cloud on Azure at a later stage, and you want to compare settings with the previous VDI deployment.
- Your VDI deployment will have also used various DNS records, and most likely, these were created in public and private DNS services. DNS type A records were used for the previous VDI deployment.

These DNS records can now be safely removed as they are no longer required for Horizon Cloud on Azure.

- The infrastructure components of the VDI deployment, including the RD Session Host servers, are all members of your internal AD Domain Services. Since we have removed the infrastructure VMs, the corresponding AD computer objects, including their DNS entries, can also now be removed. Whether or not you can also remove the RD Session Host server computer object depends on how you migrated those workloads. If you migrated the VMs themselves, you are reusing those computer objects, and you should not remove them. If you migrated based on a new set of VMs in Azure, for example, as part of your move from Windows Server to Windows 10 multi-session, you are most likely also using new names and computer objects, which means you can remove the old objects.



## Guidance on additional capabilities

This chapter highlights some of the additional features and functions that can help improve the user experience when using Horizon Cloud with Azure Virtual Desktop.

### VMware App Volumes for Horizon Cloud on Azure

VMware App Volumes is deployed as a feature of the Horizon Cloud on Azure. With VMware App Volumes on Horizon Cloud, users gain the following benefits:

- It is no longer necessary to deploy and manage servers, databases, or storage for VMware App Volumes as this is auto-provisioned and managed by Horizon Cloud on Azure.
- Tools to migrate app packages from on-premises to the cloud without repackaging.
- Feature consistency between the on-premises and Horizon Cloud on Azure. App Volumes helps to facilitate a multi-cloud, hybrid cloud solution that works with your deployment no matter where you are in your digital transformation.

The screenshot displays the VMware App Volumes management console for a Notepad++ application. At the top, it shows the application name 'Notepad++', its status 'Success' with a green checkmark, location 'Reston, VA, United States', and pod 'R-RTM-1016'. Below this, the 'Packages' section is active, showing a table of published packages. The table has columns for Status, Package Name, Marker, and Stage. Three packages are listed, all with a status of 'Packaged'. The 'Current' marker for the 'Notepad++ v7' package is highlighted with a green box.

Status	Package Name	Marker	Stage
●	Notepad++ version 7.8.8	0	Packaged
●	Notepad++ version 7.8.7	0	Packaged
●	Notepad++ v7	Current	Packaged

Figure 18: Notepad++ published as a package in VMware App Volumes

We now look at cloud-native packaging and real-time application delivery using Azure files.

## Cloud-native packaging

You can build packages using all the resources, such as desktops and images, available within Horizon Cloud on Azure. There is no need for command-line tools to build app packages on local machines and then upload them to the cloud. This is taken care of through the graphic interface.

## Real-time application delivery via Azure file shares

VMware App Volumes takes advantage of Microsoft Azure storage to manage and deliver app packages to virtual desktop users. Azure storage is auto-provisioned for the customer during setup. No upfront storage costs are involved. As you build packages and deliver them via Azure file shares, the storage usage is directly billed based on consumption. Inside Azure, applications are packaged and delivered in Microsoft's native VHD format for optimal Azure performance.

## User interface seamlessly integrated into the Horizon Control Plane

The VMware App Volumes user interface integrates into Horizon Cloud's management console seamlessly. By moving it into the Horizon Control Plane, App Volumes is now well-positioned to manage deployments, app inventory, and assignments across clouds and on-premises, and will soon deliver a real multi-cloud, hybrid-cloud solution.

In the next section, we take a look at media optimization redirection for Microsoft Teams using Horizon Cloud on Azure.

## Microsoft Teams

VMware supports media optimization redirection for Horizon Cloud on Azure.

Making video calls from a virtual desktop has been a consistent challenge. VMware and Microsoft have worked closely together to release media optimizations for Microsoft Teams. This feature allows the endpoint (physical device) to start a call rather than the traditional virtual desktop method. This improves performance as the Horizon agent circumvents the need to pass all Microsoft Teams audio and video traffic through the Virtual desktop. This resolves the previous challenges experienced by virtual desktop users where performance was impacted, and now, with media optimization, this reduces resource consumption as Microsoft Teams audio and video connections are offloaded to the endpoint. Read more [here](#).

Figure 19 shows the Microsoft Teams optimization flow detailing how audio and video is offloaded to the endpoint client:

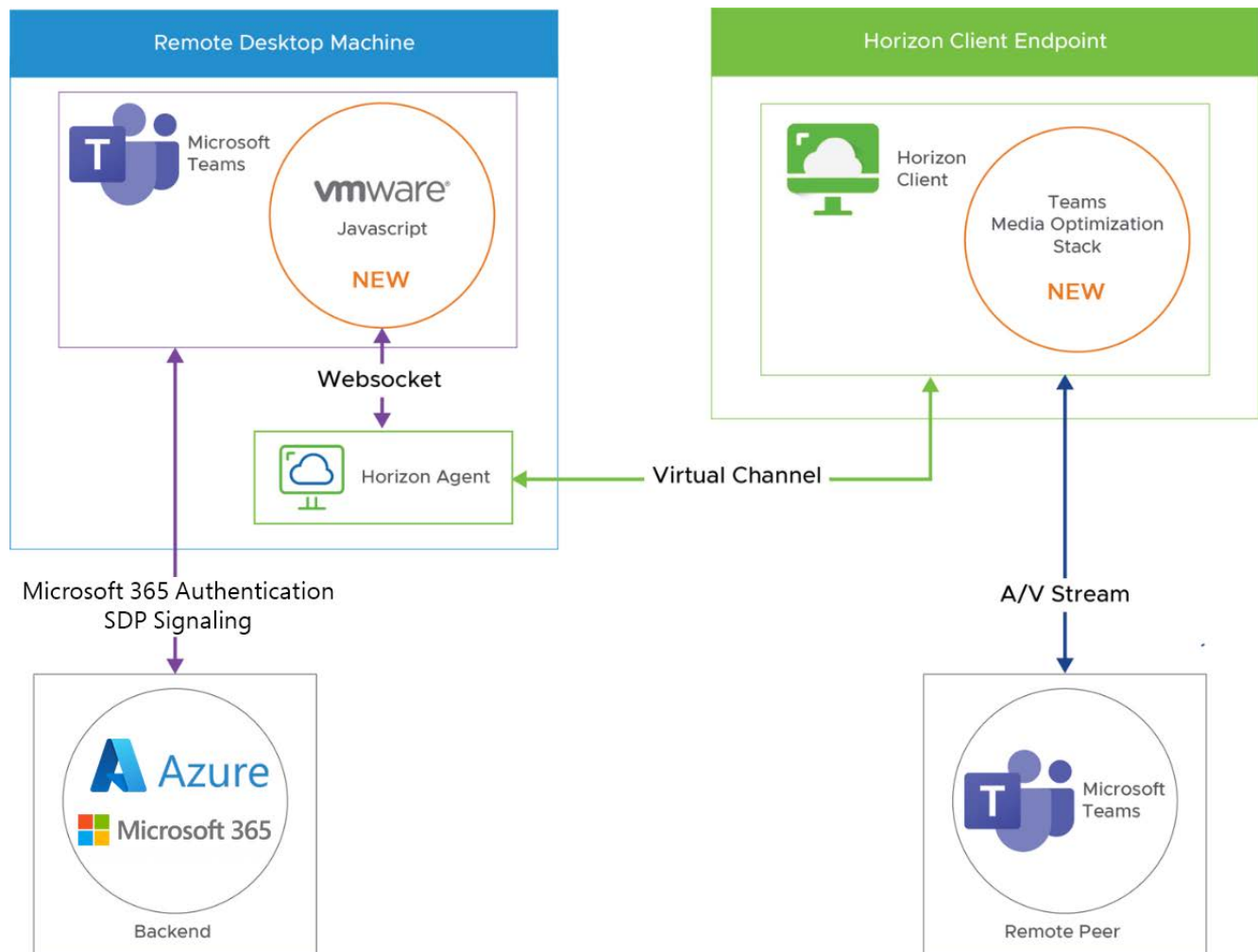


Figure 19: Microsoft Teams optimization flow

For more information on Microsoft Teams optimization with VMware Horizon, [check this documentation](#).

## Power management

Power management configurations control how a VM behaves when the associated desktop or server is not in use. A desktop is considered not in use both before a user logs in and after a user disconnects or logs off. A farm server or host is considered not in use when the last user session is ended from that host. Power policies also control how a VM behaves after completing administrative tasks, such as refresh, recompose, farm expansion, and farm refresh.

Horizon Cloud on Azure has several methods for controlling the IaaS costs of your Horizon Cloud on Azure environment. Most of these methods are included in the sizing components of the VDI user assignment configurations or RDSH/Windows 10 multi-session farm configurations. By using these sizing components, you can implement a cost-effective deployment of Horizon Cloud on Azure. At the same time, ensure that resources are available to your users when they need them.

Figure 20 shows a power management schedule being configured:

Add Power Management Schedule - Quantum-Beta-0608-1 ×

Min Desktops	Day(s)	Start	End		Timezone
1	M T W TH F SA SU	08:00	17:30	<input type="checkbox"/> All Day	America/Chicago (UTC-0... <span>×</span>
1	M T W TH F SA SU	09:00	15:00	<input type="checkbox"/> All Day	America/Chicago (UTC-0... <span>×</span>
0	All Other Times				

ADD SCHEDULE

CANCEL SAVE

Figure 20: Configuring a power management schedule

You can also configure power management for VMs used for VDI capacity in a desktop assignment for your users, and you can configure power management features when you create or edit RDSH server or Windows 10 multi-session farm configurations in the Horizon Control Plane.

For more information on Horizon Cloud's Power Management feature, click [here](#).

## Monitoring and analytics

The **Cloud Monitoring Service (CMS)** allows you to monitor capacity, usage, and health within and across your fleet of cloud-connected Horizon pods, regardless of the deployment environments in which those individual pods reside. The CMS works if the pod is cloud-connected, regardless of the underlying infrastructure components that Horizon is running on.

The Help Desk service is a component of the CMS. Help Desk allows you to monitor and troubleshoot live user sessions on any Horizon pod. Help Desk provides support staff with detailed information on each user's session, including metrics such as CPU usage, memory usage, network latency, and disk performance.

The CMS includes dashboards, activity monitoring, and reporting features with the following benefits:

- Real-time monitoring: Provides alerts for common desktop and server issues. Desktops and application servers are monitored in real time.
- Contextual metrics: Generates in-depth information about user experience and resource usage. We use contextual metrics to give you details regarding user experience and resource utilization.
- Historical utilization: Provides the ability to visualize usage with a perspective on capacity, concurrency, and uniqueness. The system enables you to go back in time to visually evaluate differences in how your deployment consumes resources.
- Endpoint landscape: Facilitates an understanding of 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.

Figure 21 shows the Horizon CMS dashboard, highlighting several sessions in a specific Azure region:



Figure 21: VMware Horizon CMS dashboard

You can read about Horizon Cloud's monitoring capabilities [here](#).

## Conclusion and resources

With the importance of the migration decision and the need to enable flexible and secure remote work for a hybrid workspace, it's key to have an understanding of the migration process to design a successful plan.

This handbook highlighted some of the key benefits of migrating your VDI to VMware Horizon Cloud with Azure Virtual Desktop. To prepare for your migration, you need to first assess your existing environment and ready the VMware Horizon Cloud environment with Azure Virtual Desktop. The guidance shared on Windows 10 multi-session, profile management, conditional access, and environment management will be useful as you move through the preparation phase.

Once you are prepared, you can deploy a Horizon Cloud tenant environment and deploy your first pod. After you have completed the deployment stage, you need to test the deployment and the VMware environment, and the best practices shared in the Deployment section can help guide you here.

The final stages are post-deployment and optimization, and here we covered a number of additional capabilities, including Microsoft Teams, VMware App Volumes, power management, and monitoring and analytics.

There are additional resources available to help along the way listed in the next section. You can get started with an [Azure free account](#) or get in touch with an [Azure sales specialist](#) to get advice and guidance on how to quickly deploy and scale Azure Virtual Desktop.

## Further reading

There are a lot of other resources and support to help. Here are a few key references:

- [Learn more](#) about VMware Horizon Cloud service and Azure Virtual Desktop.
- [Explore](#) Horizon Cloud service documentation for additional deployment guidance.
- [Download](#) the free Total Economic Impact™ of Microsoft Azure Virtual Desktop to get a detailed analysis of the return on investment and other outcomes experienced by real customers who migrated.
- [Sign up](#) for a free Azure account to try deploying your virtualized Windows desktops and apps.
- [Join](#) the Azure Migration and Modernization Program to get guidance and expert help.

## We're here to help

Learn more about how to migrate your VDI to Azure Virtual Desktop by connecting with an Azure sales specialist.

**Get in touch**

If required, use the following resources for more in-depth information on specific topics mentioned in this guide:

[Azure Reserved VM Instances \(RIs\)](#)

[Azure Virtual Desktop partner integrations](#)

[Windows 10 Computer Specifications and Systems Requirements](#)

[Remote Desktop Services – GPU acceleration](#)

[GPU optimized virtual machine sizes](#)

[Virtual Machine series](#)

[Prepare and customize a master VHD image](#)

[FSLogix Migration Preview Module](#)

[Azure Virtual Desktop pricing](#)

[Supported virtual machine OS images](#)

[Safe URL list](#)

[Windows 10 Enterprise multi-session FAQ](#)

[Host pool load-balancing methods](#)

[Recommended naming and tagging conventions](#)

[What are ARM templates?](#)

[RDS/Azure Virtual Desktop ARM templates](#)

[Business Continuity with VMware Horizon](#)

[Horizon Cloud on Microsoft Azure learning path](#)

[Horizon Cloud on Microsoft Azure Architecture](#)

[Horizon Cloud/Horizon Universal free trial](#)



# Glossary

Whether you are new to desktop virtualization or an expert in the field, there may be some terms you are not familiar with. The following are key terms introduced by Azure Virtual Desktop and Horizon Cloud on Azure.

Term	Description
<b>Active Directory Domain Services</b>	A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators
<b>Azure Active Directory (Azure AD)</b>	Azure AD is Microsoft's cloud-based identity and access management service that helps your employees to sign in and access resources.
<b>Azure Virtual Desktop</b>	A desktop and app virtualization service that runs on Microsoft Azure.
<b>Cloud Monitoring Service (CMS)</b>	Stores session, application, and desktop data from cloud-connected pods for monitoring and reporting purposes.
<b>Dynamic Environment Manager</b>	This is the concept of managing a user's persona across devices and locations. IT centrally manages policies where, regardless of how delivery is performed, end users can access their desktops and applications with personalized and consistent settings across devices.
<b>FSLogix</b>	FSLogix is designed to roam profiles in remote computing environments, such as Azure Virtual Desktop. It stores a complete user profile in a single container.
<b>FSLogix Host pool</b>	A host pool is a collection of Azure VMs that are registered to Azure Virtual Desktop.

Term	Description
<b>Horizon Cloud Pod</b>	A collection of resources/components deployed to Microsoft Azure to use Horizon Cloud with that specific Azure region.
<b>Power management</b>	Configurations control how a VM behaves when the associated desktop or server is <i>not in use</i> .
<b>RDS</b>	Remote Desktop Services is the IaaS platform building virtualization solutions.
<b>VMware App Volumes</b>	This is a real-time application delivery system that enterprises can use to dynamically deliver and manage applications.
<b>VMware Horizon Cloud Service on Microsoft Azure</b>	This delivers feature-rich virtual desktops and apps using a purpose-built <i>cloud</i> platform that is scalable across multiple deployment options.
<b>Windows 10 multi-session</b>	Windows 10 Enterprise multi-session, formerly known as Windows 10 Enterprise for Virtual Desktops (EVD), is a new Remote Desktop Session Host that allows multiple concurrent interactive sessions.

# About the author

Ryan Mangan is an end user computing (EUC) specialist. A speaker and presenter, he has helped customers and technical communities with EUC solutions—ranging from small to global (30,000+) user enterprise deployments—in various fields.

Ryan is the owner and author of [ryanmangansitblog.com](https://ryanmangansitblog.com), which has over 3 million visitors and over 70 articles on Remote Desktop Services and Azure Virtual Desktop. Some of Ryan's community and technical awards include the following:

- Author of:
  - *Quickstart Guide to Azure Virtual Desktop*
  - *An Introduction to MSIX App Attach*
- VMware vExpert for eight consecutive years
- VMware vExpert EUC 2021
- Parallels RAS VIPP – three consecutive years
- LoginVSI Technology Advocate – consecutive years
- Technical person of the year – 2017 KEMP Technologies
- Parallels RAS EMEA Technical Champion 2018
- Microsoft Community Speaker
- Top 50 IT Blogs 2020 – Feed spot
- Top 50 Azure Blogs 2020 – Feed spot