

Windows Desktops and Applications in Horizon

VMware Horizon 2209

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

<https://docs.vmware.com/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

1	Windows Desktops and Applications in Horizon	9
2	Introduction to Virtual Desktops	10
	Creating Desktop Pools in Horizon	10
	Deploying Applications that Run on Desktop Pools with VM Hosted Applications	11
	Creating Desktop Pools for Specific Types of Workers	11
3	Creating and Preparing a Virtual Machine for Cloning	15
	Creating a Virtual Machine for Cloning	16
	Create a Virtual Machine in vSphere	16
	Install a Guest Operating System	19
	Prepare a Guest Operating System for Remote Desktop Deployment	20
	Optimize Guest Operating System Performance	22
	Prepare Windows Server Operating Systems for Desktop Use	22
	Install Desktop Experience on Windows Server	24
	Install Horizon Agent on a Virtual Machine	24
	Horizon Agent Custom Setup Options	26
	Modify Installed Components with the Horizon Agent Installer	29
	Install a Horizon Agent Patch	30
	Uninstall a Horizon Agent Patch	30
	Installing Horizon Agent Silently	31
	Microsoft Windows Installer Command-Line Options	34
	Silent Installation Properties for Horizon Agent	37
	Install or Uninstall a Horizon Agent Patch Silently	42
	Configure a Virtual Machine with Multiple NICs for Horizon Agent	42
	Preparing a Golden Image Virtual Machine for Instant-Clones	43
	Configure a Golden Image Virtual Machine	44
	Activating Windows on Instant Clones	45
	Disable Windows Hibernation in the Golden Image	46
	Choosing ClonePrep or Sysprep for Customizing Your Virtual Desktops	46
	Increase the Timeout Limit for ClonePrep Customization Scripts	47
	Compute Profiles and Golden Image	48
	Creating Customization Specifications When Using Sysprep for Desktop Customization	48
	Creating Virtual Machine Templates for Full-Clone Virtual Desktops	49
	Using VMware Horizon Recording	49
	Horizon Recording Settings	54
4	Creating and Managing Instant-Clone Desktop Pools	59

Instant Clone Desktop Pools	59
Instant Clone Image Publishing and Creation Workflow	61
Worksheet for Creating an Instant-Clone Desktop Pool	62
Create an Instant-Clone Desktop Pool	90
Forensics Select Hold for Dedicated and Floating Instant Clone Desktops	91
Configure Instant Clones with vSphere Virtual Machine Encryption	95
Guest Customization for Instant Clones in VMware Horizon	96
Enabling VBS and vTPM for an Instant-Clone Desktop Pool	98
Configuring 3D Rendering Options for Instant-Clone Pools	99
Enable NVIDIA GRID vGPU for Instant-Clone Pools	100
Enable Soft 3D for Instant-Clone Pools	101
Enable vSGA for Instant-Clone Pools	102
Configure Number of Monitors and Screen Resolution	103
Allow Reuse of Existing Computer Accounts	103
Manually Customizing Machines	103
Customize Machines by Placing Them in Maintenance Mode After Pool Creation	104
Customize Machines by Starting Them in Maintenance Mode During Pool Creation	105
Patching an Instant-Clone Desktop Pool	105
Selective Patching	106
Monitor a Push-Image Operation	108
Reschedule or Cancel a Push-Image Operation	108
Perform Maintenance on Instant-Clone Hosts	109
Instant-Clone Maintenance Utilities	110

5 Creating and Managing Automated Full-Clone Desktop Pools 115

Worksheet for Creating an Automated Full-Clone Desktop Pool	115
Create an Automated Full-Clone Desktop Pool	126
Manually Customizing Machines	127
Customize Machines by Placing Them in Maintenance Mode After Pool Creation	128
Customize Machines by Starting Them in Maintenance Mode During Pool Creation	129
Desktop Settings for Automated Full-Clone Desktop Pools	129
Configuring 3D Rendering for Full-Clone Virtual Machine Pools	130
3D Renderer Options for Full-Clone Virtual Machine Pools	131
Best Practices for Configuring 3D Rendering For Full-Clone Virtual Machine Pools	133
Preparing for NVIDIA GRID vGPU Capabilities for Full-Clone Virtual Machines	136
Preparing for vDGA Capabilities for Full-Clone Virtual Machines	138
Preparing for AMD MxGPU for Full-Clone Virtual Machines	139
Preparing to Use vSGA for Full-Clone Virtual Machines	141
Preparing to Use Soft 3D for Full-Clone Virtual Machines	142
Video RAM Configuration Options for the 3D Renderer	142
Configure Full Clones with vSphere Virtual Machine Encryption	142

Rebuild a Virtual Machine in a Full-Clone Desktop Pool 143

6 Creating and Managing Manual Desktop Pools 145

Manual Pool of vSphere Virtual Machines 146

Manual Pool of Registered Non-vSphere Virtual Machines 147

Manual Pool of Registered Physical Machines 147

Prepare a non-vSphere Machine For Horizon 8 Management 149

Install Horizon Agent on a Non-vSphere Machine 150

Worksheet for Creating a Manual Desktop Pool 153

Desktop Pool Settings for Manual Pools in Horizon Console 163

Running Virtual Machines on Hyper-V 165

Create a Manual Desktop Pool 165

Managing non-vSphere Registered Machines 166

Remove a Registered Machine from a Manual Desktop Pool 167

Remove Registered Machines From Horizon 8 167

7 Configuring All Virtual Desktop Pool Types 168

Using a Naming Pattern for Desktop Pools 169

Machine-Naming Example 170

Change the Size of a Desktop Pool Provisioned by a Naming Pattern 171

Naming Machines Manually or Providing a Naming Pattern in Horizon Console 172

Specify a List of Machine Names 174

Add Machines to an Automated Pool Provisioned by a List of Names 175

Assign a Machine to a User in a Dedicated-Assignment Pool 177

Unassign a User from a Dedicated Machine in Horizon Console 178

Update Machine Aliases for Assigned Users 178

Setting Power Policies for Desktop Pools 179

Power Policies for Desktop Pools 179

Configure Dedicated Machines To Be Suspended After Users Disconnect 182

How Power Policies Affect Automated Desktop Pools 182

Power Policy Examples for Automated Pools with Floating Assignments 183

Power Policy Example for Automated Pools with Dedicated Assignments 184

Preventing Horizon 8 Power Policy Conflicts 185

Configure Desktop Session Timeouts in Horizon Console 185

Managing Desktop Pools 186

Edit a Desktop Pool 186

Fixed Settings in an Existing Desktop Pool 187

Disable or Enable a Desktop Pool 187

Disable or Enable Provisioning in a Desktop Pool 188

Duplicate an Automated Desktop Pool 188

Delete a Desktop Pool 190

Delete Virtual-Machine Desktops in a Pool	190
Export Horizon 8 Information to External Files	191
Examining GPU Resources on an ESXi Host	191
Creating Desktop Pools on a Single Host SDDC on VMware Cloud on AWS	192
Prevent Access to VMware Horizon Desktops Through RDP	192

8 Managing Storage for Virtual Desktops 194

Managing Storage with vSphere	194
Using VMware vSAN for High-Performance Storage and Policy-Based Management	195
Default Storage Policy Profiles for vSAN Datastores	196
Using Virtual Volumes for Virtual-Machine-Centric Storage and Policy-Based Management	198
Reducing Storage Requirements with Instant Clones	199
Storage Sizing for Instant-Clone Desktop Pools	200
Storage Sizing Guidelines for Instant-Clone Desktop Pools	201
Storage Sizing Formulas for Instant-Clone Desktop Pools	202
Storage Sizing Formulas for Creating Instant Clones When You Edit a Pool or Store Replicas on a Separate Datastore	203
Storing Instant Clones on Local Datastores (non-vSAN)	204
Configure View Storage Accelerator for Desktop Pools	205
Reclaim Disk Space on Instant Clones	206
Enable Periodic Space Reclamation for vSphere 6.7 and Earlier on Non-vSAN Datastores	207
Reclaiming Disk Space for vSphere 6.7 and Later On Non-vSAN Datastores	209
Reclaim Disk Space for vSphere 6.7U1 and later on vSAN datastores	209
Set Storage Accelerator and Space Reclamation Blackout Times	210

9 Monitoring Virtual Desktops and Desktop Pools 211

Monitor Virtual-Machine Desktop Status	211
Status of vCenter Server Virtual Machines	212
Recover Instant-Clone Desktops	214
Status of Unmanaged Machines	214

10 Troubleshooting Machines and Desktop Pools 216

Display Problem Machines in Horizon Console	216
Verify User Assignment for Desktop Pools	217
Restart Desktops and Reset Virtual Machines in Horizon Console	218
Send Messages to Desktop Users in Horizon Console	219
Manage Machines and Policies for Unentitled Users in Horizon Console	219

11 Setting Up Published Desktops and Applications in Horizon 220

12 Introduction to Published Desktops and Applications 221

Farms, RDS Hosts, and Published Desktops and Applications	221
Configure Horizon 8 for Published Desktops Delivery	222
Configure Horizon 8 for Published Applications Delivery	222

13 Setting Up Remote Desktop Services Hosts 224

Remote Desktop Services Hosts	224
Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use	225
Install Remote Desktop Services on Windows Server 2012 R2, 2016, or 2019	227
Install Desktop Experience on Windows Server 2012 R2, 2016, or 2019	228
Restrict Users to a Single Session	228
Install Horizon Agent on a Remote Desktop Services Host	229
Horizon Agent Custom Setup Options for an RDS Host	230
Modify Installed Components with the Horizon Agent Installer	232
Silent Installation Properties for Horizon Agent	233
Enable Time Zone Redirection for Published Desktop and Application Sessions	238
Enable Windows Basic Theme for Applications	239
Configure Group Policy to Start Runonce.exe	239
RDS Host Performance Options	240
RDS Host Printing Options	240
Configuring 3D Graphics for RDS Hosts	241
Understanding RDS Per-Device Client Access Licensing in Horizon	241

14 Creating and Managing Farms 243

Creating an Automated Instant-Clone Farm	244
Instant Clone Image Publishing and Creation Workflow for Farms	244
Preparing a Golden Image Virtual Machine for an Automated Farm	245
Worksheet for Creating an Automated Instant-Clone Farm in Horizon	247
Create an Automated Instant-Clone Farm in Horizon	255
Configuring 3D Rendering for Automated Instant Clone Farms	257
Creating a Manual Farm	258
Worksheet for Creating a Manual Farm in Horizon	258
Create a Manual Farm in Horizon	260
3D Graphics Options for Manual Farms	261
Managing Farms	263
Edit a Farm	263
Delete a Farm	263
Disable or Enable a Farm	263
Schedule Maintenance for an Automated Instant-Clone Farm in Horizon	264

15 Creating Published Desktop Pools 269

Understanding Published Desktop Pools	269
---------------------------------------	-----

Published Desktop Pools Settings	270
Create a Published Desktop Pool	271
Troubleshooting Instant Clones in the Internal VM Debug Mode	272

16 Creating Application Pools 274

Worksheet for Creating an Application Pool Manually	274
Create an Application Pool	278
Managing Application Pools	279
Edit an Application Pool	279
Delete an Application Pool	279
Duplicate an Application Pool	280
Change the Icon of a Published Application	280
Remove the Icon of a Published Application	281
Enable or Disable an Application Pool	281
Configure an Anti-Affinity Rule for an Application Pool in Horizon Console	282

17 Managing RDS Hosts and Sessions 284

Managing RDS Hosts in Horizon Console	284
Edit an RDS Host in a Manual Farm	285
Add an RDS Host to a Manual Farm	285
Remove an RDS Host from a Manual or Automated Farm	285
Remove a Registered RDS Host from Horizon	286
Disable or Enable an RDS Host in a Manual or Automated Farm	286
Status of RDS Hosts in Horizon Console	287
Monitor RDS Hosts in Horizon Console	287
Manage Published Desktop and Application Sessions in Horizon Console	289
Configuring Load Balancing for RDS Hosts in Horizon Console	290
Configure Load Balancing Settings on an RDS Host in Horizon Console	292
Load Balancing Settings	292
Writing a Load Balancing Script for an RDS Host	294
Enable the VMware Horizon View Script Host Service on an RDS Host	295
Configure a Load Balancing Script on an RDS Host	295
Verify a Load Balancing Script	296

Windows Desktops and Applications in Horizon

1

This guide describes how to create and provision pools of virtual machines and how to create and deploy pools of desktops and applications that run on Microsoft Remote Desktop Services (RDS) hosts.

Intended Audience

This information is intended for anyone who wants to create and provision desktop and application pools or to create and provision desktop and application pools. The information is written for experienced Windows system administrators who are familiar with virtual machine technology and datacenter operations.

Introduction to Virtual Desktops

2

With Horizon 8, you can create desktop pools that include thousands of virtual desktops. You can deploy desktops that run on virtual machines (VMs) or manage access to desktops that run on non-vSphere machines or physical machines. Create one VM as a golden image, and Horizon 8 can generate a pool of virtual desktops from that image. The golden image is also known as a base image.

This chapter includes the following topics:

- [Creating Desktop Pools in Horizon](#)
- [Deploying Applications that Run on Desktop Pools with VM Hosted Applications](#)
- [Creating Desktop Pools for Specific Types of Workers](#)

Creating Desktop Pools in Horizon

VMware Horizon uses desktop pools as its basis of centralized management. In Horizon 8, you create pools of virtual machines and select settings that give all the machines in a pool a common desktop definition. Horizon 8 can then deliver the desktops to end users via Horizon Clients. Horizon 8 can deliver desktops from single-user virtual desktop machines, which can be virtual machines that are managed by vCenter Server, virtual machines that run on another virtualization platform, or physical computers.

You create a desktop pool from one of the following sources:

- A virtual machine that runs on a virtualization platform other than vCenter Server that supports Horizon Agent.
- Physical desktop PC.
- A virtual machine that is hosted on an ESXi host and managed by vCenter Server.
- A session-based desktop on an RDS host. For more information about creating desktop pools from an RDS host, see the *Windows Desktops and Applications in Horizon* document.

You can create the following types of desktop pools:

Desktop Pool Type	Description
Automated	<p>Automated desktop pools use a vCenter Server virtual machine template or snapshot to create a pool of identical virtual machines.</p> <p>You can create these automated desktop pools:</p> <ul style="list-style-type: none"> ■ Instant-clone desktop pools. ■ Full-clone virtual machine desktop pools.
Manual	<p>Manual desktop pools are a collection of existing vCenter Server virtual machines, physical computers, or non-vCenter virtual machines. For manual pools, Horizon 8 does not create and manage the life cycle of the desktops in the pool. The desktops are created outside of Horizon 8 and then imported into Horizon Console.</p>

Deploying Applications that Run on Desktop Pools with VM Hosted Applications

You can deliver one or multiple published applications to end users without creating a farm of RDS hosts by creating a pool of virtual machine desktops to host the applications and then expose end users to only the published applications.

This approach benefits the following applications types:

- Applications that are only tested and certified on Windows 10.
- Applications that require .NET framework version compatibility.
- Applications that require special device support, where drivers may not run or be supported on RDS Hosts.
- Applications that require an install license and usage reporting by independent software vendors.

For more information, see the technical marketing white paper "Best Practices for Published Applications and Desktops in VMware Horizon and VMware Horizon Apps" available at <https://techzone.vmware.com>.

Creating Desktop Pools for Specific Types of Workers

The most fundamental question to consider is whether a certain type of user needs a persistent desktop or a non-persistent desktop. Whether you use persistent or non-persistent desktops depends on the specific type of worker.

Persistent Desktop

Persistent desktops have data in the operating system image itself that must be preserved, maintained, and backed up. For example, users who need to install some of their own applications or have data that cannot be saved outside of the virtual machine itself (such as on a file server or in an application database) require a persistent desktop.

There are several ways to create persistent desktops in Horizon 8:

- You can create pools of full clones (also known as full virtual machines).
- If you have already created virtual desktops or physical desktops (vCenter virtual machines, non-vCenter virtual machines, or physical PCs), you can import them into Horizon 8 as persistent desktops using the dedicated-assignment manual desktop pool.

Persistent desktops give users the highest degree of flexibility and control over their own desktops, however, they consume more compute resources and are more difficult to manage by IT. These desktops might require traditional image management techniques. Persistent desktops can have low storage costs in conjunction with certain storage system technologies. Since each persistent desktop is unique and must be preserved, backup and recovery technologies are important when considering strategies for business continuity.

Non-persistent Desktop

Non-persistent desktops are stateless images that are identical to one another. They are primarily used by users who do not need to install or preserve their own applications. Non-persistent desktops have many advantages, such as being easier to support and having lower storage costs. Other benefits include a limited need to back up the virtual machines and easier, less expensive disaster recovery and business continuity options. The virtual desktops themselves do not need to be protected as there is no unique user data stored. In the event that the virtual desktops are destroyed, you can simply re-create them from the golden image. Folder redirection and various profile technologies can optionally be used to storage user profile and user data. In Horizon 8 you can create non-persistent desktops by leveraging instant clones.

You can also specify how users are assigned desktops in a pool.

Dedicated-assignment pools	Each user is assigned a particular virtual desktop and returns to the same desktop at each login. Dedicated assignment pools require a one-to-one desktop-to-user relationship. For example, a pool of 100 desktops are needed for a group of 100 users.
Floating-assignment pools	Using floating-assignment pools also allows you to create a pool of desktops that can be used by shifts of users. For example, a pool of 100 desktops could be used by 300 users if they worked in shifts of 100 users at a time. The remote desktop is sometimes deleted and re-created after each use, offering a highly controlled environment.

Pools for Task Workers

Because task workers perform repetitive tasks within a small set of applications, you can utilize non-persistent desktops, which saves on storage and compute costs and make desktop management easier.

Use the following pool settings for instant-clone desktop pools:

- Use-floating assignment for the instant-clone desktop pool so that users log in to any available desktop. This setting reduces the number of desktops required if everyone does not need to be logged in at the same time.
- Configure the option to automatically logoff after disconnect, which deletes the instant clone whenever a user logs out. A new instant clone is created and ready for the next user to log in, thus effectively refreshing the desktop on every log out.
- To optimize compute resource utilization, use the dynamic pool provisioning capability of instant-clone desktop pools to grow or shrink the desktop pool based on demand. Be sure to specify enough spare desktops to satisfy the login rate.
- Consider storing instant-clone desktops on local ESXi data stores. This strategy can offer advantages such as utilizing inexpensive hardware, and faster virtual- machine provisioning. For a list of limitations for storing instant clones on local datastores, see [Reducing Storage Requirements with Instant Clones](#).

Note For information about other types of storage options, see [Chapter 8 Managing Storage for Virtual Desktops](#).

- Use profile management tools such as VMware Dynamic Environment Manager or Microsoft FSLogix so that users always have their preferred desktop appearance and application settings with Windows user profiles.

Pools for Knowledge Workers and Power Users

Knowledge workers usually are required to create complex documents and have them persist. Power users often need to install their own applications and have them persist. Depending on the nature and amount of personal data that must be retained, they require either a non-persistent desktop or a persistent desktop.

Use the following settings with non-persistent desktops for knowledge workers who do not need to install their own applications:

- Create dedicated-assignment desktop pools so that each user is guaranteed to have a virtual desktop anytime they login.
- Implement folder redirection, roaming profile, or another profile management solution to store and persist the user profile and user data.

For workers who must install their own applications, which adds data to the operating system disk, the best option is to create full-clone virtual machine desktops.

Pools for Kiosk Users

Kiosk users might include customers at airline check-in stations, students in classrooms or libraries, medical personnel at medical data entry workstations, or customers at self-service points. Accounts associated with client devices rather than users are entitled to use these desktop pools because users do not need to log in to use the client device or the remote desktop. Users can still be required to provide authentication credentials for some applications.

Virtual machine desktops that are set to run in kiosk mode use non-persistent desktops because user data does not need to be preserved in the operating system disk. Kiosk mode desktops are used with thin client devices or locked-down PCs. You must ensure that the desktop application implements authentication mechanisms for secure transactions, that the physical network is secure against tampering and snooping, and that all devices connected to the network are trusted.

As a best practice, use dedicated Connection Server instances to handle clients in kiosk mode, and create dedicated organizational units and groups in Active Directory for the accounts of these clients. This practice not only partitions these systems against unwarranted intrusion, but also makes it easier to configure and administer the clients.

To set up kiosk mode, you must use the `vdadmin` command-line interface and perform several procedures documented in the kiosk mode topics in the *Horizon Administration* document.

As part of this setup, you can use the following instant-clone desktop pool settings.

- Use-floating assignment for the instant-clone desktop pool so that users log in to any available desktop. This setting reduces the number of desktops required if everyone does not need to be logged in at the same time.
- Configure the option to automatically logoff after disconnect, which deletes the instant clone whenever a user logs out. A new instant clone is created and ready for the next user to log in, thus effectively refreshing the desktop on every log out.
- Consider storing instant-clone desktops on local ESXi data stores. This strategy can offer advantages such as utilizing inexpensive hardware, and faster virtual- machine provisioning. For a list of limitations for storing instant clones on local datastores, see [Reducing Storage Requirements with Instant Clones](#).

Note For information about other types of storage options, see [Chapter 8 Managing Storage for Virtual Desktops](#).

- Use an Active Directory GPO (Group Policy Object) to configure location-based printing, so that the desktop uses the nearest printer. For a complete list and description of the settings available through the Group Policy Administrative templates (ADMX files), see the *Horizon Remote Desktop Features and GPOs* document.
- Use a GPO or Smart Policies to control whether local USB devices are connected to the desktop when the desktop is launched or when USB devices are plugged in to the client computer.

Creating and Preparing a Virtual Machine for Cloning

3

You can create a pool of desktop machines by cloning a vCenter Server virtual machine (VM). Before you create the desktop pool, you need to prepare and configure this VM, which is used to spawn cloned virtual desktops. For instant-clone desktop pools, the base image is called a golden image. For full-clone desktop pools, the base image is called a Template Virtual Machine.

You can automate the creation and configuration of the VM or perform the steps manually. For more information, see [Manually Creating Optimized Windows Images for VMware Horizon VMs](#) or [Using Automation to Create Optimized Windows Images for VMware Horizon VMs](#).

This chapter is applicable if you are utilizing vSphere to create automated or manual desktop pools of virtual machines. For more information about preparing non-vSphere machines for use in manual desktop pools, see [Chapter 6 Creating and Managing Manual Desktop Pools](#).

For information on how to create optimized Windows images, see [Manually Creating Optimized Windows Images for VMware Horizon VMs](#) or [Using Automation to Create Optimized Windows Images for VMware Horizon VMs](#) in the VMware Digital Workspace Tech Zone.

For information about preparing machines that are used as Remote Desktop Services (RDS) hosts, see the *Windows Desktops and Applications in Horizon* guide.

For information about preparing Linux VMs for remote desktop deployment, see the *Linux Desktops and Applications in Horizon* guide.

This chapter includes the following topics:

- [Creating a Virtual Machine for Cloning](#)
- [Install Horizon Agent on a Virtual Machine](#)
- [Modify Installed Components with the Horizon Agent Installer](#)
- [Install a Horizon Agent Patch](#)
- [Uninstall a Horizon Agent Patch](#)
- [Installing Horizon Agent Silently](#)
- [Configure a Virtual Machine with Multiple NICs for Horizon Agent](#)
- [Preparing a Golden Image Virtual Machine for Instant-Clones](#)
- [Creating Customization Specifications When Using Sysprep for Desktop Customization](#)
- [Creating Virtual Machine Templates for Full-Clone Virtual Desktops](#)

- [Using VMware Horizon Recording](#)

Creating a Virtual Machine for Cloning

The first step in the process of deploying a pool of cloned desktops is to create a virtual machine in vSphere, install and configure the operating system.

Procedure

- 1 [Create a Virtual Machine in vSphere](#)

You can create a virtual machine in vSphere from scratch or by cloning an existing VM. This procedure describes creating a VM from scratch.

- 2 [Install a Guest Operating System](#)

After you create a virtual machine, you must install a guest operating system.

- 3 [Prepare a Guest Operating System for Remote Desktop Deployment](#)

You must perform certain tasks to prepare a guest operating system for remote desktop deployment.

- 4 [Optimize Guest Operating System Performance](#)

You can perform certain steps to optimize guest operating system performance for remote desktop deployment. While optimization is optional, taking some or all of the steps will improve your performance and VM consolidation significantly, leading to a lower cost-per-desktop.

- 5 [Prepare Windows Server Operating Systems for Desktop Use](#)

To use a supported Windows Server virtual machine as a single-session virtual desktop (rather than as an RDS host), you must perform certain steps before you install Horizon Agent in the virtual machine. You must also configure Horizon Console to treat Windows Servers as supported operating systems for Horizon 8 desktop use.

- 6 [Install Desktop Experience on Windows Server](#)

For published desktops and applications, and for virtual desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

Create a Virtual Machine in vSphere

You can create a virtual machine in vSphere from scratch or by cloning an existing VM. This procedure describes creating a VM from scratch.

Prerequisites

- Familiarize yourself with the custom configuration parameters for virtual machines. See [Virtual Machine Custom Configuration Parameters](#).

Procedure

- 1 Log in to vSphere Client.
- 2 Right-click any inventory object that is a valid main object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select **New Virtual Machine**.
- 3 Select **Create a new virtual machine** and click **Next**.
- 4 Follow the prompts to specify the virtual machine custom options.
- 5 On the **Customize hardware** page, select **Virtual Hardware** to configure hardware settings.
 - a Click **Add New Device** and select a CD/DVD drive, set the media type to use an ISO image file, select the ISO image file of an appropriate operating system, and select **Connect at power on**.
- 6 On the **Customize hardware** page, select **VM Options** to configure virtual machine settings.
 - a (Optional) In the **Boot Options**, set **Boot Delay** to 10,000 milliseconds.

You can set the boot delay to easily access the virtual machine's BIOS on boot and modify the system settings. After you modify the system settings, you can reboot the boot delay.
- 7 Click **Finish** to create the virtual machine.

What to do next

Install the operating system.

Virtual Machine Custom Configuration Parameters

You can use virtual machine custom configuration parameters as baseline settings when you create a virtual machine for remote desktop deployment.

Table 3-1. Custom Configuration Parameters

Parameter	Description and Recommendations
Name and Folder	The name and location of the virtual machine. If you plan to use the virtual machine as a template, assign a generic name. The location can be any folder within your datacenter inventory.
Host/Cluster	The ESXi server or cluster of server resources that will run the virtual machine. If you plan to use the virtual machine as a template, the location of the initial virtual machine does not necessarily specify where future virtual machines created from template will reside.
Resource Pool	If the physical ESXi server resources are divided into resource pools, you can assign them to the virtual machine.
Datastore	The location of files associated with the virtual machine.
Hardware Machine Version	The hardware machine version that is available depends on the ESXi version you are running. As a best practice, select the latest available hardware machine version, which provides the greatest virtual machine functionality. Certain Horizon 8 features require minimum hardware machine versions.

Table 3-1. Custom Configuration Parameters (continued)

Parameter	Description and Recommendations
Guest Operating System	The type of operating system that you will install in the virtual machine.
CPUs	The number of virtual processors in the virtual machine.
Memory	The amount of memory to allocate to the virtual machine.
Network	<p>The number of virtual network adapters (NICs) in the virtual machine.</p> <p>One NIC is usually sufficient. The network name should be consistent across virtual infrastructures. An incorrect network name in a template can cause failures during the instance customization phases.</p> <p>When you install Horizon Agent on a virtual machine that has more than one NIC, you must configure the subnet that Horizon Agent uses. See Configure a Virtual Machine with Multiple NICs for Horizon Agent for more information.</p> <p>Important For Windows, you must use the VMXNET 3 network adapter.</p>
SCSI Controller	<p>The type of SCSI adapter to use with the virtual machine. Select either LSI Logic SAS or VMware Paravirtual (PVSCSI).</p> <p>Using PVSCSI may require additional steps depending on the version of Windows to be installed. For more information, see the VMware Knowledge Base article Configuring disks to use VMware Paravirtual SCSI (PVSCSI) controllers (1010398).</p>
Select a Disk	<p>The disk to use with the virtual machine.</p> <p>Create a new virtual disk based on the amount of local storage that you decide to allocate to each user. Allow enough storage space for the OS installation, patches, and locally installed applications.</p> <p>To reduce the need for disk space and management of local data, you should store the user's information, profile, and documents on network shares rather than on a local disk.</p>

Create a Virtual Machine with Virtualization-Based Security

You can create a virtual machine in vSphere to use Virtualization-based security (VBS). Using a virtual machine enabled with VBS provides better protection from vulnerabilities within and malicious exploits to the operating system.

Prerequisites

- Microsoft Windows 10 (64-bit) or Windows Server 2016 (64-bit) or later operating system.
- Familiarize yourself with the custom configuration parameters for virtual machines. See [Virtual Machine Custom Configuration Parameters](#).

Note VBS is not supported for vGPU enabled virtual machines. URL Content Redirection and scanner redirection might not work properly with VBS enabled.

Procedure

- 1 Log in to vSphere Client.

- 2 Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select **New Virtual Machine**.
- 3 Select **Create a new virtual machine** and click **Next**.
- 4 Follow the prompts to specify the virtual machine custom options.
- 5 On the **Select a guest OS** page, select Windows as the guest OS and select Microsoft Windows 10 (64-bit) as the guest OS version. Then, select **Enable Windows Virtualization Based Security**.
- 6 To deploy automated desktop pools that contain full virtual machines or instant clones, on the **Customize hardware** page, verify that you do not add any Trusted Platform Module (vTPM) device. Connection Server adds a vTPM device to each virtual machine during the desktop pool creation process.
- 7 Follow the prompts to complete the virtual machine setup and click **Finish** to create the virtual machine.

What to do next

- Install the Windows 10 (64-bit) or Windows Server 2016 (64-bit) or later operating system on the virtual machine.
- On Windows 10, enable the VBS group policy. For more information, consult the article "Enable virtualization-based protection of code integrity" in the Microsoft documentation. Then reboot the virtual machine.
- On Windows Server 2016 and later builds, enable the VBS group policy, install the **Hyper-V** role and reboot the virtual machine.

Install a Guest Operating System

After you create a virtual machine, you must install a guest operating system.

Prerequisites

- For the list of supported guest operating systems, see the VMware Knowledge Base (KB) articles <https://kb.vmware.com/s/article/78714> and <https://kb.vmware.com/s/article/78715>.
- Verify that an ISO image file of the guest operating system is on a datastore on your ESXi server.
- Verify that the CD/DVD drive in the virtual machine points to the ISO image file of the guest operating system and that the CD/DVD drive is configured to connect at power on.

Procedure

- 1 In vSphere Client, log in to the vCenter Server system where the virtual machine resides.

- 2 Right-click the virtual machine, select **Power**, and select **Power On** to start the virtual machine.

Because you configured the CD/DVD drive to point to the ISO image of the guest operating system and to connect at power on, the guest operating system installation process begins automatically.

- 3 Click the **Console** tab and follow the installation instructions provided by the operating system vendor.
- 4 Activate Windows.

What to do next

Prepare the guest operating system for Horizon 8 desktop deployment.

Prepare a Guest Operating System for Remote Desktop Deployment

You must perform certain tasks to prepare a guest operating system for remote desktop deployment.

Prerequisites

- Create a virtual machine and install a guest operating system.
- Configure an Active Directory domain controller for your remote desktops. See the *Horizon Installation and Upgrade* document for more information.
- To make sure that desktop users are added to the local Remote Desktop Users group of the virtual machine, create a restricted Remote Desktop Users group in Active Directory. See the *Horizon Installation and Upgrade* document for more information.
- Verify that Remote Desktop Services are started on the virtual machine. Remote Desktop Services are required for Horizon Agent installation, SSO, and other Horizon 8 operations. You can disable RDP access to your Horizon 8 desktops by configuring desktop pool settings and group policy settings. See [Prevent Access to VMware Horizon Desktops Through RDP](#).
- Verify that you have administrative rights on the guest operating system.
- On Windows Server operating systems, prepare the operating system for desktop use. See [Prepare Windows Server Operating Systems for Desktop Use](#).
- If you intend to configure 3D graphics rendering for desktop pools, familiarize yourself with the **Enable 3D Support** setting for virtual machines. On ESXi hosts, you can select options that determine how the 3D renderer is managed on the ESXi host. For details, see the *vSphere Virtual Machine Administration* document in the vSphere documentation.

Procedure

- 1 In vSphere Client, log in to the vCenter Server system where the virtual machine resides.
- 2 Right-click the virtual machine, select **Power**, and select **Power On** to start the virtual machine.

- 3 Right-click the virtual machine, select **Guest**, and select **Install/Upgrade VMware Tools** to install the latest version of VMware Tools.

Note If you are using VMTools v11.x, see the VMware Knowledge Base (KB) article <https://kb.vmware.com/s/article/78434>.

- 4 Ensure that the virtual machine is synchronized to a reliable time source.

In general, guests can use the VMware Tools time synchronization method in preference to other methods of time synchronization. The VMware Tools online help provides information on configuring time synchronization between guest and host.

A Windows guest that is a member of a Windows domain synchronizes its time with its domain controller using the Windows Time Service. For these guests, this is the appropriate time synchronization method and VMware Tools time synchronization must not be used.

Guests must use only one method of time synchronization. For example, a Windows guest that is not a member of a Windows domain must have its Windows Time Service disabled.

Important Hosts that are being relied upon for time synchronization must themselves be synchronized to a reliable time source, using the built-in NTP client. Verify that all hosts in a cluster use the same time source.

Note Windows domain controllers can use either VMware Tools time synchronization or another reliable time source. All domain controllers within a forest and domain controllers across forests with inter-forest trusts must be configured to use the same time source.

- 5 Install service packs and updates.
- 6 Install antivirus software.
- 7 Install other applications and software, such as smart card drivers if you are using smart card authentication.

If you plan to use VMware Workspace ONE Access to offer a catalog that includes ThinApp applications, you must install Workspace ONE Intelligent Hub for Windows.

Important If you are installing Microsoft .NET Framework, you must install it after you install Horizon Agent.

- 8 If Horizon Client devices will connect to the virtual machine with the PCoIP display protocol, set the power option **Turn off the display** to **Never**.

If you do not disable this setting, the display will appear to freeze in its last state when power savings mode starts.

- 9 If Horizon Client devices will connect to the virtual machine with the PCoIP display protocol, go to **Control Panel > System > Advanced System Settings > Performance Settings** and change the setting for **Visual Effects** to **Adjust for best performance**.

If you instead use the setting called **Adjust for best appearance** or **Let Windows choose what's best for my computer** and Windows chooses appearance instead of performance, performance is negatively affected.

- 10 If a proxy server is used in your network environment, configure network proxy settings.

- 11 Configure network connection properties.

- a Assign a static IP address or specify that an IP address is assigned by a DHCP server.

Horizon 8 does not support link-local (169.254.x.x) addresses for Horizon 8 desktops.

- b Set the preferred and alternate DNS server addresses to your Active Directory server address.

- 12 (Optional) Join the virtual machine to the Active Directory domain for your remote desktops.

A golden image virtual machine for creating instant clones must either belong to the same Active Directory domain as the domain that the desktop machines will join or be a member of a workgroup.

- 13 Configure Windows Firewall to allow Remote Desktop connections to the virtual machine.

- 14 (Optional) Disable Hot Plug PCI devices.

This step prevents users from accidentally disconnecting the virtual network device (vNIC) from the virtual machine.

- 15 (Optional) Configure user customization scripts.

Optimize Guest Operating System Performance

You can perform certain steps to optimize guest operating system performance for remote desktop deployment. While optimization is optional, taking some or all of the steps will improve your performance and VM consolidation significantly, leading to a lower cost-per-desktop.

For more details including details on the operating system optimization tool, see [Windows OS Optimization Tool for VMware Horizon Guide](#).

Prepare Windows Server Operating Systems for Desktop Use

To use a supported Windows Server virtual machine as a single-session virtual desktop (rather than as an RDS host), you must perform certain steps before you install Horizon Agent in the virtual machine. You must also configure Horizon Console to treat Windows Servers as supported operating systems for Horizon 8 desktop use.

Prerequisites

- Familiarize yourself with the steps to install the Desktop Experience feature on Windows Server. See [Install Desktop Experience on Windows Server](#).
- On Windows Server machines, familiarize yourself with the steps to configure the Windows Firewall service to restart after failures occur.

Procedure

- 1 Verify that the Remote Desktop Services role is not installed.

When the Remote Desktop Services role is not present, the Horizon Agent installer prompts you to install Horizon Agent in RDS mode or desktop mode. If the Remote Desktop Services role is present, the Horizon Agent installer does not display these options and it treats the Windows Server machine as an RDS host instead of a single-session Horizon 8 desktop.

- 2 During Horizon Agent installation, select **Desktop mode** to install Horizon Agent as a single-user virtual desktop where published desktop features will not be available.

- 3 (Optional) Install the Desktop Experience feature if you plan to use the following features.

- HTML Access
- Scanner redirection
- Windows Aero

- 4 (Optional) To use Windows Aero on a Windows Server desktop, start the Themes service.

When you create or edit a desktop pool, you can configure 3D graphics rendering for your desktops. The 3D Renderer setting offers a Software option that enables users to run Windows Aero on the desktops in the pool.

- 5 On Windows Server machines, configure the Windows Firewall service to restart after failures occur.

- 6 Configure Horizon Console to treat Windows Servers as supported desktop operating systems.

If you do not perform this step, you cannot select Windows Server machines for desktop use in Horizon Console.

- a In Horizon Console, select **Settings > Global Settings**.
- b In the **General Settings** tab, click **Edit**.
- c Select the **Enable Windows Server desktops** check box and click **OK**.

Results

When you enable Windows Server desktops in Horizon Console, Horizon Console displays all available Windows Server machines, including machines on which Connection Server is installed, as potential machines for desktop use. You cannot install Horizon Agent on machines on which other Horizon 8 software components are installed.

Install Desktop Experience on Windows Server

For published desktops and applications, and for virtual desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

Windows Server operating systems are supported on machines that are used as RDS hosts and on single-user virtual machines.

Note A Windows Server 2016 or later installation with the Desktop Experience option, installs the standard user interface and all tools, including the client experience and the desktop experience features. For Windows Server 2012 RS, the client experience and desktop experience features require a separate installation. For Windows Server 2016 or later installation, select **Windows Server 2016** or **Windows Server 2019** or **Windows Server (Server with Desktop Experience)**. If you do not make a choice in the Setup wizard, Windows Server 2016 or Windows Server 2019 is installed as the Server Core installation option. You cannot switch between the installation options. If you install **Windows Server (Server with Desktop Experience)**, and later decide to use **Windows Server 2016** or **Windows Server 2019**, you must perform a fresh installation of Windows Server 2016 or Windows Server 2019.

Procedure

- 1 Log in as an administrator.
- 2 Start Server Manager.
- 3 Select **Add roles and features**.
- 4 On the Select Installation Type page, select **Role-based or feature-based installation**.
- 5 On the Select Destination Server page, select a server.
- 6 On the Select Server Roles page, accept the default selection and click **Next**.
- 7 On the Select Features page, under **User Interfaces and Infrastructure**, select **Desktop Experience**.
- 8 Follow the prompts and finish the installation.

Install Horizon Agent on a Virtual Machine

You must install Horizon Agent on virtual machines that are managed by vCenter Server so that Connection Server can communicate with them. Install Horizon Agent on all virtual machines that you use as templates for full-clone desktop pools and golden images for instant-clone desktops.

To install Horizon Agent on multiple Windows virtual machines without having to respond to wizard prompts, you can install Horizon Agent silently.

The Horizon Agent software cannot coexist on the same virtual or physical machine with other Horizon software components, including Connection Server. It can coexist with Horizon Client.

Prerequisites

- Verify that you have prepared Active Directory. See the *Horizon Installation and Upgrade* document.
- Prepare the guest operating system for remote desktop deployment. See [Prepare a Guest Operating System for Remote Desktop Deployment](#).
- To use a Windows Server virtual machine as a single-session virtual desktop (rather than as an RDS host), perform the steps described in [Prepare Windows Server Operating Systems for Desktop Use](#). To use a Windows Server virtual machine as an RDS host, see Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use in the *Windows Desktops and Applications in Horizon* document.
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at <http://www.vmware.com/go/downloadview>.
- Verify that you have administrative rights on the virtual machine.
- Familiarize yourself with the Horizon Agent custom setup options. See [Horizon Agent Custom Setup Options](#).
- Familiarize yourself with the TCP ports that the Horizon Agent installation program opens on the firewall. See the *Horizon Overview and Deployment Planning* document for more information.
- Verify that you have a minimum of 2 CPUs to install or upgrade Horizon Agent from versions 7.x or later.

Procedure

- 1 To start the Horizon Agent installation program, double-click the installer file.

The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.
- 2 Accept the VMware license terms.
- 3 If you install Horizon Agent on a Windows Server machine on which the Remote Desktop Session Host (RDSH) role is not installed, the Horizon Agent installer prompts you to install Horizon Agent in RDS mode or Desktop mode. If the RDSH role is already installed on the system, by default the Horizon Agent installer will install Horizon Agent in RDS mode.
 - If you select **RDS mode**, the installer will install the Remote Desktop Session Host (RDSH) role and/or the Desktop Experience role and prompt you to restart the system. After the roles are installed and the system is restarted, launch the installer again to continue installing Horizon Agent in RDS mode.

- If you select **Desktop mode**, the installer will install Horizon Agent as a single-user virtual desktop where published desktop features will not be available.
- 4 Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.
You must install all Horizon 8 components with the same IP version.
 - 5 Select whether to enable or disable FIPS mode.
This option is available only if FIPS mode is enabled in Windows.
 - 6 Select your custom setup options.
By default, **VMware Horizon Instant Clone Agent** is enabled.
 - 7 Accept or change the destination folder.
 - 8 Follow the prompts in the Horizon Agent installation program and finish the installation.

Note If you did not enable Remote Desktop support during guest operating system preparation, the Horizon Agent installation program prompts you to enable it. If you do not enable Remote Desktop support during Horizon Agent installation, you must enable it manually after the installation is finished.

- 9 If you selected the USB redirection option, restart the virtual machine to enable USB support.
In addition, the **Found New Hardware** wizard might start. Follow the prompts in the wizard to configure the hardware before you restart the virtual machine.

What to do next

If the virtual machine has multiple NICs, configure the subnet that Horizon Agent uses. See [Configure a Virtual Machine with Multiple NICs for Horizon Agent](#).

Horizon Agent Custom Setup Options

When you install Horizon Agent, certain features are automatically installed on all guest operating systems on which they are supported. In addition, you can select or deselect custom setup options.

To learn which features are supported on which guest operating systems, see "Feature Support Matrix for Horizon Agent" in the *Horizon Overview and Deployment Planning* document.

To change custom setup options after you install the latest Horizon Agent version, you must uninstall and reinstall Horizon Agent. For patches and upgrades, you can run the new Horizon Agent installer and select a new set of options without uninstalling the previous version.

In an IPv6 environment, VMware Audio options are selected and installed by default.

Table 3-2. Horizon Agent Features That Are Installed Automatically

Feature	Description
Core	Installs the core functionality.
PCoIP Agent	Lets users use the PCoIP display protocol to connect to the remote desktop. Installing the PCoIP Agent feature disables sleep mode on Windows desktops. When a user navigates to the Power Options or Shut Down menu, sleep mode or standby mode is inactive. Desktops do not go into sleep or standby mode after a default period of inactivity. Desktops remain in active mode.
PSG Agent	Installs the PCoIP Secure Gateway on remote desktops to implement the PCoIP display protocol.
VMware Blast	Installs the VMware Blast display protocol on remote desktops.
Windows Media Multimedia Redirection (MMR)	Extends multimedia redirection to Windows desktops and clients. This feature delivers a multimedia stream directly to the client computer, allowing the multimedia stream to be processed on the client hardware instead of the remote ESXi host.
HTML5 Multimedia Redirection	Redirects HTML5 multimedia content in a Chrome or Edge browser to the client, for performance optimization.
Browser Redirection	Renders a website on the client system instead of the agent system, and displays the website over the remote browser's viewport, when a user uses the Chrome browser in a remote desktop.
Media Optimization for Microsoft Teams	Redirects Microsoft Teams audio calls, video calls, and desktop share views to process on the client machine instead of in the virtual desktop.
Virtual video driver	Provides a virtual video driver on the remote desktop.
Unity Touch	Allows tablet and smart phone users to interact easily with Windows applications that run on the remote desktop. Users can browse, search, and open Windows applications and files, choose favorite applications and files, and switch between running applications, all without using the Start menu or Taskbar.
VMware Integrated Printing	Enables users to print to any printer available on their client machines. Location-based printing is supported. VMware Integrated Printing is supported on the following remote desktops and applications: <ul style="list-style-type: none"> ■ Desktops that are deployed on single-user machines, including Windows desktop and Windows server machines ■ Published desktops and published applications that are deployed on RDS hosts, where the RDS hosts are virtual machines or physical machines
vRealize Operations Desktop Agent	This feature that allows vRealize Operations Manager to monitor remote desktops is deprecated in this release. When you perform a fresh installation, the desktop agent will not collect data. When you perform an upgrade, if the desktop agent has been configured with vRealize Operations before the upgrade, the desktop agent will still collect and report data to vROps. You need to stop the service manually.

Table 3-3. Horizon Agent Custom Setup Options in an IPv4 Environment

Option	Description
USB Redirection	<p>Gives users access to locally connected USB devices on their desktops.</p> <p>This option is not selected by default. You must select the option to install it.</p> <p>For guidance about using USB redirection securely, see the <i>Horizon Security</i> document. For example, you can use group policy settings to disable USB redirection for specific users.</p> <p>For information about using the USB redirection feature, and USB device type limitations, see "Using USB Devices with Remote Desktops and Applications" in the <i>Horizon Remote Desktop Features and GPOs</i> document.</p>
Real-Time Audio-Video	<p>Redirects webcam and audio devices that are connected to the client system so that they can be used on the remote desktop.</p>
Client Drive Redirection	<p>Allows Horizon Client users to share local drives with their remote desktops.</p> <p>After this option is installed, no further configuration is required on the remote desktop.</p> <p>Client Drive Redirection is also supported on published desktops and published applications and on virtual desktops that run on unmanaged machines.</p>
Help Desk Plugin for Horizon Agent	<p>You must have a Horizon Enterprise edition license or Horizon Apps Advanced edition license for Horizon to use the Help Desk Tool. This option is installed and enabled by default.</p>
Scanner Redirection	<p>Redirects scanning and imaging devices that are connected to the client system so that they can be used on the remote desktop or application.</p> <p>This option is not selected by default. You must select the option to install it.</p>
Smartcard Redirection	<p>Lets users authenticate with smart cards when they use the PCoIP or VMware Blast display protocol. This option is not selected by default.</p> <p>Smartcard Redirection is supported on remote desktops that are deployed on single-user machines.</p>
Serial Port Redirection	<p>Redirects serial COM ports that are connected to the client system so that they can be used on the remote desktop.</p> <p>This option is not selected by default. You must select the option to install it.</p>
VMware Audio	<p>Provides a virtual audio driver on the remote desktop.</p>
UNC Path Redirection	<p>Redirects UNC Path in Outlook 2013, 2016, 2019, 2021 or Office365 Outlook from agent-to-client, for performance optimization.</p>
URL Content Redirection	<p>Redirects URL content in an Internet Explorer 9, 10, or 11 browser, Chrome, Edge-chromium, Firefox, and third-party not-browser application from agent-to-client, for performance optimization.</p>
VMware Horizon Instant Clone Agent	<p>Lets this virtual machine be the golden image of an instant-clone desktop pool. This option is selected by default.</p>
Fingerprint Scanner Redirection	<p>Redirects fingerprint scanner devices that are plugged into a serial port on a Windows client system to virtual desktops, published desktops, and published applications.</p>
VMware Virtualization Pack for Skype for Business	<p>Makes optimized audio and video calls with Skype for Business inside a virtual desktop. This option is not selected by default. You must select the option to install it.</p>
Horizon Performance Tracker	<p>Monitors the performance of the display protocol and system resource usage. This option is not selected by default. You must select the option to install it. .NET Framework 4.6.2 or later is required if you install Horizon Performance Tracker.</p>

Table 3-3. Horizon Agent Custom Setup Options in an IPv4 Environment (continued)

Option	Description
SDO Sensor Redirection	Enables the Simple Device Orientation (SDO) sensor redirection feature. This option is not selected by default. You must select the option to install it.
Geolocation Redirection	Enables the Geolocation Redirection feature. This option is not selected by default. You must select this option to install it.

Modify Installed Components with the Horizon Agent Installer

Horizon Agent installer allows you to modify already installed components without needing to uninstall and reinstall Horizon Agent.

You can run Horizon Agent installer on a virtual machine where Horizon Agent is already installed to modify, repair, or remove previously installed components. You can also change custom setup options silently using the command line.

Note You cannot switch between installation types, such as managed to unmanaged machines. You also cannot modify Instant Clone Agent (NGVC).

Procedure

- 1 To start the Horizon Agent installation program, double-click the installer file. The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

You can also use the **Uninstall or change a program** in the Control Panel: Click **VMware Horizon Agent**, then click **Change**.

- 2 Select **Modify** from these three options:
 - Modify: add or remove the components that are installed.
 - Repair: fix missing or corrupt files, shortcuts, and registry entries.
 - Remove: remove Horizon Agent from the computer.
- 3 Select or deselect features to add or remove them from the list.
- 4 Follow the prompts to finish the installation.
- 5 Restart the system for the changes to take effect.

What to do next

You can confirm the components that were removed (Absent) or added (Local) in the registry located at `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\Installer\Features_HorizonAgent`.

Install a Horizon Agent Patch

You can install a Horizon Agent hotpatch where Horizon Agent is already installed without needing to uninstall and reinstall Horizon Agent. You can also install a patch silently.

You can install the latest patch which is included in a Horizon Agent build.

Prerequisites

- In **Control Panel > Programs > Programs and Features** , verify Horizon Agent is already installed and note the build number.
- In **Control Panel > Programs > Programs and Features > Installed Updates**, verify the Horizon Agent Update Patch is the same build number as the Horizon Agent build.

Procedure

- 1 To start the Horizon Agent installation program, double-click the Horizon Agent Update Patch installer file. The installer filename is `VMware-Horizon-Agent-x86_64-YYMM-y.y.y-xxxxxx.msp`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.
- 2 Select **Repair** from these three options:
 - Modify: add or remove the components that are installed.
 - Repair: install patches, fix missing or corrupt files, shortcuts, and registry entries.
 - Remove: remove Horizon Agent from the computer.
- 3 Follow the prompts to finish the installation.
- 4 Restart the system for the changes to take effect.

What to do next

Verify the patch build number is updated in the registry: `HKLM:\SOFTWARE\WOW6432Node\VMware, Inc.\AgentVersions!view-agent` and `HKLM:\SOFTWARE\VMware, Inc.\Vmware VDM!BuildNumber` and in **Control Panel > Programs > Programs and Features > Installed Updates > Patch update version**.

Uninstall a Horizon Agent Patch

You can remove a Horizon Agent hotpatch where Horizon Agent is already installed without needing to uninstall and reinstall Horizon Agent. You can also uninstall a patch silently by running a PowerShell script.

Prerequisites

- In **Control Panel > Programs > Programs and Features** , verify Horizon Agent is already installed and note the build number.

- In **Control Panel > Programs > Programs and Features > Installed Updates**, verify the Horizon Agent Update Patch is the same build number as the Horizon Agent build.

Procedure

- 1 To uninstall the patch, go to **Control Panel > Programs > Uninstall or change a Program**, select the patch and click **Uninstall**.

Uninstalling a patch will revert to the previous build.

- 2 Restart the system for the changes to take effect.

What to do next

Verify that no reference of the patch exists in the registry: HKLM:\SOFTWARE\WOW6432Node\VMware, Inc.\AgentVersions!view-agent and HKLM:\SOFTWARE\VMware, Inc.\Vmware VDM!BuildNumber Or in **Control Panel > Programs > Programs and Features**.

Installing Horizon Agent Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install Horizon Agent on several Windows virtual machines or physical computers. In a silent installation, you do not have to respond to wizard prompts. A silent upgrade uses the same install commands. You can also modify already installed Horizon Agent components silently.

You can perform a silent installation either by entering parameters manually on the command line or by using a settings file.

About Silent Installation

With silent installation, you can efficiently deploy Horizon 8 components in a large enterprise.

If you do not want to install all features that are installed automatically or by default, you can use the `ADDLOCAL` MSI property to selectively install individual setup options and features. For details about the `ADDLOCAL` property, see [Table 3-5. MSI Command-Line Options and MSI Properties](#).

You can modify features by using the `ADDLOCAL` and `REMOVE` MSI properties.

You can use the following PowerShell command to query the registry of installed components on the system where Horizon Agent is installed for the `ModifyPath` base command line:

```
Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object
DisplayName, ModifyPath |
Where-Object {$_.DisplayName -eq 'VMware Horizon Agent'} | Format-Table -AutoSize
```

The output:

DisplayName	ModifyPath
VMware Horizon Agent	MsiExec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111}

Prerequisites

- Verify that you have prepared Active Directory. See the *Horizon Installation and Upgrade* document.
- Prepare the guest operating system for desktop deployment. See [Prepare a Guest Operating System for Remote Desktop Deployment](#).
- To use Windows Server as a single-session remote desktop or as an RDSH host, perform the steps described in [Prepare Windows Server Operating Systems for Desktop Use](#).

Note The Horizon Agent installer does not automatically install any role in silent mode. If you want RDS mode, then pre-install the RDSH role on the system.

- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at <http://www.vmware.com/go/downloadview>.

The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

- Verify that you have administrative rights on the virtual machine or physical PC.
- Familiarize yourself with the Horizon Agent custom setup options. See [Horizon Agent Custom Setup Options](#).
- Familiarize yourself with the MSI installer command-line options. See [Microsoft Windows Installer Command-Line Options](#).
- Familiarize yourself with the silent installation properties available with Horizon Agent. See [Silent Installation Properties for Horizon Agent](#).
- Familiarize yourself with the TCP ports that the Horizon Agent installation program opens on the firewall. See the *Horizon Overview and Deployment Planning* document for more information.
- Verify that the latest Windows Update patches are installed on the guest operating systems on which you plan to install Horizon Agent silently. In certain cases, an interactive installation by an administrator might be required to execute pending Windows Update patches. Verify that all OS operations and subsequent reboots are completed.

Install Horizon Agent Silently By Entering Parameters on the Command Line

- 1 Open a Windows command prompt on the virtual machine or physical PC.

The following example installs Horizon Agent with the components Core, VMware Blast, PCoIP, Unity Touch, PSG, USB redirection, and Real-Time Audio-Video components.


```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn
VDM_VC_MANAGED_AGENT=1 ADDLOCAL=Core,USB,RTAV"
```

The following example installs Horizon Agent on an unmanaged computer and registers the desktop with the specified Connection Server, `cs1.companydomain.com`. In addition, the installer installs the Core, VMware Blast, PCoIP, Unity Touch, PSG, VMware Integrated Printing, and USB redirection components.

```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn
VDM_VC_MANAGED_AGENT=0 VDM_SERVER_NAME=cs1.companydomain.com
VDM_SERVER_USERNAME=admin.companydomain.com VDM_SERVER_PASSWORD=secret
ADDLOCAL=Core,PrintRedir,USB"
```

The following example modifies and removes the USB component from an existing installation:

```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn REMOVE=USB"
```

ProductCode-driven command line example: `msiexec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111} /qn REMOVE=USB`

The following example modifies the agent installation by replacing Horizon Performance Tracker with the Horizon Help Desk Tool: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=HelpDesk REMOVE=PerfTracker"`

ProductCode-driven command line example: `msiexec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111} /qn ADDLOCAL=HelpDesk REMOVE=PerfTracker`

The following example modifies the agent installation by adding serial port and scanner redirection: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=SerialPortRedirection,ScannerRedirection"`

ProductCode-driven command line example: `msiexec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111} /qn ADDLOCAL=SerialPortRedirection,ScannerRedirection`

Note If you install Horizon Agent on a Windows Server machine, and you intend to configure the machine as a single-user Horizon desktop rather than as an RDS host, you must include the `VDM_FORCE_DESKTOP_AGENT=1` property in the installation command. This requirement applies to machines that are managed by vCenter Server and unmanaged machines.

When the installation is complete, if the virtual machine has multiple NICs, configure the subnet that Horizon Agent uses. See [Configure a Virtual Machine with Multiple NICs for Horizon Agent](#).

Install Horizon Agent Silently Using a Settings File

- 1 Create a text file containing the parameters you want to use for the installation.
 - The file can be located on either a local or network drive. Using mapped drives is also supported.
 - The file can have any extension, but must be text-only.
 - Each parameter must be on its own line.

- Any other text (besides the parameters themselves) must be commented out using a hash sign (#) at the beginning of the line.
- Both whitespace and empty newlines are allowed in the file.

Note If you install Horizon Agent on a Windows Server machine, and you intend to configure the machine as a single-user Horizon desktop rather than as an RDS host, you must include the `VDM_FORCE_DESKTOP_AGENT=1` property in the settings file. This requirement applies to machines that are managed by vCenter Server and unmanaged machines.

Attention The installer does not process passwords. If your file includes a known password property such as `VDM_SERVER_PASSWORD`, the installer fails to parse the file and returns an error. To include a password, you must enter it manually on the command line. When you enter a password in this way, it is passed only once and is not logged anywhere.

- 2 Open a Windows command prompt on the virtual machine or physical PC and enter the following.

```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /v SETTINGS_FILE=<file path>
```

For example:

```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /v  
SETTINGS_FILE=C:\Users\vmware\desktop\demo\agent-settings.txt
```

When the installation is complete, if the virtual machine has multiple NICs, configure the subnet that Horizon Agent uses. See [Configure a Virtual Machine with Multiple NICs for Horizon Agent](#).

Microsoft Windows Installer Command-Line Options

To install VMware Horizon 8 components silently, you must use Microsoft Windows Installer (MSI) command-line options and properties. The Horizon 8 component installers are MSI programs and use standard MSI features.

For details about MSI, see the Microsoft Web site. For MSI command-line options, see the Microsoft Developer Network (MSDN) Library Web site and search for MSI command-line options. To see MSI command-line usage, you can open a command prompt on the Horizon 8 component computer and type `msiexec /?`.

To run a Horizon 8 component installer silently, you begin by silencing the bootstrap program that extracts the installer into a temporary directory and starts an interactive installation.

At the command line, you must enter command-line options that control the installer's bootstrap program.

Table 3-4. Command-Line Options for a Horizon 8 Component's Bootstrap Program

Option	Description
/s	<p>Disables the bootstrap splash screen and extraction dialog, which prevents the display of interactive dialogs.</p> <p>For example: VMware-Horizon-Connection-Server-y.y.y-xxxxxx.exe /s</p> <p>The /s option is required to run a silent installation.</p>
/v" MSI_command_line_options"	<p>Instructs the installer to pass the double-quote-enclosed string that you enter at the command line as a set of options for MSI to interpret. You must enclose your command-line entries between double quotes. Place a double quote after the /v and at the end of the command line.</p> <p>For example: VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"command_line_options"</p> <p>To instruct the MSI installer to interpret a string that contains spaces, enclose the string in two sets of double quotes. For example, you might want to install the Horizon 8 component in an installation path name that contains spaces.</p> <p>For example: VMware-Horizon-Connection-Server-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"""</p> <p>In this example, the MSI installer passes on the installation-directory path and does not attempt to interpret the string as two command-line options. Note the final double quote that encloses the entire command line.</p> <p>The /v"command_line_options" option is required to run a silent installation.</p>

You control the remainder of a silent installation by passing command-line options and MSI property values to the MSI installer, `msiexec.exe`. The MSI installer includes the Horizon 8 component's installation code. The installer uses the values and options that you enter in the command line to interpret installation choices and setup options that are specific to the Horizon 8 component.

Table 3-5. MSI Command-Line Options and MSI Properties

MSI Option or Property	Description
/qn	<p>Instructs the MSI installer not to display the installer wizard pages.</p> <p>For example, you might want to install Horizon Agent silently and use only default setup options and features:</p> <p>VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn"</p> <p>Alternatively, you can use the /qb option to display a basic progress dialog box in a noninteractive, automated installation.</p> <p>The /qn or /qb option is required to run a silent installation.</p> <p>For information about additional /q parameters, see the Microsoft Dev Center website.</p>
INSTALLDIR	<p>Specifies an alternative installation path for the Horizon 8 component.</p> <p>Use the format <code>INSTALLDIR=path</code> to specify an installation path. You can ignore this MSI property if you want to install the Horizon 8 component in the default path.</p> <p>This MSI property is optional.</p>

Table 3-5. MSI Command-Line Options and MSI Properties (continued)

MSI Option or Property	Description
ADDLOCAL	<p>Determines the component-specific options to install.</p> <p>In an interactive installation, the Horizon 8 installer displays custom setup options that you can select or deselect. In a silent installation, you can use the <code>ADDLOCAL</code> property to selectively install individual setup options by specifying the options on the command line. Options that you do not explicitly specify are not installed.</p> <p>In both interactive and silent installations, the Horizon 8 installer automatically installs certain features. You cannot use <code>ADDLOCAL</code> to control whether or not to install these non-optional features.</p> <p>Type <code>ADDLOCAL=ALL</code> to install all custom setup options that can be installed during an interactive installation, including those that are installed by default and those that you must select to install, except NGVC. NGVC and SVI Agent are mutually exclusive.</p> <p>The following example installs Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and all features that are supported on the guest operating system: <code>VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</code></p> <p>If you do not use the <code>ADDLOCAL</code> property, the custom setup options that are installed by default and the automatically installed features are installed. Custom setup options that are off (unselected) by default are not installed.</p> <p>The following example installs Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and the on-by-default custom setup options that are supported on the guest operating system: <code>VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn</code></p> <p>To specify individual setup options, type a comma-separated list of setup option names. Do not use spaces between names. Use the format <code>ADDLOCAL=value,value,value...</code></p> <p>You must include <code>Core</code> when you use the <code>ADDLOCAL=value,value,value...</code> property.</p> <p>The following example installs Horizon Agent with the Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and Instant Clone Agent features:</p> <p><code>VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,NGVC</code></p> <p>The preceding example does not install other components, even those that are installed by default interactively.</p> <p>The <code>ADDLOCAL</code> MSI property is optional.</p>
REBOOT	<p>You can use the <code>REBOOT=ReallySuppress</code> option to allow system configuration tasks to complete before the system reboots.</p> <p>This MSI property is optional.</p>
REINSTALL	<p>You can use the <code>REINSTALL=ALL</code> option to install a Horizon Agent patch.</p> <p>The following example installs the patch:</p> <p><code>msiexec /p VMware-Horizon-Agent-x86_64-YYMM-y.y.y-xxxxxx.msp /qn</code> <code>REINSTALL=ALL</code></p> <p>This MSI property is optional.</p>

Table 3-5. MSI Command-Line Options and MSI Properties (continued)

MSI Option or Property	Description
REMOVE	<p>You can use the REMOVE=<value> option to remove a feature.</p> <p>The following example uninstalls the USB feature:</p> <pre>VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn REMOVE=USB"</pre> <p>This MSI property is optional.</p>
/l*v log_file	<p>Writes logging information into the specified log file with verbose output.</p> <p>For example: /l*v ""%TEMP%\vmmsi.log""</p> <p>This example generates a detailed log file that is similar to the log generated during an interactive installation.</p> <p>You can use this option to record custom features that might apply uniquely to your installation.</p> <p>You can use the recorded information to specify installation features in future silent installations.</p> <p>The /l*v option is optional.</p>

Silent Installation Properties for Horizon Agent

You can include specific properties when you silently install Horizon Agent from the command line. You must use a *PROPERTY=value* format so that Microsoft Windows Installer (MSI) can interpret the properties and values. A silent upgrade uses the same install commands. You can also modify already installed Horizon Agent components silently.

The following table shows the Horizon Agent silent installation properties that you can use at the command-line.

Table 3-6. MSI Properties for Silently Installing Horizon Agent

MSI Property	Description	Default Value
ENABLE_UNC_REDUCTION	<p>Specifies whether the UNC Path Redirection feature is installed. A value of 1 installs the feature. You must use group policy settings to configure which UNC's to redirect. See "Configuring UNC Path Redirection" in the <i>Horizon Remote Desktop Features and GPOs</i> document.</p> <p>This MSI property is optional.</p>	0
IGNORE_DOTNET_CHECK	<p>Determines whether the installer checks for a minimum .NET version. By default, when Horizon Performance Tracker is selected, the installer performs a pre-check to confirm that .NET 4.6.2 or later is installed, and stops the install process if it is not.</p> <p>A value of 1 cancels this pre-check. A value of 0 allows the pre-check to proceed.</p>	%ProgramFiles%\VMware\VMware View\Agent
INSTALLDIR	<p>Path and folder in which the Horizon Agent software is installed. For example:</p> <pre>INSTALLDIR=""D:\abc\my folder""</pre> <p>The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path.</p> <p>This MSI property is optional.</p>	

Table 3-6. MSI Properties for Silently Installing Horizon Agent (continued)

MSI Property	Description	Default Value
RDP_CHOICE	Determines whether to enable Remote Desktop Protocol (RDP) on the desktop. A value of 1 enables RDP. A value of 0 leaves the RDP setting deactivated. This MSI property is optional.	1
SUPPRESS_RUNONCE_CHECK	Ignores pending Windows Update tasks scheduled at the next operating system reboot in the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce and RunOnceEx keys. Using this flag allows concurrent installation but does not guarantee the installation outcome when the system updates affect the Horizon Agent run-time dependencies. This MSI property is optional.	None
URL_FILTERING_ENABLED	Specifies whether the URL Content Redirection feature is installed. A value of 1 installs the feature. You must use group policy settings to configure which URLs to redirect. See "Configuring URL Content Redirection" in the <i>Horizon Remote Desktop Features and GPOs</i> document. This MSI property is optional.	0
VDM_SKIP_BROKER_REGISTRATION	A value of 1 skips unmanaged desktops.	None
VDM_VC_MANAGED_AGENT	Determines whether vCenter Server manages the virtual machine on which Horizon Agent is installed. A value of 1 configures the desktop as a vCenter Server-managed virtual machine. A value of 0 configures the desktop as unmanaged by vCenter Server. This MSI property is required. Note The installer repair option is not supported for an unmanaged installation. Repairing such an installation results in an installation of a managed Horizon Agent.	None
VDM_SERVER_NAME	Host name or IP address of the Connection Server instance on which the Horizon Agent installer registers an unmanaged desktop. This property applies to unmanaged desktops only. For example: VDM_SERVER_NAME=10.123.01.01 This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops that are managed by vCenter Server.	None
VDM_SERVER_USERNAME	User name of the administrator on the Connection Server instance. This MSI property applies only to unmanaged desktops. For example: VDM_SERVER_USERNAME=domain\username This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops managed by vCenter Server.	None

Table 3-6. MSI Properties for Silently Installing Horizon Agent (continued)

MSI Property	Description	Default Value
VDM_SERVER_PASSWORD	Connection Server administrator user password. For example: VDM_SERVER_PASSWORD=secret This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops that are managed by vCenter Server.	None
VDM_IP_PROTOCOL_USAGE	Specifies the IP version that Horizon Agent uses. Valid values are IPv4 and IPv6.	IPv4
VDM_FIPS_ENABLED	Specifies whether to enable or disable FIPS mode. A value of 1 enables FIPS mode. A value of 0 disables FIPS mode. If this property is set to 1 and Windows is not in FIPS mode, the installer will stop.	0
VDM_FORCE_DESKTOP_AGENT	If you install Horizon Agent on a Windows Server machine and configure it as a single-user Horizon desktop rather than as an RDS host, set the value to 1. This requirement applies to machines managed by vCenter Server and unmanaged machines. For non-server Windows guests that host application sessions, set the value to 0. This MSI property is optional.	0

In a silent installation command, you can use the `ADDLOCAL` property to specify options that the Horizon Agent installer configures.

The following table shows the Horizon Agent options that you can enter at the command line. These options have corresponding setup options that you can deselect or select during an interactive installation.

When you do not use the `ADDLOCAL` property at the command line, Horizon Agent installs all of the options that are installed by default during an interactive installation, if they are supported on the guest operating system. When you use `ADDLOCAL=ALL`, Horizon Agent installs all of the following options, both on-by-default and off-by-default, if they are supported on the guest operating system.

For more information, see the `ADDLOCAL` table entry in [Microsoft Windows Installer Command-Line Options](#).

If you use `ADDLOCAL` to specify features individually (you do not specify `ADDLOCAL=ALL`), you must always specify `Core`.

You can modify features by using the `ADDLOCAL` and `REMOVE` MSI properties. Use the following PowerShell command to query the registry of installed components on the system where Horizon Agent is installed for the `ModifyPath` base command line:

```
Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* |
    Select-Object DisplayName, ModifyPath | Where-Object {$_.DisplayName -eq 'VMware
Horizon
    Agent'} | Format-Table -AutoSize
```

The output:

DisplayName	ModifyPath
VMware Horizon Agent	MsiExec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111}

The following example modifies and removes the USB component from an existing installation:

```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn REMOVE=USB"
```

The following example modifies the agent installation by replacing Horizon Performance

Tracker with the Horizon Help Desk Tool: VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=HelpDesk REMOVE=PerfTracker"

The following example modifies the agent installation by adding serial port

and scanner redirection: VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=SerialPortRedirection,ScannerRedirection"

Table 3-7. Horizon Agent Silent Installation Options and Interactive Custom Setup Options

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When ADDLOCAL Is Not Used
Core	The core Horizon Agent functions. If you specify ADDLOCAL=ALL, the Core features are installed.	Yes
PCoIP	PCoIP Protocol Agent	Yes
USB	USB Redirection	No
NGVC	Instant Clone Agent	No
RTAV	Real-Time Audio-Video	Yes
ClientDriveRedirection	Client Drive Redirection	Yes
SerialPortRedirection	Serial Port Redirection	No
ScannerRedirection	Scanner Redirection	No
GEOREDIR	Geolocation Redirection	No
V4V	Horizon Monitoring Service Agent	Yes
SmartCard	Smartcard This feature is not installed by default in an interactive installation.	No
VmwVaudio	VMware Audio (virtual audio driver)	Yes

Table 3-7. Horizon Agent Silent Installation Options and Interactive Custom Setup Options (continued)

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When ADDLOCAL Is Not Used
VmWVidd	VMware Indirect Display Driver	<p>Yes</p> <p>Note VmWVidd is installed and marked as Local in the registry only if:</p> <ul style="list-style-type: none"> ■ Desktop Mode Windows Server is RS4 and above (OS build 17134 - version 1803), or ■ Server is 19H1 and above (OS build 18362 - version 1903) <p>VmWVidd is installed and set as <code>Absent</code> in the registry in Windows Server 2019 (version 1809) std and datacenter with the RDS role.</p> <p>VmWVidd will be installed and set as <code>Local</code> in the registry in Windows Server 2022 with the RDS role.</p>
TSMMR	Windows Media Multimedia Redirection (MMR)	Yes
RDP	Enables RDP in the registry if you use the <code>RDP_CHOICE=1</code> property on the command line or select RDP as the default display protocol when you create or edit a desktop pool. This feature is hidden during interactive installations.	Yes
VMWMediaProviderProxy	VMware Virtualization Pack for Skype for Business	No
RDSH3D	3D rendering on RDS hosts	No
BlastUDP	UDP Transport support for Blast	Yes
SdoSensor	SDO Sensor Redirection	No
PerfTracker	Horizon Performance Tracker	No
HelpDesk	Horizon Help Desk Tool	Yes
PrintRedir	VMware Integrated Printing	Yes
PSG	This feature sets a registry entry that tells Connection Server whether Horizon Agent is using IPv4 or IPv6.	Yes

Install or Uninstall a Horizon Agent Patch Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install and uninstall a Horizon Agent patch. In a silent installation, you use the command line and do not have to respond to wizard prompts.

Prerequisites

- Verify that you have administrative rights on the virtual machine or physical PC.
- Download the Horizon Agent Update Patch installer file from the VMware product page at <http://www.vmware.com/go/downloadview>.

The installer filename is `VMware-Horizon-Agent-x86_64-YYMM-y.y.y-xxxxxx.msp`, where `YYMM` is the marketing version number, `y.y.y` is the internal version number, and `xxxxxx` is the build number.

Procedure

- 1 Open a Windows command prompt as administrator on the virtual machine or physical PC.

- 2 To install a Horizon Agent patch where Horizon Agent is installed, run the .msp file:

```
msiexec /p VMware-Horizon-Agent-x86_64-YYMM-y.y.y-xxxxxx.msp /qn REINSTALL=ALL"
```

After installing the patch, verify the patch build number is updated in the registry: `HKLM:\SOFTWARE\WOW6432Node\VMware, Inc.\AgentVersions!view-agent` and `HKLM:\SOFTWARE\VMware, Inc.\Vmware VDM!BuildNumber`.

- 3 To uninstall a Horizon Agent patch where Horizon Agent is installed, run a PowerShell script:

```
remove-patch.ps1
```

ProductCode-driven command line example: `msiexec /package {product_code} /uninstall {patch_guid} /passive`

After uninstalling the patch, check the registry: `HKLM:\SOFTWARE\WOW6432Node\VMware, Inc.\AgentVersions!view-agent` and `HKLM:\SOFTWARE\VMware, Inc.\Vmware VDM!BuildNumber` that no reference of the patch exists. Verify the services are in the same state as they were before uninstalling the patch.

Configure a Virtual Machine with Multiple NICs for Horizon Agent

When you install Horizon Agent on a virtual machine that has more than one NIC, you must configure the subnet that Horizon Agent uses. The subnet determines which network address Horizon Agent provides to the Connection Server instance for client protocol connections.

Procedure

- ◆ On the virtual machine on which Horizon Agent is installed, open a command prompt, type *regedit.exe* and create a registry entry to configure the subnet.

For example, in an IPv4 network: **HKLM\Software\VMware, Inc.\VMware VDM\IpPrefix = *n.n.n.n/m* (REG_SZ)**

In this example, *n.n.n.n* is the TCP/IP subnet and *m* is the number of bits in the subnet mask.

Note In releases earlier than Horizon 8 6 version 6.1, this registry path was **HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = *n.n.n.n/m* (REG_SZ)**. The old registry setting is not used with View Agent 6.1 or later. If you upgrade View Agent from an earlier release to version 6.1 or later, make sure to use the current registry setting.

Preparing a Golden Image Virtual Machine for Instant-Clones

To deploy an instant-clone desktop pool, you must first prepare a golden image virtual machine in vCenter Server.

■ [Configure a Golden Image Virtual Machine](#)

After creating a virtual machine that you plan to use as a golden image, configure the Windows environment.

■ [Activating Windows on Instant Clones](#)

To make sure that Windows 10 and Windows Server clones are properly activated when the clones are created, you must use Microsoft volume activation on the golden image virtual machine. The volume-activation technology requires a volume license key.

■ [Disable Windows Hibernation in the Golden Image](#)

The Windows hibernation feature creates a hidden system file, *Hiberfil.sys* and uses this file to store information that is needed for hybrid sleep. Disabling hibernation reduces the size of an instant clone's virtual disk.

■ [Choosing ClonePrep or Sysprep for Customizing Your Virtual Desktops](#)

There are two options for customizing instant clone virtual machines: VMware ClonePrep or Microsoft Sysprep.

■ [Increase the Timeout Limit for ClonePrep Customization Scripts](#)

ClonePrep post-synchronization or power-off scripts have a timeout limit of 20 seconds. You can increase this limit by changing the *ExecScriptTimeout* Windows registry value on the golden image virtual machine.

■ Compute Profiles and Golden Image

The VMware Horizon 8 compute profile feature significantly improves golden image management and reduces the number of golden images required to create desktop pools for different requirements.

Configure a Golden Image Virtual Machine

After creating a virtual machine that you plan to use as a golden image, configure the Windows environment.

Prerequisites

- Verify that you prepared a virtual machine to use for deploying remote desktops. See [Creating a Virtual Machine for Cloning](#).

The golden image can either belong to the same Active Directory domain as the domain that the desktop machines will join or be a member of a workgroup.

- Verify that the virtual machine was not converted from an instant clone.

Important You also cannot use an instant clone as a golden image.

- When you install Horizon Agent on the golden image, verify that the **VMware Horizon Instant Clone Agent** option for instant clones is selected. See [Install Horizon Agent on a Virtual Machine](#).
- To deploy Windows machines, configure a volume license key and activate the golden image virtual machine's operating system with volume activation. See [Activating Windows on Instant Clones](#).
- Verify that you followed the best practices for optimizing the operating system. See [Optimize Guest Operating System Performance](#).
- Familiarize yourself with the procedure for disabling searching Windows Update for device drivers. See the Microsoft Technet article, "Disable Searching Windows Update for Device Drivers" at [http://technet.microsoft.com/en-us/library/cc730606\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx).

Procedure

- ◆ Verify that the system disk contains a single volume.
- ◆ Verify that the virtual machine does not contain an independent disk. However, the golden image virtual machine can contain multiple disks.

An independent disk is excluded when you take a snapshot of the virtual machine. Clones are based on a snapshot and therefore will not contain the independent disk.

- ◆ Disable the hibernation option to reduce the size of each clone's virtual disk.

- ◆ Before you take a snapshot of the golden image, disable searching Windows Update for device drivers.

This Windows feature can interfere with the customization process. As each clone is customized, Windows might search for the best drivers on the Internet for that clone, resulting in delays.

- ◆ In vSphere Client, disable the vApp Options setting on the golden image virtual machine.
- ◆ On Windows Server 2012 R2 machines, disable the scheduled maintenance task that recovers disk space by removing unused features.

For example: `Schtasks.exe /change /disable /tn
"\Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup"`

- ◆ Disable the HotPlug capability on removable devices. See [KB 1012225](#).

What to do next

Use vSphere Client to take a snapshot of the golden image virtual machine in its powered-down state. This snapshot is provides the base image for the clones.

Important Before you take a snapshot, shut down the golden image virtual machine.

Activating Windows on Instant Clones

To make sure that Windows 10 and Windows Server clones are properly activated when the clones are created, you must use Microsoft volume activation on the golden image virtual machine. The volume-activation technology requires a volume license key.

To activate Windows with volume activation, you use Key Management Service (KMS), which requires a KMS license key. See your Microsoft dealer to acquire a volume license key and configure volume activation.

Note Multiple Activation Key (MAK) licensing is not supported. Active Directory-based activation is not supported.

Before you create an instant-clone desktop pool, you must use volume activation to activate Windows on the golden image.

The following steps describe how activation takes place:

- 1 Invoke a script to remove the existing license. For more information, see the Microsoft Windows documentation to remove the Windows license key using a command.
- 2 Restart Windows.
- 3 Invoke a script that uses KMS licensing to activate Windows.

KMS treats each activated clone as a computer with a newly issued license.

Disable Windows Hibernation in the Golden Image

The Windows hibernation feature creates a hidden system file, `Hiberfil.sys` and uses this file to store information that is needed for hybrid sleep. Disabling hibernation reduces the size of an instant clone's virtual disk.

Caution When you make hibernation unavailable, hybrid sleep does not work. Users can lose data if a power loss occurs.

Procedure

- 1 In vSphere Client, select the golden image virtual machine and select **Open Console**.
- 2 Log in as an administrator.
- 3 Disable the hibernation option.
 - a Click **Start** and type `cmd` in the **Start Search** box.
 - b In the search results list, right-click **Command Prompt** and click **Run as Administrator**.
 - c At the **User Account Control** prompt, click **Continue**.
 - d At the command prompt, type `powercfg.exe /hibernate off` and press Enter.
 - e Type `exit` and press Enter.

Choosing ClonePrep or Sysprep for Customizing Your Virtual Desktops

There are two options for customizing instant clone virtual machines: VMware ClonePrep or Microsoft Sysprep.

ClonePrep is a VMware customization process run during instant clone deployment to personalize each desktop clone created from the parent image. During the initial startup of each desktop, ClonePrep:

- Creates a new computer account in Active Directory for each desktop.
- Gives the instant clone desktop a new name.
- Joins the desktop to the appropriate domain.

Sysprep is a Microsoft tool to deploy the configured operation system installation from a base image. The desktop can then be customized based on an answer script. Sysprep can modify a larger number of configurable parameters than ClonePrep, but ClonePrep is significantly faster. Majority of instant clone customers choose ClonePrep

The following table lists the main differences between ClonePrep and Sysprep:

Function	ClonePrep	Sysprep
Removing local accounts	No	Yes
Changing Security Identifiers (SID)	No	Yes

Function	ClonePrep	Sysprep
Removing parent from domain	No	Yes
Changing computer name	Yes	Yes
Joining the new instance to the domain	Yes	Yes
Generating new SID	No	Yes
Language, regional settings, date, and time customization	No	Yes
Number of reboots	0	2
Requires configuration file and Sysprep	No	Yes
KMS license activation	Yes	No (performed by Agent)
Post customization script, pre-shutdown script	Yes	No

It is recommended that you use ClonePrep unless there are specific Sysprep capabilities required for your environment.

For instant clones and ClonePrep, the table below shows the effect of various operations on SIDs.

	Creation	Push Image	On User Logout
ClonePrep	Parent Image's SID are used for the desktops	SIDs are preserved unless parent image is changed	SIDs are preserved unless parent image is changed

Increase the Timeout Limit for ClonePrep Customization Scripts

ClonePrep post-synchronization or power-off scripts have a timeout limit of 20 seconds. You can increase this limit by changing the `ExecScriptTimeout` Windows registry value on the golden image virtual machine.

Instead of increasing the timeout limit you can also use your customization script to launch another script or process that performs the long-running task.

Note Some ClonePrep customization scripts can finish running within the 20-second limit. Test your scripts before you increase the limit.

Procedure

- 1 On the golden image virtual machine, start the Windows Registry Editor.

- a Select **Start > Command Prompt**.
- b At the command prompt, type **regedit**.

- 2 In the Windows registry, locate the `vmware-viewcomposer-ga` registry key.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vmware-viewcomposer-ga
```

3 Click **Edit** and modify the registry value.

```
Value Name: ExecScriptTimeout
Value Type: REG_DWORD
Value unit: milliseconds
```

The default value is 20000 milliseconds.

Compute Profiles and Golden Image

The VMware Horizon 8 compute profile feature significantly improves golden image management and reduces the number of golden images required to create desktop pools for different requirements.

Please refer to [Instant Clone Desktop Pools](#) to learn more about this feature.

Creating Customization Specifications When Using Sysprep for Desktop Customization

When you customize a clone using Sysprep, you need to provide a customization specification.

You create customization specifications by using the Customization Specification wizard in vSphere. See the *vSphere Virtual Machine Administration* document for information on using the Customization Specification wizard.

It is recommended that you test a customization specification in vSphere before you use it to create a desktop pool.

Note the following requirements and limitations:

- Windows is the only supported operating system for Instant Clone desktops with Sysprep customization.
- Linux is not supported as the target guest operating system.
- When you use a Sysprep customization specification to join a Windows desktop to a domain, you must use the fully qualified domain name (FQDN) of the Active Directory domain. You cannot use the NetBIOS name.
- Using a custom Sysprep answer file is not supported.
- On the **Computer Name** page of the wizard, the **Use the virtual machine name** option must be selected.
- The **Automatically logon as Administrator** option is not supported. If you select this option during the customization process, the system ignores the setting.
- Only single NIC configurations are supported.
- Entering FQDN and AD domain credentials different from those configured for the pool is not supported. If you enter these values, the system ignores them and joins the domain configured for the pool.

- If any explicit DNS server setup is required for the domain join, you must select **Manually Select custom settings** on the **Network** page and enter the settings.

Creating Virtual Machine Templates for Full-Clone Virtual Desktops

You must create a virtual machine template before you can create an automated pool that contains full-clone virtual machines.

A virtual machine template is a main copy of a virtual machine that can be used to create and provision new virtual machines. Typically, a template includes an installed guest operating system and a set of applications.

You create virtual machine templates in vSphere Client. You can create a virtual machine template from a previously configured virtual machine, or you can convert a previously configured virtual machine to a virtual machine template.

See the *vSphere Basic System Administration* guide for information on using vSphere Client to create virtual machine templates. See [Chapter 5 Creating and Managing Automated Full-Clone Desktop Pools](#) for information on creating automated pools.

Note A virtual machine template is not for creating an instant-clone desktop pool.

Using VMware Horizon Recording

The VMware Horizon Recording feature allows administrators to record desktop and application sessions to monitor user behavior for Windows remote desktops and applications.

Administrators can observe a user's exact keystrokes, cursor and mouse activity, and other user behavior in a recorded desktop or application session. In addition to providing greater security and auditing for user behavior, recording also helps with troubleshooting and reproducing issues the user experiences during a session. Administrators can play back, store, and audit the recordings.

When a user logs on, Horizon Recording starts automatically, displaying the default message **Your session is being recorded in accordance with security policies**. The recording runs as long as the session is in a connected state. Recording stops when the user logs out or disconnects. If the user changes the screen resolution of the desktop or application session, Horizon Recording creates a new segment of the recording. Recording file sizes vary based on the duration of the connected session. Recordings are stored in MP4 format and can be downloaded to play in a local player or viewed in the Horizon Recording web console.

Components

Horizon Recording consists of the following components:

- **Horizon Recording Server:** Collects information about the session as well as raw recording data for storage and playback.

- **Horizon Recording Agent:** Records a user session, registers the session with the Horizon Recording Server, and uploads recording data.

These components are available for VMware Horizon 8 2106 and later. The installation file is available on VMware Customer Connect.

Note Like certain other Horizon 8 features, this feature is not available for every subscription. For more information, see [VMware Horizon Subscription Feature comparison](#).

Web Interface

After you have installed the Horizon Recording Server (see below), you can access the Horizon Recording web console, which displays the following:

- **Dashboard** includes a list of recent recordings, the server, database, and folder where recordings are stored, as well as recording information such as start time, duration, size, and state. You can lock, unlock, and delete recordings.
- **Recordings** includes a list of all recordings with information such as name, launched resource, location, start and end dates, start time, duration, size, and state. You can lock, unlock, and delete recordings.
- **Audit Trail** tracks all user actions in the user interface.

Install the Horizon Recording Server

Install the Horizon Recording Server component on a machine to collect information about the session as well as raw recording data for storage and playback.

The Horizon Recording Server component consists of these items:

- A database for session information storage and configuration
- A Windows NTFS folder for recording storage
- A web service for collecting recording data, administration, and playback

You can deploy the Horizon Recording Server as a standalone setup where the server is installed on a machine that leverages a local SQLite database stored in the installation directory as `local.db` and a local NTFS folder.

You can also deploy the Horizon Recording Server in a high availability environment using multiple servers behind a load balancer, leveraging Microsoft SQL or PostgreSQL databases, as well as a shared NTFS folder on all servers for storing recording data. Load balancers configured with L4 load distribution are supported.

Minimum Server Resource Requirements (required to support 2,000 active recordings)

Resource	Minimum Value
CPU	4 vCPU
Memory	8 GB
Free Disk Space	20 GB
	Note This depends on the type of applications the user runs in the session and also the frame change rate. You must monitor usage and add extra disk space as required.

Note The Horizon Recording Server is built in .Net Core and requires a 64-bit Windows Server operating system that is a member of the domain if you use group extraction. The server operating system must be Windows Server 2016 or later (64-bit).

To install the Horizon Recording Server, perform the following steps.

- 1 Download the `HorizonRecordingServer.exe` file and copy it to a local folder on the server.
- 2 Run the installer and follow the steps. Default credentials are shown below.

Username/Password: **administrator/Recording123**

The server is now available on `https://<localservername>:9443`

- 3 Manually secure the recordings folder permissions so that only the recording server's active directory accounts have access to the folder to add, modify, or delete recordings.

- To uninstall the Horizon Recording Server, use Add Remove Programs (`appwiz.cpl`) to remove the Horizon Recording server binaries and then delete the following components manually:

- The local database file (`local.db`) in installation directory
- The logs located in `C:\programdata\VMware\Horizon Recording`
- Local recordings located in `installation directory\Recordings`

- To reset the installation:

- a Stop the Horizon Recording service.
- b Delete the Recordings folder from the installation directory.
- c Delete the `servicesettings.json` file and the `local.db` file from the installation directory.
- d Start the Horizon Recording service.

The `servicesettings.json` and `local.db` files are recreated afresh.

Install the Horizon Recording Agent

Install the Horizon Recording Agent component on all Horizon machines where you want to record sessions.

The Horizon Recording Agent registry settings are stored in

HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Recording Agent

Minimum Resource Requirements

Resource	Minimum Value (VDI)	Minimum Value (RDSH - 80 sessions)
CPU	2 vCPU	64 vCPU
Memory	2 GB	64 GB
Free Disk Space	5 GB	50 GB
	Note This depends on the type of applications the user runs in the session and the frame change rate. You must monitor usage and add extra disk space as required.	Note This depends on the type of applications the user runs in the session and the frame change rate. You must monitor usage and add extra disk space as required.

Additional System Requirements

- Horizon 8 2106 or later for VDI; Horizon 8 2111 or later for RDSH
- Instant Clone Agent or Full Clone Agent
- Windows 10 1909 or later 64-bit operating system for VDI; Windows Server 2016 or later 64-bit operating system for RDSH
- Microsoft .Net framework 4.6.1 or later
- VMware Blast
- Port 9443 allowed in the firewall inbound rules on the Horizon Recording Server

To install the Horizon Recording Agent, perform the following steps.

- 1 Download the `HorizonRecordingAgent.exe` file and copy it to a local folder.
- 2 Run the installer and follow the steps.
- 3 When prompted for the connection, provide the correct URL of the recording server in the format `https://<FQDN or IP address of recording server>:9443` along with the User Name and Password.
 - a Select the **This machine is a template** check box if the machine is a parent VM and a pool will be created from it.
 - b Click **Register**.
 - c If the certificate of the server is untrusted, accept the thumbprint of the server when prompted.
- To uninstall the Horizon Recording Agent, use Add Remove Programs (`appwiz.cpl`) to remove the Horizon Recording agent binaries and then delete the following components manually:
 - Logs located in `C:\programdata\VMware\Horizon Recording`

- Any local pending recordings located in `installation directory\Recordings`
- To delete the agents from the registered machines:
 - a In **Administrator > Manage Agents**.
 - b Select the Name of the agent and then click **Delete**.
 - c Read the confirmation message carefully and proceed with the deletion.

Upgrade the Horizon Recording Server

Before upgrading the Horizon Recording Server, do the following:

- Confirm that there are no active recordings.
- Create a backup of the Recordings folder, the `servicesettings.json` file, and the `local.db` (if you are using SQLite for the database).

To upgrade the Horizon Recording Server, perform the following steps.

- 1 Download the `HorizonRecordingServer.exe` file.
- 2 Copy the `HorizonRecordingServer.exe` file to a local folder on the server.
- 3 Run `HorizonRecordingServer.exe`.

Note the following:

- By default, the server is upgraded in the same `C:\Program Files\VMware\Desktop Recording Server` folder.
 - If you change the upgrade location to a new folder, the configuration is not retained, and is treated as a fresh installation. As a result, you cannot access or play back the old recordings from the web console after the upgrade.
 - If you do not change the default location, then all the configurations are retained, and you can access and play back the recordings from the web console after the upgrade.
- After the upgrade, the log location for the server changes to a new `C:\ProgramData\VMware\Horizon Recording` folder. The old logs are still available in `C:\ProgramData\VMware\Horizon Desktop Recording`.

Upgrade the Horizon Recording Agent

Before upgrading the Horizon Recording Agent, confirm that there are no active recordings on the agent.

Note It is recommended to upgrade the server before upgrading the agent.

To upgrade the Horizon Recording Agent, perform the following steps.

- 1 Download the `HorizonRecordingAgent.exe` file.
- 2 Copy the `HorizonRecordingAgent.exe` file to a local folder on the agent.

3 Run `HorizonRecordingAgent.exe`.

Note the following:

- By default, the agent is upgraded in the same `C:\Program Files\VMware\Desktop Recording Agent` folder.

If you change the upgrade location to a new folder, then the configuration is not retained, and is treated as a fresh installation.
- The Horizon Recording Server address is auto-populated during the upgrade procedure.
- After the agent is upgraded, the log location of the agent is changed to a new `C:\ProgramData\VMware\Horizon Recording` folder. The old logs are still available in `C:\ProgramData\VMware\Horizon Desktop Recording`.

Horizon Recording Settings

This topic describes settings for the VMware Horizon Recording feature.

Horizon Recording Settings in the Web Interface

In **Administrator > Manage Agents**, you can see the details of the machines that are registered with this instance of the recording server.

In **Administrator > Service Settings**, you can change the authentication, client, and server settings for the recording application, as well as recording criteria.

The following credentials are stored in the database. By default, the administrator has full control of the service settings, while the viewer can only find, watch, and download recordings.

Username/Password: **administrator/Recording123**

Username/Password: **viewer/Recording456**

You can select a user and change these passwords in **Authentication Settings**:

Authentication Settings	Description
LDAPS Integration	Disable or enable LDAPS integration. If enabled, enter the following information: <ul style="list-style-type: none"> ■ LDAPS URL ■ Bind User DN ■ Bind User Password ■ Search Base ■ Administrative Group DN ■ Viewer User Group DN ■ User Search Filter ■ Group Search Filter
Local Users	Select a user and click Change Password to change the password for that user.

Under **Client Settings**, the following settings affect the behavior of the Horizon Recording Agent:

Client Settings	Description
Notification Message	Message displayed to the user when their session is being recorded.
Split Recordings by Duration	Enable/Disable
Maximum Recording Duration	<p>The maximum duration of a recording before it is stopped and a new recording is started (in minutes). Minimum value is 30; maximum value is 600.</p> <p>Note This setting appears only when the Split Recordings by Duration option is enabled.</p>
Chunk size	The buffer size on the Horizon Recording Agent for each recording screen. When this buffer is filled, the data is submitted to the Horizon Recording Server.
Upload Interval	The length of time an active recording chunk will be uploaded to the server if the buffer has not yet filled. For example, if the interval is set to 5 minutes and the buffer has yet to fill, when this timespan has elapsed, the current recording screen data is uploaded to the server and a new chunk is created. This setting ensures a smaller window for missed recordings if the Horizon Recording Agent encounters a failure.

Under **Recording Criteria**, the following settings dictate the session types that are recorded:

Recording Criteria	Description
Record Local Sessions	Instructs the Horizon Recording Agent to record all sessions that are brokered from internal connection servers on the LAN.
Record Remote Sessions	Instructs Horizon Recording Agent to record all sessions that are brokered via a Unified Access Gateway.
Groups to record	Lists specific groups of users to be recorded using the session type recording criteria. If you do not add a group, all users will be evaluated for recording.

Under **Local Server Settings**, the following settings affect the local server currently connected to the database. To change local server settings, use the **Edit Deployment** wizard (see below).

Local Server Settings	Description
Database Connection Type	<p>This local server setting is read from the <code>servicesettings.json</code> file on the local server. Supported database types are:</p> <ul style="list-style-type: none"> ■ SQLite (local file) ■ MSSQL (Microsoft SQL) - Must be the same version of MSSQL database that is being used as the Connection Server Event database. ■ PostgreSQL - Must be the same version of PostgreSQL database that is being used as the Connection Server Event database.
Database Connection String	Identifies the server instance and database connection. Example: <code>Data Source=Local.db</code>

Under **Cluster Settings**, the following settings affect all the servers connected to the database. To change cluster storage location, use the **Edit Deployment** wizard (see below).

Cluster Settings	Description
Recording Storage Folder	File path of the folder in which the Horizon Recording Server stores active recording data or finished recordings. Location of this folder depends on the deployment type: NTFS Share or Local. This folder must be secured manually.
Encrypt Recordings	<p>Enable/Disable</p> <p>Note Enabling this will encrypt the recordings before storing them on the file system. The recordings on the file system cannot be played because they are encrypted and in .bin format. Only the admin user that can log on to the web console should be able to view and play them, because they are not decrypted until the moment when playback is requested from the web console.</p>
Conversion Chunk Size	Buffer size used to convert active recordings to finished recordings. The default value is 10.
Conversion Thread Count	The number of threads dedicated to converting finished raw recordings to MP4/binary format. Please do not change this value unless instructed to do so.
Conversion Wait Time	Amount of time a pending recording conversion has to wait before attempting to convert the files from active to finished. The default value is 10 minutes.
Raw Files	<p>This setting affects both the Horizon Recording Agent and the Horizon Recording Server.</p> <ul style="list-style-type: none"> ■ Horizon Recording Agent: instructs the agent to delete the recording when it has uploaded the data to the server successfully. ■ Horizon Recording Server: instructs the server to retain the raw files post conversion to MP4. <p>This setting is enabled by default. Disabling this setting compromises the security of the files.</p>
Retention Settings	Number of days a recording is retained on the server, after which the web service deletes the recordings. Locked recordings are excluded from the retention rules and remain on the server.

The SSL certificate used by the Horizon Recording Server is retrieved from the local machine's certificate store. It has a friendly name and a private key. If the SSL certificate does not exist, it is created on service startup. To install a custom certificate, rename the existing certificate to **HorizonRecordingServer** and install the certificate to the machine store. Restart the Horizon Recording Server service for the changes to take effect.

Note The SSL certificate must be trusted by the Horizon Recording Agent; otherwise the trusted thumbprints you added during installation will not contain the new certificate's thumbprint.

You can configure additional settings, such as the JWT token timeout and the SSL/TLS port, in the `servicesettings.json` file in the installation directory. You must stop the service before modifying this file and these settings only affect the server you modify. These settings must match on all recording servers participating in the cluster.

```
{
  "HTTPSPort": 9443,
  "DBConnectionString": "GlmrgliM0TpWt5nbC1RQyjoG]
  "JWTTokenLifeSpan": 60,
  "DBType": 1,
  "ConnectionStringIsEncrypted": true
}
```

Edit Deployment Wizard

You can modify Horizon Recording Server settings with the **Edit Deployment** wizard.

Modifying Horizon Recording Server settings affect both the local server settings, such as the database connection, and the cluster's storage location. After the wizard completes, the local web service is restarted to update the database. Any changes to the storage location affect all servers in the cluster immediately.

Note Data is never migrated when modifying the deployment. Only the service configuration and user authentication details are migrated. Make sure to back up all recordings in the database by downloading the recordings, then deleting the sessions in advance to avoid having unwanted data.

Also note the following:

- In a standalone mode, you can only modify the local server's database connection if there are no active sessions in progress.
- You can select the database type and connection string. These settings are encrypted and stored in the `servicesettings.json` file in the server installation directory. If the user specified in the connection string has permissions to create the database, the web service will create a database. Otherwise, pre-create an empty database with the desired name and verify that the account provided has the ability to create the required tables.
- The account must have the ability to make database layout changes for future upgrades where the database schema may change, and the web service will automatically perform the migrations.
- The web service will be restarted after the database has been instantiated and the local users and settings have been migrated.
- Modifying the cluster's storage location immediately affects all servers in the cluster. Do not modify the storage location when there are active recordings occurring. Data is not migrated when modifying the storage location.

Logging

By default, the Horizon Recording Server and Horizon Recording Agent logs are in `C:\programdata\VMware\Horizon Recording`.

To troubleshoot any issues, you can extend the logging by modifying the `NLog.config` file. Changing the minlevel to Debug or Trace increases the size of the log files.

```
<rules>
/logger name="*" minlevel="Trace" writeTo="WebServiceLogging" />
</rules>
```

Creating and Managing Instant-Clone Desktop Pools

4

To provide users access to instant-clone desktops, you must create an instant-clone desktop pool.

This chapter includes the following topics:

- [Instant Clone Desktop Pools](#)
- [Instant Clone Image Publishing and Creation Workflow](#)
- [Worksheet for Creating an Instant-Clone Desktop Pool](#)
- [Create an Instant-Clone Desktop Pool](#)
- [Forensics Select Hold for Dedicated and Floating Instant Clone Desktops](#)
- [Configure Instant Clones with vSphere Virtual Machine Encryption](#)
- [Guest Customization for Instant Clones in VMware Horizon](#)
- [Enabling VBS and vTPM for an Instant-Clone Desktop Pool](#)
- [Configuring 3D Rendering Options for Instant-Clone Pools](#)
- [Configure Number of Monitors and Screen Resolution](#)
- [Allow Reuse of Existing Computer Accounts](#)
- [Manually Customizing Machines](#)
- [Patching an Instant-Clone Desktop Pool](#)
- [Monitor a Push-Image Operation](#)
- [Reschedule or Cancel a Push-Image Operation](#)
- [Perform Maintenance on Instant-Clone Hosts](#)
- [Instant-Clone Maintenance Utilities](#)

Instant Clone Desktop Pools

An instant clone desktop pool is an automated desktop pool created from a golden image using the vmFork technology (called the instant clone API) in vCenter Server.

Instant clone replaces View Composer linked clone as the process for creating non-persistent desktops in Horizon 8. In addition to using the instant clone API from vCenter Server, Horizon 8 also creates several types of internal VMs (Internal Template, Replica VM, and Parent VM) to manage these clones in a more scalable way.

Instant clones share the virtual disk of the parent VM and consume less storage than full VMs. In addition, instant clones share the memory of the parent VM when they are first created, which contributes to fast provisioning. As users log into these cloned desktops, additional memory is consumed.

While the use of a parent VM is helpful in improving the provisioning speed, it does increase the memory requirement across the cluster. In some cases when the benefit of having more memory outweighs the increase in provisioning speed, Horizon 8 automatically chooses to provision instant clones directly from a replica VM without creating any parent VM. This feature is called Smart Provisioning. A single instant clone pool can have instant clones that are created with or without parent VMs.

Computer-based group policy objects (GPOs) that require a reboot on the golden image VM do not apply to instant clones because instant clones are created in a powered-on state. To apply the golden image VM GPOs to instant clones, see [Applying Computer-based GPOs that Require Reboot on Instant Clones](#) below.

Instant clone desktop pools have the following benefits:

- The provisioning of instant clones is fast.
- Instant clones are always created in a powered-on state, ready for users to connect. Guest customization and joining the Active Directory domain are completed as part of the initial power-on workflow.
- You can patch a pool of instant clones in a rolling process with zero downtime.

Compute Profiles for Instant Clone Desktop Pools

A compute profile of an instant clone desktop pool is the number of vCPUs and vRAM allocated to each desktop in a pool. When creating an instant clone desktop pool, the administrator must specify the golden image and snapshot, as described in the [Worksheet for Creating an Instant-Clone Desktop Pool](#). By default, Horizon 8 inherits the compute profile of the selected snapshot to create the desktop pool. Previously, if an administrator wanted to create two different pools of instant clone virtual desktops that use the same OS image but have different VM compute profiles, they had to create and maintain two golden images or two snapshots. This complicates the management of images and makes patch updates more time-consuming. With the compute profile feature, administrators can override the default compute profile and specify the desired vCPU, vRAM, and cores per socket to create the desktop pool. In this way, the same golden image and snapshot can be used to create multiple desktop pools where each pool has a different VM compute profile.

Administrators can change the compute profile for a pool during one of the following workflows:

- [Create an Instant-Clone Desktop Pool](#)

- [Patching an Instant-Clone Desktop Pool](#)
- [Selective Patching](#)

Applying Computer-based GPOs that Require Reboot on Instant Clones

Some computer-based GPOs are processed at Windows startup and typically require a reboot for them to be applied to the desktop. To apply these GPOs properly to instant clones, follow these steps:

- 1 Create or update the computer-based policy settings in the target OU for the instant-clone desktops.
- 2 Take a new snapshot of the existing parent VM (or create a new parent VM) in vCenter Server. Even if nothing has changed on the parent VM, this will publish a new base image for the clones, which then receive the GPOs created in the previous step.
- 3 In the administration console, push a new image to update the existing pool (or create a new pool) of instant clones using the parent VM in vCenter Server and the new snapshot created in the previous step. The GPOs are then applied to the instant clones.

Note the following:

- Changes to foreground GPOs always require re-publishing as described in the preceding steps.
- To ensure that background policies are applied before user login, apply `Always wait for the network at computer startup and logon **` and re-publish as described in the group solution policy. This policy is located at `Computer Configuration\Administrative Templates\System\Logon`.

Instant Clone Image Publishing and Creation Workflow

Publishing an image is a process by which internal VMs needed for instant cloning are created from a golden image and its snapshot. This process only happens once per image and may take some time.

Horizon 8 performs the following steps to create a pool of instant clones:

- 1 Horizon 8 publishes the image that you select. In vCenter Server, four folders (`ClonePrepInternalTemplateFolder`, `ClonePrepParentVmFolder`,

ClonePrepReplicaVmFolder, and ClonePrepResyncVmFolder) are created if they do not exist, and some internal VMs that are required for cloning are created. In Horizon Console, you can see the progress of this operation on the **Summary** tab of the desktop pool. During publishing, the Pending Image pane shows the name and state of the image.

Note Do not tamper with the four folders or the internal VMs that they contain. Otherwise, errors might occur. The internal VMs are removed when they are no longer needed. Normally the VMs are removed within 5 minutes of pool deletion or a push-image operation. However, sometimes the removal can take up to 30 minutes. If there are no internal VMs in all four folders, these folders are unprotected and you can delete these folders.

- 2 After the image is published, Horizon 8 creates the instant clones. This process is fast. During this process, the Current Image pane in Horizon Console shows the name and state of the image.

After the pool is created, you can change the image through the push-image operation. As with the creation of a pool, the new image is first published. Then the clones are recreated.

When an instant clone pool is created, Horizon 8 spreads the pool across datastores automatically in a balanced way. If you edit a pool to add or remove datastores, rebalancing of the cloned desktops happens automatically when a new clone is created.

Worksheet for Creating an Instant-Clone Desktop Pool

When you create an instant-clone desktop pool, you can configure certain options. You can use this worksheet to record your configuration options before you create the pool.

Before creating an instant-clone desktop pool, take a snapshot of the golden image. You must shut down the golden image in vCenter Server before taking the snapshot.

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool

Option	Option	Description	Enter Your Value Here
Type	Select Automated Desktop Pool .		
vCenter Server	Select Instant Clone and select the vCenter Server that manages the instant-clone VMs.		
User assignment	The following settings determine how end users are assigned to the desktops in this pool.		

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Select Floating or Dedicated .	<p>In a floating instant-clone desktop pool, users are assigned random desktops from the pool. When a user logs out, the instant clone desktop VM is deleted. A new clone is then regenerated using the latest golden image, based on the pool provisioning setting.</p> <p>In a dedicated instant-clone desktop pools, users are assigned a particular remote desktop and return to the same desktop at each login. When a user logs out, a refresh operation retains the computer name and the Mac address of the VM, deletes the desktop clone, and regenerates a new desktop clone from the latest golden image with the retained computer name and Mac address. You can optionally configure the instant-clone desktop pool to not refresh after logout.</p>	
	Enable Automatic Assignment	<p>In a dedicated-assignment pool, a machine is assigned to a user when the user first logs in to the pool. You can also explicitly assign machines to users.</p> <p>If you do not enable automatic assignment, you must explicitly assign a machine to each user. For more information, see Assign a Machine to a User in a Dedicated-Assignment Pool.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Enable Multi-User Assignment	<p>In a dedicated-assignment pool, you can assign multiple users to each machine in the pool.</p> <p>Multi-user assignment is not supported for automatic user assignment.</p> <p>If an assigned user has a connected or disconnected session on a multi-user assignment machine, other assigned users will be unable to launch a session on that machine. For more information, see Assign a Machine to a User in a Dedicated-Assignment Pool.</p>	
Storage Optimization	Storage Policy Management: <ul style="list-style-type: none"> ■ Use VMware Virtual SAN ■ Do not use VMware Virtual SAN 	Specify whether to use VMware vSAN, if available. vSAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of ESXi hosts.	
	Select separate datastores for replica and OS disks	<p>Specify whether to store the replica and OS disks on a datastore that is different from the datastores that the instant clones are on.</p> <p>If you select this option, you can select the options to select one or more instant-clone datastores or replica disk datastores.</p>	
Desktop Pool Identification		The following settings allow you to identify and describe the pool you are creating.	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	ID	<p>The unique name that identifies the desktop pool.</p> <p>If you have multiple Connection Server configurations, make sure that another Connection Server configuration does not use the same pool ID. A Connection Server configuration can consist of a single Connection Server or multiple Connection Servers</p>	
	Display name	The pool name that users see when they log in from a client. If you do not specify a name, the pool ID is used.	
	Access group	<p>Select an access group for the pool or leave the pool in the default root access group.</p> <p>If you use an access group, you can delegate managing the pool to an administrator who has a specific role.</p> <p>Note Access groups are different from vCenter Server folders that store desktop VMs. You select a vCenter Server folder later in the wizard.</p>	
Provisioning Settings		The following settings allow you to provide details on how the pool is provisioned.	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Enable Provisioning	<p>You can enable or disable virtual machine provisioning in the desktop pool. When you disable provisioning in the desktop pool, Horizon 8 stops provisioning new virtual machines for the desktop pool. After you disable provisioning, you can enable provisioning again.</p> <p>Before you change a desktop pool's configuration, you can disable provisioning to ensure that no new machines are created with the old configuration. You can also disable provisioning to prevent Horizon 8 from using additional storage when a pool is close to filling up the available space.</p> <p>When you first create a desktop pool and disable this option, Horizon 8 creates a desktop pool without any virtual machines. If you edit a desktop pool and disable provisioning, Horizon 8 does not allow any new virtual machines to be provisioned in this desktop pool. End users can still connect to existing virtual machines.</p> <p>For instant-clone desktop pools that are configured to refresh after a user logs out, Horizon 8 deletes the old clone and creates a new clone to replace. This operation will continue to work even if you have disabled pool provisioning.</p>	
	Stop provisioning on Error	Specify whether Horizon 8 stops provisioning desktop VMs if an error occurs and prevents the error from affecting multiple VMs.	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Virtual Machine Naming	Choose whether to provision machines by manually specifying a list of machine names or by providing a naming pattern and the total number of machines.	
	Specify names manually	Enter names that will be used to create new virtual machines. Each line must contain a unique machine name. Optionally, for dedicated desktop pools, a user name can be specified. Specific user names will be ignored for floating desktop pools.	
	# Unassigned Machines Kept Powered On	The number must be a valid integer greater than 0 and less than or equal to the maximum number of names specified. The default is 1. This option is available for instant clone dedicated pools with virtual machines specified manually and is not available for instant clone floating pools	
	Naming Pattern	If you use this naming method, provide the pattern. The pattern you specify is used as a prefix in all the machine names, followed by a unique number to identify each machine. See Using a Naming Pattern for Desktop Pools .	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Provision Machines		
	<ul style="list-style-type: none"> ■ Machines on Demand: Min number of machines ■ All Machines Up-Front 	<p>Specify whether to provision all desktop VMs when the pool is created or to provision the VMs when they are needed.</p> <ul style="list-style-type: none"> ■ Machines on demand. When the pool is created, Horizon 8 creates the number of VMs based on the Min number of machines value or the Number of spare (powered on) machines value, whichever is higher. Additional VMs are created to maintain this minimum number of available VMs as more users connect to desktops. This provides dynamic pool expansion capability where the size of the pool expands and contracts to accommodate the number of users who need desktops. When Horizon 8 is deployed on VMware Cloud on AWS, you can configure the Elastic DRS feature (rapid scaling) so that additional hosts can be automatically created (and conversely decommissioned) to meet the capacity required by the desktop pool. For more information about VMware Cloud on AWS, see the VMware Cloud on AWS 	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
		documentation at https://docs.vmware.com/en/VMware-Cloud-on-AWS/index.html .	
		<p>Note Provisioning machines on demand is only available for machines that use a naming pattern. It is disabled for virtual machines whose names are specified manually in both dedicated and floating pools.</p> <p>■ All machines up front. When the pool is created, Horizon 8 provisions the number of VMs you specify in Max number of machines. For a floating instant-clone desktop pool, the MAC address is preserved on a resync or refresh.</p>	
	Desktop Pool Sizing: Maximum Machines	Specify the maximum number of desktop VMs and powered on spare machines in the pool. For details, see Naming Machines Manually or Providing a Naming Pattern in Horizon Console .	
	Desktop Pool Sizing: Spare (Powered On) Machines	Specify the number of desktop VMs to keep available to users. For details, see Naming Machines Manually or Providing a Naming Pattern in Horizon Console .	
	Virtual Device: Add vTPM Device to VMs	Select the checkbox to add a Virtual Trusted Platform Module (vTPM) device to VMs.	
vCenter Settings		The following settings describe vCenter attributes for the pool of desktops.	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Golden Image in vCenter	Select the golden image in vCenter Server for the pool.	
	Snapshot	<p>Select the snapshot you took of the golden image.</p> <p>To specify the number of monitors and resolution for your instant-clone desktop pool, you must configure these parameters in the golden image and then take a snapshot. See Configure Number of Monitors and Screen Resolution.</p>	
	VM Folder Location	Select the folder in vCenter Server for the desktop VMs.	
	Cluster	Select the vCenter Server cluster for the desktop VMs.	
	Resource pool	Select the vCenter Server resource pool for the desktop VMs.	
	Datastores	<p>Select one or more datastores for the desktop VMs.</p> <p>The Select Instant Clone Datastores window provides high-level guidelines for estimating the pool's storage requirements. These guidelines help you determine which datastores are large enough to store the clones. The Storage Overcommit value is always set to Unbounded and is not configurable.</p> <hr/> <p>Note Instant clones and Storage vMotion are compatible. When you create an instant-clone desktop pool on a Storage DRS datastore, the Storage DRS cluster does not appear in the list of datastores. However, you can select individual Storage DRS datastores.</p> <hr/>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Networks	<p>Note If the selected snapshot has multiple network adapters, the wizard shows a selection grid for each adapter. To change the number of adapters, make the change on the golden image, take a new snapshot, and select that snapshot to use for the new pool.</p> <p>If the selected snapshot has multiple network adapters, the wizard selects the network type of Adapter 1 as the network type. To change the network type for the snapshot, edit the network type on the golden image, take a new snapshot, and select that snapshot to use for the new pool.</p> <p>Select the networks to use for the instant-clone desktop pool. You can select multiple vLAN networks to create a larger instant-clone desktop pool. This option uses the network type from the snapshot that was selected to create the pool and displays networks based on the network type of the snapshot: DVS, NSX-t, or Standard. You can use the same network as the selected snapshot or select a network from the list of available options. Networks are filtered based on the snapshot network type and the networks available in the selected cluster.</p> <p>The Select Networks wizard provides a list relevant networks based on the network type of the network you configured in the</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
		<p>snapshot's preferred network adapter (Network Adapter 1 while the snapshot was taken).</p> <p>To use multiple networks for a network adapter, you must unselect Use network from golden image (which uses the network and network type from the selected snapshot) and then select the networks to use with the new pool. The Show all networks for each network adapter switch shows or hides (greys out) incompatible networks for all network types. By default, only compatible networks are shown.</p> <hr/> <p>Important If you already have another pool using same parent and same snapshot but created with different networks than the parent VM, the new Instant Clone pool will not use the parent VM network as expected. To avoid this outcome, select the Show All Networks option and then manually select the desired network.</p> <hr/> <p>Note You can select any one available Standard network per network adapter. It is not supported to use more than one Standard network per network adapter.</p> <hr/> <p>The wizard displays error messages for the following incompatible networks:</p> <ul style="list-style-type: none"> ■ vmcNetworks - The network belongs to the VMC internal network. 	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
		<ul style="list-style-type: none"> ■ dvsUplinkPort - The network does not meet the naming standards for a virtual switch uplink port. ■ notConfiguredOnAllHosts - The network is not configured on all hosts in the cluster. ■ This network is on <network type 1>. Only networks on <network type 2> can be selected. <ul style="list-style-type: none"> - The network is not the same type as the network in the selected snapshot. <p>The wizard also provides the list of ports and port bindings that are available to use: static (early binding) and ephemeral.</p> <p>All selected NSX-t network segments must be the same size, such as all /24 networks. Unequal sized segments can result in provisioning errors.</p>	
	CPU	<p>Update the default CPU if desired.</p> <ul style="list-style-type: none"> ■ The default value is taken from the selected snapshot in vCenter. ■ You can update this value again in the future using the Push Image function. <p>Note The CPU value must be a multiple of the Cores per Socket value.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	RAM	<p>Update the default RAM if desired.</p> <ul style="list-style-type: none"> ■ The default value is taken from the selected snapshot in vCenter. ■ You can update this value again in the future using the Push Image function. <p>Note If you set a memory reservation on the Golden Image VM through vSphere Client, use the "Reserve all guest memory (All locked)" option to ensure the correct behavior when creating pools with different amounts of RAM than the Golden Image.</p>	
	Cores per Socket	<p>Update the default Cores per Socket if desired.</p> <ul style="list-style-type: none"> ■ The default value is taken from the selected snapshot in vCenter. ■ You can update this value again in the future using the Push Image function. 	
Desktop Pool Settings		The following settings determine the desktop state, power status, and display protocol when a virtual machine is not in use.	
	State	<ul style="list-style-type: none"> ■ Enabled. After being created, the pool is enabled and ready for immediate use. ■ Disabled. After being created, the pool is disabled and not available for use, and provisioning is stopped for the pool. Select this setting if you want other forms of baseline maintenance. 	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Connection Server restrictions	<ul style="list-style-type: none"> ■ No Restrictions. The desktop pool can be accessed by any Connection Server instance. ■ Restricted to these Tags. Select one or more Connection Server tags to make the desktop pool accessible only to Connection Server instances that have those tags. You can use the check boxes to select multiple tags. <p>You can restrict access to the pool to certain Connection Servers by clicking Browse and selecting one or more Connection Servers.</p> <p>If you intend to provide access to desktops through VMware Workspace ONE Access, and you configure Connection Server restrictions, the VMware Workspace ONE Access application might display desktops to users when those desktops are actually restricted. VMware Workspace ONE Access users will be unable to launch these desktops.</p>	
	Category Folder	<p>Specifies the name of the category folder that contains a Start menu shortcut for the desktop pool entitlement on Windows client devices. For more information, see "Configuring Shortcuts for Entitled Pools" in the <i>Horizon Administration</i> document.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Client Restrictions	Select whether to restrict access to entitled desktop pools from certain client computers. You must add the names of the computers that are allowed to access the desktop pool in an Active Directory security group. You can select this security group when you add users or groups to the desktop pool entitlement.	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Session Types	<p>You can enable the VM Hosted Applications feature by selecting the supported session type for the desktop pool:</p> <ul style="list-style-type: none"> ■ Desktop. Select this option to use the pool as a regular desktop pool. All the virtual machines in the pool can only be used to host desktops. ■ Application. Select this option to use all the virtual machines in the pool to host applications. ■ Desktop and Application. When this option is selected, the virtual machine in the pool can either host a regular desktop session or host an application session. The first connection to the particular virtual machine will determine the session type of the virtual machine. <p>For more information about the VM Hosted Applications feature, see the technical marketing white paper "Best Practices for Published Applications and Desktops in VMware Horizon and VMware Horizon Apps" available at https://techzone.vmware.com.</p>	
	Remote Machine Power Policy	<p>Determines the power state of instant-clones after provisioning completes. This option is only available for dedicated instant-clone desktop pools .</p> <p>For descriptions of the power-policy options, see Power Policies for Desktop Pools.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Log Off After Disconnect	<ul style="list-style-type: none"> ■ Immediately. Users are logged off when they disconnect. ■ Never. Users are never logged off. ■ After. The time after which users are logged off when they disconnect. Type the duration in minutes. <p>The logoff time applies to future disconnections. If a desktop session is already disconnected when you set a logoff time, the logoff duration for that user starts when you set the logoff time, not when the session was originally disconnected. For example, if you set this value to 5 minutes, and a session was disconnected 10 minutes earlier, Horizon 8 will log out that session 5 minutes after you set the value.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Bypass Session Timeout (Application and Desktop and Application session types)	<p>Enable this setting to allow application sessions to run forever. When enabled, all the application sessions belonging to the desktop pool will never be disconnected automatically, neither when reaching the max session timeout nor when reaching the global idle timeout.</p> <p>This setting is available when you select session types Application and Desktop or Application.</p> <p>Application sessions that run forever are supported on Windows and Linux clients.</p> <p>You cannot enable this setting if any of the applications belonging to the desktop pool is part of Global Application Entitlement as local pools.</p> <p>This setting is not available for application pools in a cloud pod architecture environment.</p> <p>Application sessions that run forever are not supported for unauthenticated users.</p> <p>Do not enable this setting if the max session timeout value is set to Never.</p> <p>When you restart Connection Server, existing forever running application sessions no longer run indefinitely.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Allow Users to Restart Machines	<p>Specify whether users can reset the virtual machine or restart the virtual desktop.</p> <p>A reset operation resets the virtual machine without a graceful operating system restart.</p> <p>A restart operation restarts the virtual machine with a graceful operating system restart.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Refresh OS disk After Logoff	<p>Select whether and when to refresh the OS disks. This option is available for dedicated assignment pools.</p> <ul style="list-style-type: none"> ■ Always. The OS disk is refreshed every time the user logs off. Select this option to use App Volumes with dedicated instant clones. ■ Every. The OS disk is refreshed at regular intervals of a specified number of days. Enter the number of days. The number of days is counted from the last refresh, or from the initial provisioning if no refresh has occurred yet. For example, if the specified value is 3 days, and three days have passed since the last refresh, the desktop is refreshed after the user logs off. ■ At. The OS disk is refreshed when its current size reaches a specified percentage of its maximum allowable size. The maximum size of a instant clone's OS disk is the size of the replica's OS disk. Enter the percentage at which refresh operations occur. ■ Never. The OS disk is never refreshed. 	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Reclaim VM disk space	<p>Determine whether to allow ESXi hosts to reclaim unused disk space on instant clones that are created in space-efficient disk format. The space reclamation feature reduces the total storage space required for instant clone desktops.</p> <hr/> <p>Note This setting is only applicable if you use a vSphere version earlier than 6.7 and if you use non-vSAN storage. For vSphere 6.7 and later, space reclamation is done automatically by vSphere and no additional steps are needed on Horizon 8.</p> <hr/>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Initiate reclamation when unused space on VM exceeds:	<p>Type the minimum amount of unused disk space, in gigabytes, that must accumulate on a instant clone OS disk to trigger space reclamation. When the unused disk space exceeds this threshold, Horizon 8 initiates the operation that directs the ESXi host to reclaim space on the OS disk.</p> <p>This value is measured per virtual machine. The unused disk space must exceed the specified threshold on an individual virtual machine before Horizon 8 starts the space reclamation process on that machine.</p> <p>The default value is 1 GB.</p> <hr/> <p>Note This setting is only applicable if you use a vSphere version earlier than 6.7 and if you use non-vSAN storage. For vSphere 6.7 and later, space reclamation is done automatically by vSphere and no additional steps are needed on Horizon 8.</p>	
	Show Assigned Machine Name	<p>Displays the host name of the assigned machine instead of the desktop pool display name when you log in to Horizon Client.</p> <p>If no machine is assigned to the user, then Display Name (No Machine Assigned) appears for the desktop pool when you log in to Horizon Client.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Show Machine Alias Name	<p>Displays the machine alias name set for the assigned users of the machine instead of the desktop display name for the desktop pool in Horizon Client. Applies only to dedicated desktop entitlements.</p> <p>If no machine alias name is set but the Show Assigned Machine Name is set, then the machine host name appears for the desktop pool in Horizon Client. Otherwise, the desktop display name appears for the desktop pool in Horizon Client.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Empty session timeout (Applications only)	<p>Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log out from empty application sessions. Select Never, Immediate, or set the number of minutes as the timeout value. The default is After 1 minute. If you select Immediate, the session logs you out or disconnects within 30 seconds.</p> <p>You can further reduce the time the session logs out or disconnects by editing a registry key on the RDS Host on which Horizon Agent is installed. Navigate to <code>HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params</code> and set a value for <code>WindowCheckInterval</code>. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session logout to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session logout to 5 seconds.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Pre-launch session timeout (applications only)	Determines the timeout for the application session before the session is disconnected or logged off.	
	When timeout occurs (applications only)	Determines whether an empty application session is disconnected or logged off after the Empty session timeout limit is reached. Select Disconnect or Log off . A session that is logged off frees up resources, but opening an application takes longer. The default is Disconnect .	
	Allow user to initiate separate sessions from different client devices (Desktops only)	With this option selected, a user connecting to the same desktop pool from different client devices gets different desktop sessions. The user can only reconnect to an existing session from the same client device. When this setting is not selected, users are always reconnected to their existing session no matter which client device is used.	
Remote Display Setting		The following settings describe how the desktops are displayed to the end-users.	
	Default display protocol	Select the default display protocol. The choices are VMware Blast , PCoIP , and Microsoft RDP .	
	Allow users to choose protocol	Specify whether users can choose display protocols other than the default. <ul style="list-style-type: none"> ■ Yes. Allow users to choose a display protocol. ■ No. Do not allow users to choose a display protocol. 	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	3D Renderer	<p>This field shows the type of 3D Render available for the instant-clone pool. This is not a selectable field. Depending on what you configured on the ESXi host and the golden image used for this pool, Horizon 8 will automatically display one of the following two options:</p> <ul style="list-style-type: none"> ■ NVIDIA GRID vGPU. 3D rendering is enabled for NVIDIA GRID vGPU. ■ Manage using vSphere Client. The 3D Renderer option that you configured in vSphere Client. <p>See Configuring 3D Rendering Options for Instant-Clone Pools.</p>	
	Allow Session Collaboration	<p>Select Enabled to allow users of the desktop pool to invite other users to join their remote desktop sessions. Session owners and session collaborators must use the VMware Blast protocol.</p>	
Guest Customization			
	Domain	<p>Select an Active Directory domain. The drop-down list shows the domains that you specify when you configure instant-clone domain administrators.</p>	
	AD container	<p>Specify the Active Directory container's relative distinguished name.</p> <p>For example: CN=Computers</p> <p>In the Add Desktop Pool window, you can browse the Active Directory tree for the container. You can also copy, paste, or enter the path for the AD tree for the container.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Allow Reuse of Existing Computer Accounts	<p>Select this option to use existing computer accounts in Active Directory when the virtual machine names of new instant clones match the existing computer account names. See Allow Reuse of Existing Computer Accounts.</p> <hr/> <p>Note Recover operation does not take this setting into consideration and always reuses the machine name.</p>	
	Image Publish Computer Account	<p>Instant Clone publishing needs an additional computer account in the same AD domain as the clones. Computer accounts are typically auto-created as needed. If you want to use pre-created computer accounts instead, also pre-create the additional computer account and specify its name here. This removes the need to delegate Create and Delete of computer objects to the provisioning account.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Use ClonePrep or a customization specification (Sysprep)	<p>Choose whether to use ClonePrep or select a customization specification (Sysprep) to configure licensing, domain attachment, DHCP settings, and other properties on the machines.</p> <p>ClonePrep can run a customization script on instant-clone machines before they are powered off and after they are created or an image has been pushed to them.</p> <p>After you use ClonePrep or Sysprep when you create a pool, you can edit the customization type or spec name. Changes to the customization spec are not reflected on the pool until a new push image is scheduled, and the currently published image continues to use the old spec even if it has been edited or deleted. If push image fails, the pool continues using the old unedited spec. However, the pool settings continue to point to the new spec name if it has been changed.</p> <p>For more information about the differences between ClonePrep and Sysprep, see Choosing ClonePrep or Sysprep for Customizing Your Virtual Desktops.</p>	
	Power-Off Script Name	Specify the path name of a script to run on the desktop VMs and the script parameters before the VMs are powered off.	
	Power-Off Script Parameters	Example: p1 p2 p3	

Table 4-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Post-Synchronization Script Name	Specify the path name of a script to run on the desktop VMs and the script parameters after the VMs are created.	
	Post-Synchronization Script Parameters	Example: p1 p2 p3	

Create an Instant-Clone Desktop Pool

Horizon 8 creates the instant-clone desktop virtual machines (VMs) based on the settings that you specify when you create the pool.

Prerequisites

- Verify that the virtual switch that the instant-clone VMs connect to has enough ports to support the expected number of VMs. Each network card on a VM requires one port.
- Verify that you have the golden image ready. For more information, see [Creating a Virtual Machine for Cloning](#).

Note You cannot create an instant-clone desktop pool from a VM template. You must first convert the VM template to a VM.

- Gather the configuration information for the pool. See [Worksheet for Creating an Instant-Clone Desktop Pool](#).
- Verify that you added an instant-clone domain administrator in Horizon Console. See "Add an Instant-Clone Domain Administrator" in the *Horizon Installation and Upgrade* document.
- Before creating an instant-clone desktop pool, take a snapshot of the golden image. You must shut down the golden image in vCenter Server before taking the snapshot.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Click **Add**.
- 3 Select **Automated Desktop Pool** and click **Next**.
- 4 Select **Instant Clones**, select the vCenter Server instance, and click **Next**.

5 Follow the prompts to create the pool.

Use the configuration information you gathered in the worksheet. You can go directly back to any wizard page by clicking the page name in the navigation pane.

Note If you are a VMware Carbon Black customer and select a golden image configured with Carbon Black for the new pool, then the screen displays information from the Carbon Black Scan for each snapshot listed.

- If you select the Show All Images check box, the list might include snapshots that are not compatible and cannot be selected.
 - If no value appears in the Carbon Black Scan (% Complete) column, that indicates that the Carbon Black sensor was not enabled in the Instant Clone golden image when the snapshot was taken. For more information, see the [VMware Carbon Black Cloud Documentation](#).
-

What to do next

Entitle users to access the pool. See "Entitling Users and Groups" in the *Horizon Administration* document.

Forensics Select Hold for Dedicated and Floating Instant Clone Desktops

The purpose of the forensics select hold feature is to provide accurate and non-modified data for legal, security, and operational needs. The currently supported use case allows the live capture of data associated with a user's desktop on a periodic basis when a user is put into a select hold for legal, incident response, or operational reasons. Putting a user on forensics select hold makes the user's desktops temporarily persistent, thus avoiding refreshing or deletion ("re-imaging") of the desktop and providing the administrator with the ability to access the user's desktop for investigative purposes with minimum impact to the user's experience.

How the Forensics Select Hold Feature Works

■ Role-based access control

The forensics feature is controlled by the global privilege FORENSICS. The Super Administrator can assign this privilege to another administrator, who is known as the Forensics Administrator, but this privilege is not enabled for the Super Administrator by default. For more information, see "Global Privileges" in the *Horizon Administration* document.

■ Archival datastore

The archival datastore is a mounted NFS or VMFS set globally in LDAP. Horizon 8 reads this setting from LDAP to determine where to place archived data. By default, the setting is to use the same datastore that the pool is on.

- Select hold workflow

- Putting users on hold

A hold can only be applied at an individual AD user level. When the Forensic Administrator puts a user on hold using the API, the following occur:

- If the user is already using a VM, then the hold applies to the VM they are currently logged into, and to any other VMs assigned to the user.
- When that user logs into a VM, Horizon 8 changes the state of the instant clone VM from stateless to stateful, but leaves the stateful VM in its original pool.
- The user under hold continues to log back into the same VM and to see all the previous changes they made to their desktop. Horizon 8 does not alter the content of the VM in any way.
- A status indicator in the administration console shows that the VM is in hold.
- The VM is tagged in vCenter so that vCenter administrators know not to alter it.

- During the hold period

After a user is put on hold, the forensics team can access the stateful desktop for investigation as well as capture the live data on the fly. For this data capture, the forensics administrator has the following options.

- Use the `Archive` API. The `Archive` API can work across multiple VMs and multiple users. You can only archive an individual VM when the user is not logged in. If user is logged in, then the archival command needs to be delayed until the user logs out.

Archival operation is as follows:

- The VM is shut down.
 - All disks are consolidated.
 - All snapshots are consolidated.
 - The VMDK file is copied to the selected archival location.
 - The VM is re-synced to the target image.
 - Use your own scripts or third party tools. In this case, you can choose whether to archive just hypervisor memory, just the VMDKs of the VMs, or both hypervisor memory and VMDKs.

The `isHeldUser` environment variable indicates whether the user connecting to the session is a held user. Based on the value of this variable, you can trigger data collection scripts when a held user logs on to a desktop. A script can be triggered when the Script Host Service is running on the Connection Server VM. For more information, see *Activate the VMware Horizon View Script Host Service in the [Horizon Remote Desktop Features and GPOs](#) document.*

Things to note during the hold period:

- A held VM cannot be refreshed, recovered, removed, or put into maintenance mode. This applies only to the held VM, not to any other VMs in the same pool.
- A pool containing held VMs cannot be deleted.
- When the auto shrink capability of the pool is set, Horizon 8 prioritizes the held VM so that it is not lost.
- When the instant clone pool needs to undergo pool refresh or patch update, there are two possible options:
 - When a pool containing held VMs needs to be refreshed and the archival datastore is not set, push image ignores the stateful VMs. This preserves the VMs under hold for forensics purposes, and the user continues to be directed to the persistent VM when they log in. These VMs must then be patched with separate tools like persistent VMs.
 - When a pool containing held VMs needs to be refreshed and the archival datastore is set, Horizon 8 first performs a push image on all the other VMs in the pool, then archives the held VMs. After the held VMs have been archived, Horizon 8 performs a normal push image process on them. The next time the held user logs back in, they get a pristine VM, which turns into a stateful VM, and the process repeats. Note that every time a patch operation happens, additional storage is required to copy and archive the stateful VM.
- Removing users from hold

When the Forensics Administrator releases a user from hold using the API, the following occur.

- Horizon 8 turns the VM back into a stateless VM.
- On the next user logoff, the VM is deleted and recreated from the golden image, thus reverting to a pristine state.

■ Forensic operations in the Events database

All operations, including granting of the FORENSICS privilege and holding/releasing users, are captured in the Events database. This can be used to notify any scripts that need to run.

Using APIs to Perform Forensics Select Hold Functions

You can use Horizon APIs to perform forensics select hold as described below. For each API, there is a link to its documentation on the VMware {code} website.

- Create Forensic Administrator Role and Assign a User
 - a Create the custom Forensic Administrator role using the following API:

```
/config/v1/roles
```

Documentation for this API is found [here](#).

- b Assign the custom Forensic Administrator role by following the instructions in "Create an Administrator in Horizon Console" in the *Horizon Administration* guide.

- Designate a datastore for archiving

To designate a datastore for archiving virtual disks and memory, use the following API:

```
/config/v1/virtual-centers/{id}/action/mark-datastores-for-archival
```

Documentation for this API is found [here](#).

- Put User on Hold

To put a user on hold, use the following API:

```
/external/v1/ad-users-or-groups/action/hold
```

The API returns the desktop ID, pool ID, and machine state for all desktops that are assigned to the held user. You can use this alert information to trigger scripted data collection.

Documentation for this API is found [here](#).

In vCenter, the `ForensicHold` tag is applied to all the VMs used by held users.

- Archive the Virtual Disk and Memory of a VM

To archive the virtual disk and memory of a VM, use the following API:

```
/inventory/v1/machines/action/archive
```

Documentation for this API is found [here](#).

- Archiving occurs when the user logs out of the held VM.
- When VMs have been archived, they are shown inside the `Archive` folder on the archive datastore (as specified above in the API) in vCenter.
- If a VM has more than one disk, then only the primary disk is archived. Multi-disk archival is not supported in this release.

- Release User From Hold

To release a user from hold, use the following API:

```
/external/v1/ad-users-or-groups/action/release-hold
```

The API returns the desktop ID, pool ID, and machine state for all desktops that are assigned to the held user. You can use this alert information to trigger scripted data collection.

Documentation for this API is found [here](#).

- List Held Users

To list held users, use the following API:

```
/external/v1/ad-users-or-groups/held-users-or-groups
```

Documentation for this API is found [here](#).

- List Held Machines

To produce a list of machines currently on hold, use the following API:

```
/inventory/v3/machines
```

Documentation for this API is found [here](#).

Note This API returns all machines. In the response, VMs on hold have the value "held_machine": true.

Configure Instant Clones with vSphere Virtual Machine Encryption

You can configure instant clones to use the vSphere Virtual Machine Encryption feature so that instant-clone desktops have the same encryption keys.

Prerequisites

- vSphere 7.0 or later.
- Create the Key Management Server (KMS) cluster with key management servers.
- To create a trust between KMS and vCenter Server, accept the self signed CA certificate or create a CA signed certificate.
- In vSphere Client, create the `VMcrypt/VMEncryption` storage profile.

Note For details about the Virtual Machine Encryption feature in vSphere, see the *vSphere Security* document in the vSphere documentation.

Procedure

- 1 To configure instant-clones that use the same encryption keys, use the vSphere Client to create a golden image VM with the `vmencrypt` storage policy.

The `vmencrypt` storage policy applies only when the golden image VM does not have any snapshots. The clone inherits the golden image encryption state, including keys.

- 2 Take snapshot of the golden image VM with the `vmencrypt` storage policy applied.
- 3 Create instant-clone desktops that point to the golden image VM with the `vmencrypt` storage policy applied so that all desktops have the same encryption keys.

Note VM Encryption and Content Based Read Cache (CBRC) are not compatible. To use VM Encryption, you must disable CBRC globally by disabling View Storage Accelerator in Horizon Console by navigating to **Settings > Servers**.

Guest Customization for Instant Clones in VMware Horizon

There are two options for customizing instant clone virtual machines during the creation process: VMware ClonePrep or Microsoft Sysprep.

ClonePrep is a VMware customization process run during instant clone deployment to personalize each desktop clone created from the parent image.

Sysprep is a Microsoft tool to deploy the configured operation system installation from a base image. The desktop can then be customized based on an answer script.

For more information about the differences between ClonePrep and Sysprep, see [Choosing ClonePrep or Sysprep for Customizing Your Virtual Desktops](#).

- [ClonePrep Guest Customization](#)
- [Sysprep Guest Customization](#)

ClonePrep Guest Customization

ClonePrep ensures that all instant clones join an Active Directory domain. The clones have the same computer security identifiers (SIDs) as the golden image. ClonePrep also preserves the globally unique identifiers (GUIDs) of applications, although some applications generate a new GUID during customization.

When you add an instant-clone desktop pool, you can specify a script so that it runs immediately after a clone is created and another script to run before the clone is powered off.

■ How ClonePrep Runs Scripts

ClonePrep uses the Windows `CreateProcess` API to run scripts. Your script can invoke any process that can be created with the `CreateProcess` API. For example, `cmd`, `vbscript`, `exe`, and batch-file processes work with the API.

Specifically, ClonePrep passes the path of the script as the second parameter to the `CreateProcess` API and sets the first parameter to `NULL`. For example, if the script path is `c:\myscript.cmd`, the call to `CreateProcess` is `CreateProcess(NULL, c:\myscript.cmd, ...)`.

■ Providing Paths to ClonePrep Scripts

You can specify the scripts when you create or edit the desktop pool. The scripts must reside on the golden image. You cannot use a UNC path to a network share.

If you use a scripting language that needs an interpreter to run the script, the script path must start with the interpreter executable. For example, instead of specifying `C:\script\myvb.vbs`, you must specify `C:\windows\system32\cscript.exe c:\script\myvb.vbs`.

Important Put the ClonePrep customization scripts in a secure folder to prevent unauthorized access.

- ClonePrep Script Timeout Limit

By default, ClonePrep terminates a script if the execution takes longer than 20 seconds. You can increase this timeout limit. For details, see [Increase the Timeout Limit for ClonePrep Customization Scripts](#).

Alternatively, you can specify a script that runs another script or process that takes a long time to run.

- ClonePrep Script Account

ClonePrep runs the scripts using the same account that the VMware Horizon Instant Clone Agent service uses. By default, this account is Local System. Do not change this login account. If you do, the clones can fail to start.

- ClonePrep Process Privileges

For security reasons, certain Windows operating system privileges are removed from the VMware Horizon Instant Clone Agent process that runs ClonePrep customization scripts. The scripts cannot perform actions that require those privileges.

The process that runs ClonePrep scripts do not have the following privileges:

- SeCreateTokenPrivilege
- SeTakeOwnershipPrivilege
- SeSecurityPrivilege
- SeSystemEnvironmentPrivilege
- SeLoadDriverPrivilege
- SeSystemtimePrivilege
- SeUndockPrivilege
- SeManageVolumePrivilege
- SeLockMemoryPrivilege
- SeIncreaseBasePriorityPrivilege
- SeCreatePermanentPrivilege
- SeDebugPrivilege
- SeAuditPrivilege

- ClonePrep Script Logs

ClonePrep writes messages to a log file located in `C:\ProgramData\Vmware\VDM\Logs`.

Sysprep Guest Customization

Note the following information regarding Sysprep in Microsoft Windows 10 guests.

- To run Sysprep on some older versions of Windows 10, you must remove Appx Packages installed for all users. In some newer updates of Windows 10, Sysprep automatically removes these packages so you do not have to do so. For instructions on removing Appx packages, see the [Microsoft support site](#).
- Sysprep can fail because there are Windows updates pending. To prevent this, run a Microsoft Windows update on golden image VM and consider disabling the Microsoft Windows update service for instant clone. You can also check the Windows update page to confirm that there are no pending updates or errors displayed.
- By default, Sysprep generalize disables the built-in administrator account. If there is no other user account on the golden image VM, and if clone customization fails, users are not able to log in to the clone VM to collect debug information. When attempting to log in as local administrator, users will see a message on login screen saying 'Your account has been disabled. Please see your system administrator.' To resolve this issue, create new user accounts on the golden image VM following the instructions on the [Microsoft support site](#).

Caution Instant Clone Sysprep customization does not support adding vTPM device for clones. Enabling this option leads to unpredictable behavior.

Enabling VBS and vTPM for an Instant-Clone Desktop Pool

You can enable Microsoft VBS and add a Virtual Trusted Platform Module (vTPM) device to instant-clone desktop pools.

To set up the Key Management Server cluster, which is a prerequisite, see "Set up the Key Management Server Cluster" in the *vSphere Security* document in the vSphere documentation..

For compatibility requirements, see "Securing Virtual Machines with Virtual Trusted Platform Module" in the *vSphere Security* document in the vSphere documentation.

The golden image used for vTPM instant-clone desktop pools must have VBS enabled when creating the VM and the local security policy set to enable VBS inside the guest operating system.

You can also select or deselect the option to add or remove a vTPM during a push-image operation.

Note Horizon does not use Smart Provisioning on instant clones configured with vTPM.

Caution Instant Clone Sysprep customization does not support adding vTPM device for clones. Enabling this option leads to unpredictable behavior.

Configuring 3D Rendering Options for Instant-Clone Pools

When you create or edit a desktop pool of virtual machines, you can configure 3D graphics rendering for your desktops. You must configure 3D settings in ESXi hosts and in the golden image in vSphere Client.

Horizon 8 does not directly control settings for 3D rendering of an instant-clone pool as it does with full-clone virtual machines. You need to configure 3D settings in the ESXi hosts, and then in your golden image using the vSphere Client. Instant-clone virtual machines will inherit those settings from the golden image. Horizon Console will display some of the settings you configured, but you cannot edit or interact with those settings.

End users can take advantage of 3D applications for design, modeling, and multimedia, which typically require GPU hardware to perform well. For users that do not require physical GPU, a software option provides graphics enhancements that can support less demanding applications. Instant-clones support the following 3D graphics options:

NVIDIA GRID vGPU (shared GPU hardware acceleration)

This feature allows a physical GPU on an ESXi host to be shared among virtual machines. This feature offers flexible hardware-accelerated 3D profiles ranging from lightweight 3D task workers to high-end workstation graphics power users.

Soft 3D

Software-accelerated graphics allow you to run DirectX 9 and OpenGL 2.1 applications without requiring a physical GPU. For users that do not require a physical GPU, a software option provides graphics enhancements that can support less demanding applications, such as Windows AERO, Microsoft Office, and Google Earth.

Virtual Shared Graphics Acceleration (vSGA)

This feature allows multiple virtual machines to share the physical GPUs on ESXi hosts and is suitable for mid-range 3D design, modeling, and multimedia applications.

Note Instant-clones do not support Virtual Directed Graphics Acceleration (vDGA) or AMD MxGPU.

In some cases, if an application such as a video game or 3D benchmark forces the desktop to display in full screen resolution, the desktop session can be disconnected. Possible workarounds include setting the application to run in Windows mode or matching the Horizon 8 session desktop resolution to the default resolution expected by the application.

Note that this guide does not provide complete information for configuring virtual machines and ESXi hosts for vSGA or NVIDIA GRID vGPU. These tasks must be done with vSphere Client before you attempt to create desktop pools in Horizon Console. For instructions about these tasks, see the [VMware white paper](#) the about graphics acceleration. For instructions about NVIDIA GRID vGPU, see the [NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1](#).

To disable 3D rendering in the vSphere Client, deselect **Enable 3D Support** for the golden image using the vSphere Client. See *Configuring 3D Graphics in the vSphere Virtual Machine Administration* guide.

Enable NVIDIA GRID vGPU for Instant-Clone Pools

You can configure NVIDIA GRID vGPU in ESXi hosts and in the golden image in vSphere Client.

The ESXi host assigns GPU hardware resources to virtual machines on a first-come, first-served basis as virtual machines are created. By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is the **best performance** mode. If you would rather have the ESXi host assign virtual machines to the same physical GPU until the maximum number of virtual machines is reached before placing virtual machines on the next physical GPU, you can use the **GPU consolidation** mode. You can configure this mode in vCenter Server for each ESXi host that has vGPU installed. For more information, see the VMware Knowledge Base (KB) article <https://kb.vmware.com/s/article/55049>.

If you are only using a single vGPU profile per vSphere cluster, set the GPU assignment policy for all GPU hosts within the cluster to the **best performance** mode in order to maximize performance. In this case, you can also have instant-clone pools and full-clone pools that use the same vGPU profile in the same vSphere cluster.

You can have a cluster with some GPU enabled hosts and some non-GPU enabled hosts.

Note vMotion of vGPU Virtual Machines

- vMotion of vGPU Virtual Machines is supported starting with vSphere 6.7. See [here](#) for details on how to configure this and more information.
 - vSphere Distributed Resource Scheduler (DRS) in vSphere 6.7 Update 1 and later supports initial placement of vGPU VMs without load balancing support.
 - DRS in vSphere 6.7 or vSphere 7.0 versions earlier than vSphere 7.0 U3f will not automatically vMotion vGPU VMs when ESXi hosts are placed in maintenance mode. An administrator is required to manually initiate vMotion of vGPU VMs in order to allow ESXi hosts to enter maintenance mode.
 - DRS in vSphere 7.0 U3f and later can be configured to allow automatic vMotion when hosts are placed in maintenance mode. See <https://kb.vmware.com/s/article/88271> for instructions. DRS load balancing remains unsupported for vGPU VMs.
-

NVIDIA GRID vGPU has these potential constraints:

- RDP is not supported.
- The virtual machines must be hardware version 11 or later.
- Horizon 8 does support creating a vGPU instant-clone pool using a cluster with some vGPU enabled hosts and non-vGPU enabled hosts, and will just ignore the non-vGPU enabled hosts when creating the pool. You can not use vMotion to move an instant-clone from a GPU-enabled ESXi host to an ESXi host that does not have GPU hardware configured.

To enable an instant-clone pool to use NVIDIA GRID vGPU:

Procedure

- 1 Install NVIDIA GRID vGPU in the physical ESXi hosts.
- 2 In vCenter Server hardware graphics configuration, select the Host Graphics tab, and in **Edit Host Graphics Settings**, select **Shared Direct**.
ESXi host uses the NVIDIA GRID card for vGPU.
- 3 Prepare a golden image with NVIDIA GRID vGPU configured, including selecting the vGPU profile you want to use.
- 4 Take a snapshot of the golden image.
- 5 In Horizon Console, when you create an instant-clone pool, select this golden image and snapshot.

Results

Horizon 8 automatically displays **NVIDIA GRID vGPU** in the 3D Render field. Horizon 8 also displays the vGPU profile you chose in the golden image. Instant clones inherit the settings configured in the vSphere Client for the golden image.

The vGPU profile cannot be edited from Horizon Console during the instant-clone pool creation process. To edit the vGPU profile for a pool once the pool has been created, you can create a new image with the updated vGPU profile, take a snapshot, and then do a push-image operation. See [Patching an Instant-Clone Desktop Pool](#).

Enable Soft 3D for Instant-Clone Pools

When you enable Soft 3D, ESXi host uses software 3D graphics rendering.

If a GPU graphics card is installed on the ESXi host, this pool will not use it. Horizon 8 does not control or configure 3D rendering settings because they are all set in the golden image VM using vSphere Client.

To enable Soft 3D in the golden image VM:

Procedure

- 1 In the vSphere Client, 3D Render field, select **Software**.
- 2 Configure **Number of displays**, **Total video memory**, and **3D memory** for the instant-clones to inherit from the golden image.
- 3 Take a snapshot of the golden image.
- 4 In Horizon Console, when you create an instant-clone pool, select this golden image and snapshot.

Results

Horizon 8 automatically displays **Manage Using vSphere Client** in the 3D Render field. Instant-clones inherit the settings configured in the vSphere Client for the golden image.

Enable vSGA for Instant-Clone Pools

When you enable vSGA, ESXi host uses hardware 3D rendering, provided that GPU resources are available on the ESXi hosts.

To enable vSGA, install GPU graphics cards and the associated vSphere Installation Bundles (VIBs) on the ESXi hosts. For a list of supported GPU hardware, see the [VMware Hardware Compatibility List](#).

Procedure

- 1 In vCenter Server hardware graphics configuration, select the Host Graphics tab, and in **Edit Host Graphics Settings**, select **Shared**.
ESXi host uses the GPU hardware for vSGA mode.
- 2 In the vSphere Client, configure the golden image 3D Render field with these two options.
 - Select **Hardware**. Select this option if you only want to use vSGA hardware 3D render. Potential constraints when selecting this option are that when all GPU resources on an ESXi host are reserved, Horizon 8 cannot create another virtual machine for the next user, and the user will receive an error message. You must manage the allocation of GPU resources and the use of vMotion to ensure that resources are available for your desktops. vMotion is supported for vSGA-enabled hosts, but only across those hosts with GPU hardware. When you configure hardware-based 3D rendering, you can examine the GPU resources that are allocated to each virtual machine on an ESXi host. For details, see [Examining GPU Resources on an ESXi Host](#).
 - Select **Automatic**. If you select this option, vSGA-enabled virtual machines can switch dynamically between software and hardware 3D rendering. Automatic uses hardware acceleration if there is a capable and available hardware GPU in the ESXi host. If a hardware GPU is not available, the virtual machine uses software 3D rendering for any 3D tasks. This option ensures that some type of 3D rendering takes place even when GPU resources are completely reserved.
- 3 Configure **Number of displays**, **Total video memory**, and **3D memory** for the instant-clones to inherit from the golden image.
- 4 Take a snapshot of the golden image.
- 5 In Horizon Console, when you create an instant-clone pool, select this golden image and snapshot.

Results

Horizon 8 automatically displays **Manage Using vSphere Client** in the 3D Render field. Instant-clones inherit the settings configured in the vSphere Client for the golden image.

Configure Number of Monitors and Screen Resolution

You can specify the number of monitors and resolution for your instant-clone desktop pool in the vSphere Client by setting those parameters in the golden image and taking a snapshot.

The required vRAM size is calculated based on your specifications. Select the snapshot of the golden image to use for the pool. The snapshot lists the following details:

- Number of monitors
- VRAM size
- Resolution

The instant-clone desktop pool created is based on the golden image snapshot and inherits those memory settings. You cannot configure these settings in Horizon Console for instant-clones.

For more information about configuring video memory settings in vSphere Client, see *vSphere Single Host Management* in the vSphere documentation.

For more information about changing the resolution for your instant-clone desktop pool, see the VMware Knowledge Base (KB) article <http://kb.vmware.com/kb/2151745>.

Allow Reuse of Existing Computer Accounts

You can configure instant-clones to reuse existing AD computer account names.

Enable this option if you have a limited number of computer accounts to use. When an instant-clone is created, if an existing AD computer account name matches the instant-clone virtual machine name, Horizon 8 uses the existing computer account after resetting the password. Otherwise, a new computer account is created. When the instant clone is deleted, Horizon 8 does not delete the corresponding computer accounts. The existing computer accounts must be located in the Active Directory container that you specify with the AD container setting.

When this option is disabled, a new AD computer account is created when Horizon 8 creates an instant-clone. When the instant-clone is deleted, Horizon 8 deletes the corresponding computer account. If an existing computer account matches the instant-clone virtual machine name, Horizon 8 reuses the existing computer account after resetting the password.

This option is disabled by default.

Manually Customizing Machines

After you create an automated pool, you can customize particular machines without reassigning ownership. By starting the machines in maintenance mode, you can modify and test the machines before you release them to users.

Maintenance mode prevents users from accessing their desktops. If you start machines in maintenance mode, Horizon 8 places each machine in maintenance mode when the machine is created. In a dedicated-assignment pool of full virtual machines, you can use maintenance mode to log in to a machine without having to reassign ownership to your own administrator account. When you finish the customization, you do not have to return ownership to the user assigned to the machine.

To perform the same customization on all machines in an automated pool, customize the virtual machine you prepare as a template. Horizon 8 deploys your customization to all the machines.

Note You can start machines in maintenance mode if you manually specify machine names for the pool, not if you name machines by providing a naming pattern.

Customize Machines by Placing Them in Maintenance Mode After Pool Creation

After a desktop pool is created, you can customize, modify, or test individual machines by placing them in maintenance mode. When a machine is in maintenance mode, users cannot access the virtual machine desktop.

You place existing machines in maintenance mode one at a time. You can remove multiple machines from maintenance mode in one operation.

When you create a desktop pool, you can start all the machines in the pool in maintenance mode if you specify machine names manually.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Click the link for the pool.
- 3 Select the **Machines** tab.
- 4 Select a machine.
- 5 Select **Enter Maintenance Mode** from the **More Commands** drop-down menu.
- 6 Customize, modify, or test the virtual machine desktop.
- 7 Repeat steps to select a machine and customize, modify, or test the virtual machine desktop.
- 8 Select the customized machines and select **Exit Maintenance Mode** from the **More Commands** drop-down menu.

Results

The modified virtual machine desktops are available to users.

Customize Machines by Starting Them in Maintenance Mode During Pool Creation

You can customize individual machines after a pool is created by starting the machines in maintenance mode.

Procedure

- 1 In Horizon Console, begin creating an automated desktop pool by starting the **Add Pool** wizard.
- 2 On the Provisioning Settings page, select **Specify names manually**.
- 3 Select **Start machines in maintenance mode**.
- 4 Complete the **Add Pool** wizard to finish creating the desktop pool.
- 5 In vCenter Server, log in, customize, and test the individual virtual machines.
You can customize the machines manually or by using standard Windows systems-management software such as Altiris, SMS, LanDesk, or BMC.
- 6 In Horizon Console, select **Inventory > Machines**.
- 7 Select specific machines to release to your users.
- 8 Click **More Commands > Exit Maintenance Mode**.

What to do next

Notify your users that they can log in to their desktops.

Patching an Instant-Clone Desktop Pool

To patch a pool of instant-clone desktops, you can use the push-image operation for a rolling patching process with zero downtime.

The image you used to create a pool is the default image. By default, all patching operations use this image to update all machines in the pool. Depending on how you want the golden image to be managed, you can change the golden image and snapshot source in your pool from vCenter to Image Catalog or reverse. For more information on the Image Management Service, see the *Managing Horizon Images from the Cloud* document.

You can optionally publish a secondary image, which you can use to update a subset of the machines in the pool while leaving the rest unchanged. Find out more in [Selective Patching](#).

When you are using the default image, the workflow for the patching process is as follows:

- Prepare a new golden image and snapshot based on the updated operating system image or applications.

- Schedule a push-image operation with the updated golden image and snapshot. When the push-image operation starts, Horizon 8 deletes old instant-clone desktops that are unused and quickly creates new instant clones based on the new image. The new clones are ready for users to log in.
- Old instant-clone desktops that are in-use remain undisturbed. When the user logs out, Horizon 8 deletes the old instant clone and recreates a new instant clone based on the updated image. The new instant clone is ready for the next user to log in.
- Once all the users have logged out, Horizon 8 patches the entire pool.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Click the pool ID.
- 3 On the **Summary** tab, click **Maintain > Schedule**.

The **Schedule Push Image** window opens.

- 4 On the Image step, select the snapshot to use. The default image for the pool is already selected. If the image source is Image Catalog, please select stream and marker.

Note If you are a VMware Carbon Black customer and select a golden image configured with Carbon Black, then the screen displays information from the Carbon Black Scan for each snapshot listed.

- If you select the Show All Images check box, the list might include snapshots that are not compatible and cannot be selected.
 - If no value appears in the Carbon Black Scan (% Complete) column, that indicates that the Carbon Black sensor was not enabled in the Instant Clone golden image when the snapshot was taken. For more information, see the [VMware Carbon Black Cloud Documentation](#).
-

- 5 On the Schedule step, select the **Schedule image push** option.

You can schedule the task to start immediately or sometime in the future. For clones with user sessions, you can specify whether to force the users to log out or to wait. When the users log out, Horizon 8 recreates the clones.

- 6 On the Ready to Complete step, click **Finish**.

Results

When you schedule this operation, publishing of the new image starts immediately. Pool update starts at the time that you specify in the **Schedule Push Image** wizard.

Selective Patching

Consider a scenario where before updating an entire pool with a new image, you would like to first try it out on a subset of the pool so that you know that the new image works, and users are able to

login. This feature gives administrators an option to either update the entire pool or specify a set of machines to update. It allows a single desktop pool to support two images at the same time.

Patch Selected VMs In the Pool Using a Secondary Image

When you are using a secondary image, the workflow for the patching process is as follows:

- Prepare a secondary golden image and snapshot based on the updated operating system image or applications.
- Perform a push-image operation with the secondary golden image and snapshot. You have two options for this operation:
 - Publish the secondary image without immediately applying it to any machines in the pool.
 - Publish the secondary image and immediately apply it to selected machines in the pool.
- After you have published the secondary image, options are enabled to apply either of the images to selected machines without using the **Schedule Push Image** process.

To patch selected VMs in the pool using the secondary image, perform the following steps.

- 1 In Horizon Console, select **Inventory > Desktops**
- 2 Click the pool ID.
- 3 On the **Summary** tab, click **Maintain > Schedule**.

The **Schedule Push Image** window opens.

- 4 On the Image step, select the secondary image and snapshot to use.

Note If you are a VMware Carbon Black customer and select a golden image configured with Carbon Black, then the screen displays information from the Carbon Black Scan for each snapshot listed.

- If you select the Show All Images check box, the list might include snapshots that are not compatible and cannot be selected.
 - If no value appears in the Carbon Black Scan (% Complete) column, that indicates that the Carbon Black sensor was not enabled in the Instant Clone golden image when the snapshot was taken. For more information, see the [VMware Carbon Black Cloud Documentation](#).
-

- 5 On the Schedule step, select the **Publish Secondary image** option.

To immediately apply the secondary image to selected machines, select the **Push to specific machines** check box and then select machines from the list.

- 6 On the Ready to Complete step, click **Finish**.

Switching Between the Default and Secondary Image

After you have published the secondary image, options are enabled on the **Machines (Instant Clone Details)** tab to apply either of the images to selected machines.

- To apply the secondary image, select the machines on the **Machines (Instant Clone Details)** page and then select **More Commands > Apply Secondary Image**.
- To apply the default image, select the machines on the **Machines (Instant Clone Details)** page and then select **More Commands > Apply Default Image**.

Promote or Cancel the Secondary Image

If the new image meets your acceptance criteria, you can promote this secondary image to be your default image. Otherwise, you can cancel the secondary image and the default image will get applied to the desktop pool.

- There is an option on the **Summary** tab to promote the secondary image. This causes the secondary image to become the new default image on the pool and applies it to all the machines in the pool. To promote the secondary image, select **Maintain > Promote Secondary Image**.
- To cancel the secondary image, select **Maintain > Cancel** on the **Summary** tab.
 - If the pool is set to refresh on logoff, the desktops that are currently on the secondary image will revert to the default image once the user logs off.
 - If the pool is not set to refresh on logoff, the desktops on the secondary image remain on it unless a recover, delete, or refresh is performed on the desktop.

Monitor a Push-Image Operation

You can monitor the progress of a push-image operation on an instant-clone desktop pool.

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Click the pool ID.

The **Summary** tab shows the current image and pending image information, including any push-image error messages.

3 Click the **Tasks** tab.

The list of tasks that are associated with the push-image operation appears.

Reschedule or Cancel a Push-Image Operation

You can reschedule or cancel a push-image operation on an instant-clone desktop pool.

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Click the pool ID.

The **Summary** tab shows the current image and pending image information.

3 Select **Maintain > Reschedule** or **Maintain > Cancel**.

4 Follow the prompts.

Results

If you reschedule or cancel the push-image operation while clone creation is in progress, the clones that have the new image remain in the pool and the pool has a mix of clones, some with the new image and the others with the old image. To ensure that all the clones have the same image, you can remove all the clones. Horizon 8 recreates the clones with the same image.

Perform Maintenance on Instant-Clone Hosts

You can perform maintenance on hosts where instant clones reside by putting the ESXi hosts into maintenance mode. You can use the vSphere client to put the ESXi host into maintenance mode.

In most cases, using instant clones does not change your operational flow of how you perform ESXi host maintenance tasks. Horizon 8 will automatically delete the instant clone parentVMs to allow the ESXi host to go into maintenance mode. When you use VMware Update Manager, an extra step is required.

If you use VMware Update Manager to update your ESXi hosts, you must delete or disable the instant clone parentVM before VMware Update Manager can successfully update the ESXi hosts. If you use an older version of Horizon, you must manually delete the instant clone parentVM on all the ESXi hosts by using the instant-clone utilities. To use the instant-clone utilities, see [Instant-Clone Maintenance Utilities](#).

Starting with Horizon 8 version 2006, you can globally disable all of the instant clone parentVMs in a vCenter so that VMware Update Manager can update the ESXi hosts in that vCenter. If you disable parentVM setting for a vCenter, Horizon 8 will automatically delete all the parentVMs on every single host in that vCenter, so that the hosts can go into maintenance mode without any manual intervention. Deleting the parentVM does not impact the operations of instant clones as Horizon 8 can create instant clones with or without parentVMs.

To selectively disable parentVMs for certain clusters only rather than the entire vCenter, see the KB article [80369](#). If you leave the parentVM setting for the vCenter disabled, any new instant clones are then provisioned without parentVMs. If you want Horizon 8 to use parentVMs when creating instant clones, then you can re-enable the parentVM setting for the vCenter after VMware Update Manager completes host maintenance. You must disable the parentVM for the vCenter before every update event.

Note If you use VMware Update Manager, keep the instant clone parentVMs disabled for your vCenter to simplify your ESXi maintenance.

Procedure

- 1 In Horizon Console, select **Settings > Servers**.
- 2 Select the server from the list, click **More** and select **Disable ParentVMs**.
- 3 Log in to vSphere client.
- 4 Select the ESXi host that you want to put into maintenance and click **Maintenance Mode > Enter Maintenance Mode**.

Instant-Clone Maintenance Utilities

On the Connection Server are three utilities that you can use for the maintenance of instant-clone VMs in vCenter Server and the clusters that the VMs are in.

The utilities are `IcMaint.cmd`, `IcUnprotect.cmd`, and `IcCleanup.cmd` and are located in `C:\Program Files\VMware\VMware View\Server\tools\bin`.

IcMaint.cmd

Typically, when you put the ESXi host into maintenance mode, Horizon will automatically delete the parent VM so that the host can go into maintenance mode without any manual intervention.

However, you can use this command to delete cp-parent VMs. The host is not automatically put into maintenance mode. To perform maintenance on the host, the vCenter Server administrator must manually put the host into maintenance mode.

Syntax:

```
IcMaint.cmd -vc hostname_or_IP_address -uid user_ID -hostName ESXi_hostname -maintenance ON|OFF
```

Parameters:

- `-vc` *host name or IP address of vCenter Server*
- `-uid` *vCenter Server user ID*
- `-hostname` *ESXi host name*
- `-maintenance` `ON|OFF`

This parameter specifies whether the host is available for hosting the golden image VM.

After the command is run on the host, the InstantClone.Maintenance annotation value is set to 1 and the golden image VMs are deleted. After the golden image VMs are deleted, the InstantClone.Maintenance annotation value is set to 2 and no more golden image VMs are created on the host. When you run this command again with `-maintenance OFF`, the InstantClone.Maintenance annotation value is cleared for the host to become available for hosting golden image VMs.

All the parameters are required.

IcUnprotect.cmd

After ClonePrep creates folders and VMs, you can use this utility to unprotect folders and VMs, delete VMs, and detect VMs whose golden image or snapshot is deleted. ClonePrep is the mechanism that customizes instant clones during the creation process.

Note An internal service for instant clones that runs during instant clone operations, detects if any internal folders need to be reprotected. If these folders are not empty then the service automatically protects the folders again.

Syntax:

```
IcUnprotect.cmd -vc hostname_or_IP_address -uid user_ID [-includeFolders][-skipCertVeri]
```

Parameters:

- `-action`

You can use the following options for this parameter:

- `unprotect`. Unprotect internal VMs.
- `delete`. Delete internal VMs.
- `detect`. Detect and list internal VMs whose golden image or snapshot is deleted.

If you don't specify the `-action` parameter, the internal VMs are unprotected by default.

- `-vc` *host name or IP address of vCenter Server*

- `-uid` *vCenter Server user ID*

- `-clientId` *instant-clone client ID* (Optional)

If `clientId` is not specified, protection is removed from all ClonePrep VMs in all data centers.

- `-domain` *domain name* (Optional)

You can use multiple domain names separated by comma and no space.

- `-host` *host name* (Optional)

You can use multiple host names separated by comma and no space.

- `-datastore datastore name` (Optional)

You can use multiple datastore names separated by comma and no space.

- `-vmName VM name` (Optional)

You can use multiple VM names separated by comma and no space.

- `-vmType internal VM type` (Optional)

You can use multiple VM types separated by comma and no space. You can use `template`, `replica`, `parent` as options for this parameter.

- `-includeFolders include folders`

This parameter unprotects the folders in addition to the VMs.

- `-skipCertVeri skip certification verification`

`IcUnprotect.cmd` enforces host name verification. You must enter the correct host name of the vCenter Server instead of its IP address when you specify the command parameters. To disable host name verification and use the IP address of vCenter Server instead, use `-skipCertVeri`.

Specify the following parameters to delete all parent VMs in vCenter Server:

```
IcUnprotect -action delete -vc <IP address of vCenter Server> -uid <vCenter Server user ID>
-clientId <instant clone client ID> -host <hostname 1>,<hostname 2> -vmType parent
```

Specify the following parameters to delete specific parent VMs in vCenter Server:

```
IcUnprotect -action delete -vc <IP address of vCenter Server> -uid <vCenter Server user ID>
-clientId <instant clone client ID> -host <hostname 1>,<hostname 2> -vmType parent -vmName
<parent VM name 1>,<parent VM name 2>
```

IcCleanup.cmd

You can use this utility to unprotect and delete some or all of the internal VMs created by instant clones. This utility also provides a list command to group internal VMs into the hierarchical structure according to their golden VM and the snapshot used to create the instant clone pool. The list command has a detect option which only reveals the internal VM groups with priming tag or snapshot missing. You can then unprotect and delete a specific group or all of these groups. You can also output all the groups into a disk file for future reference.

Syntax:

```
iccleanup.cmd -vc vcName -uid userId [-skipCertVeri] [-clientId clientUuid]
```

Parameters:

- `-vc host name or IP address of vCenter Server`
- `-uid vCenter Server user ID`

- `-skipCertVeri` *Skip the vCenter Server certificate verification (Optional)*
- `-clientId` *Client UUID, the unique ID for the server cluster made up of Connection Server and one or more replica servers. (Optional)*

Note To find the client UUID, log into Connection Server or any of the replica servers, run ADSI Edit. In **DC=vdi, dc=vmware, dc=int > OU=Properties > OU=Global > CN=Common**, find the value for `pae-GUID`, which is the value for the client UUID. If you do not specify the client UUID, the cleanup tool will deal with all the internal VMs. If you specify the client UUID, the cleanup tool will deal with only the internal VMs that belong to that particular client UUID.

Commands:

- `list` List some or all the internal VMs and present them in a hierarchical structure, also known as internal VM groups. Options include:
 - `-all` List all the internal VM groups
 - `-D, --detect` Detect mode lists only the internal VM groups with missing priming tag or snapshot
 - `-h, --help` Print the available usage and options for this command

After you run the `list` command, you can see qualified internal VMs presented in a hierarchical structure known as internal VM groups. For these internal VM groups, you can run these commands:

- `unprotect` Unprotect some or all the internal VM groups using these options:
 - `-all` Unprotect all the internal VMs. Without the `-I` option, you must specify `-all` to unprotect all the internal VM groups
 - `-I, --index` Unprotect a certain internal VM group
 - `-h, --help` Print the available usage and options for this command
- `delete` Delete some or all the internal VM groups
- `output` Output the internal VM groups into a disk file.
 - `-F, --file` File name to save the internal VM groups
 - `-h, --help` Print the available usage and options for this command
- `back` Return to the main menu
- `unprotect unprotect` some or all the internal VMs, including folders. Options include:
 - `-A, --adDomain` Domain name
 - `-H, --host` Host name
 - `-D, --datastore` Datastore name
 - `-T, --vmType` Internal VM type: template, replica, or parent

- `-N, --name` Internal VM name
- `-I, --includeFolders` Include the internal VM folders
- `-all` Unprotect all the internal VMs
- `-h, --help` Print the available usage and options for this command
- `delete` delete some or all internal VMs, including folders. Options include:
 - `-A, --adDomain` Domain name
 - `-H, --host` Host name
 - `-D, --datastore` Datastore name
 - `-T, --vmType` Internal VM type: template, replica, or parent
 - `-N, --name` Internal VM name
 - `-I, --includeFolders` Include the internal VM folders
 - `-all` Delete all the internal VMs
 - `-h, --help` Print the available usage and options for this command
- `exit` Log off vCenter Server and quit the program

Creating and Managing Automated Full-Clone Desktop Pools

5

With an automated desktop pool that contains full-clone virtual machines, you create a virtual machine template and Horizon 8 uses that template to create virtual machine desktops.

Depending on how you want the golden image to be managed, you can change the golden image and snapshot source in your pool from vCenter to Image Catalog or reverse. You must rebuild the virtual machine associated with the edited template source for the change to take effect. For more information on the Image Management Service, see the *Managing Horizon Images from the Cloud* document.

This chapter includes the following topics:

- [Worksheet for Creating an Automated Full-Clone Desktop Pool](#)
- [Create an Automated Full-Clone Desktop Pool](#)
- [Manually Customizing Machines](#)
- [Desktop Settings for Automated Full-Clone Desktop Pools](#)
- [Configuring 3D Rendering for Full-Clone Virtual Machine Pools](#)
- [Configure Full Clones with vSphere Virtual Machine Encryption](#)
- [Rebuild a Virtual Machine in a Full-Clone Desktop Pool](#)

Worksheet for Creating an Automated Full-Clone Desktop Pool

When you create an automated desktop pool of full clones, you can configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines

Category	Option	Description	Enter Your Value Here
Type	Select Automated Desktop Pool .		
vCenter Server	Select Full Virtual Machines and select the vCenter Server that manages the virtual machines in the pool.		
User assignment		The following settings determine how end users are assigned to the desktops in this pool.	
	Select Floating or Dedicated .	<p>Choose the type of user assignment:</p> <ul style="list-style-type: none"> ■ With a floating-assignment full clone, users get a random desktop every time they log in. When a user logs out, the desktop is returned to the pool and another user can log into that desktop. ■ With a dedicated-assignment full clone, each desktop is assigned to a specific user. Once a user is assigned a desktop, no other user can use the desktop. Users receive the same machine each time they log in. 	
	Enable Automatic Assignment	<p>In a dedicated-assignment pool, a machine is assigned to a user when the user first logs in to the pool. You can also explicitly assign machines to users.</p> <p>If you do not enable automatic assignment, you must explicitly assign a machine to each user.</p> <p>You can assign machines manually even when automatic assignment is enabled. See Assign a Machine to a User in a Dedicated-Assignment Pool.</p>	
	Enable Multi-User Assignment	<p>In a dedicated-assignment pool, you can assign multiple users to each machine in the pool.</p> <p>Multi-user assignment is not supported for automatic user assignment desktop pools.</p> <p>If an assigned user has a connected or disconnected session on a multi-user assignment machine, other assigned users will be unable to launch a session on that machine. See Assign a Machine to a User in a Dedicated-Assignment Pool.</p>	
Storage Optimization	Storage Policy Management: <ul style="list-style-type: none"> ■ Use VMware Virtual SAN ■ Do not use VMware Virtual SAN 	<p>Specify whether to use VMware vSAN, if available. vSAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of ESXi hosts.</p>	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
Desktop Pool Identification		The following settings allow you to identify and describe the pool you are creating.	
	ID	<p>The unique name that identifies the pool in Horizon Console.</p> <p>If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID.</p> <p>You cannot edit or change the Desktop Pool ID after you create the desktop pool.</p>	
	Display Name	The pool name that users see when they log in from a client device. If you do not specify a display name, the pool ID is displayed to users.	
	Access Group	<p>Select an access group in which to place the pool or leave the pool in the default root access group.</p> <p>If you use an access group, you can delegate managing the pool to an administrator who has a specific role.</p> <hr/> <p>Note Access groups are different from vCenter Server folders that store desktop virtual machines. You select a vCenter Server folder later in the wizard with other vCenter Server settings.</p>	
Provisioning Settings		The following settings allow you to provide details on how the pool is provisioned.	
	Enable Provisioning	<p>You can enable or disable virtual machine provisioning in the desktop pool. When you disable provisioning in the desktop pool, Horizon 8 stops provisioning new virtual machines for the desktop pool. After you disable provisioning, you can enable provisioning again.</p> <p>Before you change a desktop pool's configuration, you can disable provisioning to ensure that no new machines are created with the old configuration. You can also disable provisioning to prevent Horizon 8 from using additional storage when a pool is close to filling up the available space.</p> <p>When you create a desktop pool and disable this option, Horizon 8 creates a desktop pool without any virtual machines. If you edit a desktop pool and disable provisioning, Horizon 8 does not allow any new virtual machines to be provisioned in this desktop pool. End users can still connect to existing virtual machines.</p>	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Stop Provisioning on Error	You can direct Horizon 8 to stop provisioning or continue to provision virtual machines in a desktop pool after an error occurs during the provisioning of a virtual machine. If you leave this setting selected, you can prevent a provisioning error from recurring on multiple virtual machines.	
	Virtual Machine Naming	Choose whether to provision machines by manually specifying a list of machine names or by providing a naming pattern and the total number of machines.	
	Specify Names Manually	If you specify names manually, prepare a list of machine names and, optionally, the associated user names.	
	Start machines in maintenance mode		
	# Unassigned Machines Kept Powered On	The number must be a valid integer greater than 0 and less than or equal to the maximum number of names specified. The default is 1.	
	Use a Naming Pattern	If you use this naming method, provide the pattern. The pattern you specify is used as a prefix in all the machine names, followed by a unique number to identify each machine.	
	Provision Machines: <ul style="list-style-type: none"> ■ Machines on Demand ■ All Machines Up-Front 	<p>If you use a naming pattern and provision machines on demand, specify a minimum number of machines in the pool.</p> <p>The minimum number of machines is created when you create the pool.</p> <p>If you provision machines on demand, additional machines are created as users connect to the pool for the first time or as you assign machines to users.</p>	
	Maximum number of machines	<p>If you use a naming pattern, specify the total number of machines in the pool.</p> <p>You can also specify a minimum number of machines to provision when you create the pool.</p>	
	Number of spare (powered on) machines	<p>If you specify names manually or use a naming pattern, specify how many machines to keep available and powered on for new users.</p> <p>When you specify names manually, this option is called # Unassigned machines kept powered on.</p>	
	Virtual Device: Add vTPM Device to VMs	Select the check box to add a Virtual Trusted Platform Module (vTPM) device to VMs.	
vCenter Settings		The following settings describe vCenter attributes for the pool of desktops.	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Virtual Machine Template	Select the virtual machine template to use for creating the pool.	
	VM Folder Location	Select the folder in vCenter Server in which the desktop pool resides.	
	Host or Cluster	Select the ESXi host or cluster on which the virtual machines run.	
	Resource pool	Select the vCenter Server resource pool in which the desktop pool resides.	
	Datastores	<p>Choose the type of datastore:</p> <ul style="list-style-type: none"> ■ Individual datastore. Select individual datastores on which to store the desktop pool. ■ Storage DRS. Select the Storage Distributed Resource Scheduler (DRS) cluster that contains shared or local datastores. Storage DRS is a load balancing utility that assigns and moves storage workloads to available datastores. <p>Note If you use vSAN, there is only one datastore.</p>	
	Network	Select the network to use for this pool or use the same network as the golden image.	
Desktop Pool Settings		The following settings determine the desktop state, power status, and display protocol when a virtual machine is not in use.	
	State	<ul style="list-style-type: none"> ■ Enabled. After being created, the desktop pool is enabled and ready for immediate use. ■ Disabled. After being created, the pool is disabled and not available for use, and provisioning is stopped for the pool. Select this setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance. <p>When this state is in effect, remote desktops are unavailable for use.</p>	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Connection Server Restrictions	<ul style="list-style-type: none"> ■ No Restrictions. The desktop pool can be accessed by any Connection Server instance. ■ Restrictions to these Tags. Select one or more Connection Server tags to make the desktop pool accessible only to Connection Server instances that have those tags. You can use the check boxes to select multiple tags. <p>If you intend to provide access to desktops through VMware Identity Manager, and you configure Connection Server restrictions, the VMware Identity Manager application might display desktops to users when those desktops are actually restricted. VMware Identity Manager users will be unable to launch these desktops.</p>	
	Category Folder	Specifies the name of the category folder that contains a Start menu shortcut for the desktop pool entitlement on Windows client devices. For more information, see "Configuring Shortcuts for Entitled Pools" in the <i>Horizon Administration</i> document.	
	Client Restrictions	Select whether to restrict access to entitled desktop pools from certain client computers. You must add the names of the computers that are allowed to access the desktop pool in an Active Directory security group. You can select this security group when you add users or groups to the desktop pool entitlement.	
	Session Type	<p>You can enable the VM Hosted Applications feature by selecting the supported session type for the desktop pool:</p> <ul style="list-style-type: none"> ■ Desktop. Select this option to use the pool as a regular desktop pool. All the virtual machines in the pool can only be used to host desktops. ■ Application. Select this option to use all the virtual machines in the pool to host applications. ■ Desktop and Application. When this option is selected, the virtual machine in the pool can either host a regular desktop session or host an application session. The first connection to the particular virtual machine will determine the session type of the virtual machine. <p>For more information about the VM Hosted Applications feature, see the technical marketing white paper "Best Practices for Published Applications and Desktops in VMware Horizon and VMware Horizon Apps" available at https://techzone.vmware.com.</p>	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Remote Machine Power Policy	<p>Determines how a virtual machine behaves when the user logs off of the associated desktop.</p> <p>For descriptions of the power-policy options, see Power Policies for Desktop Pools.</p> <p>For more information about how power policies affect automated pools, see How Power Policies Affect Automated Desktop Pools.</p>	
	Log Off After Disconnect	<ul style="list-style-type: none"> ■ Immediately. Users are logged out when they disconnect. ■ Never. Users are never logged out. ■ After. The time after which users are logged off when they disconnect. Type the duration in minutes. <p>The logout time applies to future disconnections. If a desktop session is already disconnected when you set a logout time, the logout duration for that user starts when you set the logout time, not when the session was originally disconnected. For example, if you set this value to 5 minutes, and a session was disconnected 10 minutes earlier, Horizon 8 will log out of that session 5 minutes after you set the value.</p>	
	Bypass Session Timeout (Application and Desktop and Application session types)	<p>Enable this setting to allow application sessions to run forever. When enabled, all the application sessions belonging to the desktop pool are never disconnected automatically, neither when reaching the max session timeout nor when reaching the global idle timeout.</p> <p>This setting is available when you select session types Application and Desktop or Application.</p> <p>Application sessions that run forever are supported on Windows and Linux clients.</p> <p>You cannot enable this setting if any of the applications belonging to the desktop pool is part of Global Application Entitlement as local pools.</p> <p>This setting is not available for application pools in a cloud pod architecture environment.</p> <p>Application sessions that run forever are not supported for unauthenticated users.</p> <p>Do not enable this setting if the max session timeout value is set to Never.</p> <p>When you restart Connection Server, existing forever running application sessions no longer run indefinitely.</p>	
	Allow Users to Restart Machines	Allow users to reset or restart their own desktops.	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Empty session timeout (Applications only)	<p>Determines the amount of time that an empty application session remains open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log off empty application sessions. Select Never, Immediate, or set the number of minutes as the timeout value. The default is After 1 minute. If you select Immediate, the session logs off or disconnects within 30 seconds. You can further reduce the time the session logs off or disconnects by editing a registry key on the RDS Host on which Horizon Agent is installed. Navigate to</p> <pre>HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wsm\applaunchmgr\Params</pre> <p>and set a value for <code>WindowCheckInterval</code>. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session log off to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session log off to 5 seconds.</p>	
	Pre-launch session timeout (Applications only)	Determines the timeout for the application session before the session is disconnected or logged off.	
	When timeout occurs (Applications only)	Determines whether an empty application session is disconnected or logged off after the Empty session timeout limit is reached. Select Disconnect or Log off . A session that is logged out frees up resources, but opening an application takes longer. The default is Disconnect .	
	Show Assigned Machine Name	<p>Displays the host name of the assigned machine instead of the desktop pool display name when you log in to Horizon Client.</p> <p>If no machine is assigned to the user, then Display Name (No Machine Assigned) appears for the desktop pool when you log in to Horizon Client.</p>	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Show Machine Alias Name	<p>Displays the machine alias name set for the assigned users of the machine instead of the desktop display name for the desktop pool in Horizon Client. Applies only to dedicated desktop entitlements.</p> <p>If no machine alias name is set but the Show Assigned Machine Name is set, then the machine host name appears for the desktop pool in Horizon Client. Otherwise, the desktop display name appears for the desktop pool in Horizon Client.</p>	
	Delete machine on Logoff	<p>Select whether to delete floating assignment, full clone virtual machines.</p> <ul style="list-style-type: none"> ■ No. Virtual machines remain in the desktop pool after users log out. ■ Yes. Virtual machines are powered off and deleted as soon as users log out. <p>This option is not applicable for dedicated assignment, full clone virtual machines.</p>	
Remote Display Settings		The following settings describe how the desktops are displayed to the end-users.	
	Default Display Protocol	<p>VMware Blast. The VMware Blast Extreme protocol is built on the H.264 protocol and supports the broadest range of client devices, including smart phones, tablets, ultra-low-cost PCs, and Macs, across any network.</p> <p>PCoIP. PCoIP is supported as the display protocol for virtual and physical machines that have Teradici hardware. PCoIP provides an optimized PC experience for the delivery of images, audio, and video content for a wide range of users on the LAN or across the WAN.</p> <p>Microsoft RDP. Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data. RDP is a multichannel protocol that allows a user to connect to a computer remotely.</p>	
	Allow Users to Choose Protocol	Allow users to override the default display protocol for their desktops in Horizon Client.	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	3D Renderer	<p>You can configure the 3D Renderer to use software rendering or hardware rendering based on physical GPU graphics cards installed on hosts.</p> <p>If you select RDP as the Default Display Protocol, you must enable the Allow users to choose protocol setting (select Yes) to enable 3D rendering. If the default display protocol is RDP and you disable the Allow users to choose protocol setting (select No), the 3D rendering option is disabled.</p> <p>With the hardware-based 3D Renderer options, users can take advantage of graphics applications for design, modeling, and multimedia. With the software 3D Renderer option, users can take advantage of graphics enhancements in less demanding applications such as AERO, Microsoft Office, and Google Earth. For more details, see Configuring 3D Rendering for Full-Clone Virtual Machine Pools.</p> <p>When you edit this setting, you must power off existing virtual machines, verify that the machines are reconfigured in vCenter Server, and power on the machines to cause the new setting to take effect. Restarting a virtual machine does not cause the new setting to take effect.</p>	
	VRAM Size	The amount of 3D VRAM allocated to each desktop.	
	Maximum Number of Monitors	<p>If you select PCoIP or VMware Blast as the display protocol, you can select the maximum number of monitors on which users can display the desktop. You can select up to four monitors.</p> <p>When the 3DRenderer setting is not selected, the Max number of monitors setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the number of monitors, more memory is consumed on the associated ESXi hosts. Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution.</p> <p>When you edit the pool, you must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.</p>	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Maximum Resolution of Any One Monitor	<p>If you select PCoIP or VMware Blast as the display protocol, you should specify the maximum resolution of any one monitor.</p> <p>The maximum resolution of any one monitor is set to 1920 x 1200 pixels by default, but you can configure this value.</p> <p>When the 3D Renderer setting is not selected, the Max resolution of any one monitor setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the resolution, more memory is consumed on the associated ESXi hosts.</p> <p>Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution.</p> <p>When you edit the pool, you must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.</p>	
	Allow Session Collaboration	Select Enabled to allow users of the desktop pool to invite other users to join their remote desktop sessions. Session owners and session collaborators must use the VMware Blast protocol.	
Advanced Storage Options		The following settings are for advanced storage options.	
	Use View Storage Accelerator	<p>Determine whether ESXi hosts cache common virtual machine disk data. View Storage Accelerator can improve performance and reduce the need for extra storage I/O bandwidth to manage boot storms and anti-virus scanning I/O storms. This feature is enabled by default.</p> <p>Note The Horizon console does not save the blackout times if you add or delete blackout times and then disable View Storage Accelerator.</p>	
	Regenerate Storage Accelerator After	Select the number of days to regenerate the Storage Accelerator. Add blackout days and times in the Set Blackout Days window.	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Transparent Page Sharing Scope	<p>Select the level at which to allow transparent page sharing (TPS). The choices are Virtual Machine (the default), Pool, Pod, or Global. If you turn on TPS for all the machines in the pool, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications.</p> <p>Page sharing happens on the ESXi host. For example, if you enable TPS at the pool level but the pool is spread across multiple ESXi hosts, only virtual machines on the same host and within the same pool will share pages. At the global level, all machines managed by VMware Horizon on the same ESXi host can share memory pages, regardless of which pool the machines reside in.</p> <hr/> <p>Note The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.</p>	
Guest Customization	Guest customization	<p>Select a customization specification (SYSPREP) from the list to configure licensing, domain attachment, DHCP settings, and other properties on the machines. You can only select a customization specification that matches the guest operating system of the template.</p> <p>Alternatively, you can customize the machines manually after they are created.</p>	
	Allow Reuse of Existing Computer Accounts	<p>Select this option to allow reuse of previously used machine names.</p> <hr/> <p>Note Rebuild operation does not take this setting into consideration and always reuses the machine name.</p>	

Create an Automated Full-Clone Desktop Pool

You can create an automated desktop pool based on a virtual machine template that you select. Horizon 8 dynamically deploys the desktops, creating a new virtual machine in vCenter Server for each desktop.

Prerequisites

- Prepare a virtual machine template that Horizon 8 will use to create the machines. Horizon Agent must be installed on the template. See [Chapter 3 Creating and Preparing a Virtual Machine for Cloning](#).
- If you intend to use a customization specification, make sure that the specifications are accurate. In vSphere Client, deploy and customize a virtual machine from your template using the customization specification. Fully test the resulting virtual machine, including DHCP and authentication.
- Verify that you have a sufficient number of ports on the ESXi virtual switch that is used for the virtual machines that are used as remote desktops. The default value might not be sufficient if you create large desktop pools. The number of virtual switch ports on the ESXi host must equal or exceed the number of virtual machines multiplied by the number of virtual NICs per virtual machine.
- Gather the configuration information you must provide to create the pool. See [Worksheet for Creating an Automated Full-Clone Desktop Pool](#).
- If you intend to provide access to your desktops and applications through VMware Workspace ONE Access, verify that you create the desktop and application pools as a user who has the Administrators role on the root access group in Horizon Administrator. If you give the user the Administrators role on an access group other than the root access group, VMware Workspace ONE Access will not recognize the SAML authenticator you configure in Horizon 8, and you cannot configure the pool in VMware Workspace ONE Access.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Click **Add**.
- 3 Select **Automated Desktop Pool** and click **Next**.
- 4 Select **Full Virtual Machines**, select the vCenter Server instance, and click **Next**.
- 5 Follow the prompts to create the pool.

Use the configuration information you gathered in the worksheet. You can go directly back to any wizard page by clicking the page name in the navigation pane.

What to do next

Entitle users to access the pool. See "Entitling Users and Groups" in the *Horizon Administration* document.

Manually Customizing Machines

After you create an automated pool, you can customize particular machines without reassigning ownership. By starting the machines in maintenance mode, you can modify and test the machines before you release them to users.

Maintenance mode prevents users from accessing their desktops. If you start machines in maintenance mode, Horizon 8 places each machine in maintenance mode when the machine is created. In a dedicated-assignment pool of full virtual machines, you can use maintenance mode to log in to a machine without having to reassign ownership to your own administrator account. When you finish the customization, you do not have to return ownership to the user assigned to the machine.

To perform the same customization on all machines in an automated pool, customize the virtual machine you prepare as a template. Horizon 8 deploys your customization to all the machines.

Note You can start machines in maintenance mode if you manually specify machine names for the pool, not if you name machines by providing a naming pattern.

Customize Machines by Placing Them in Maintenance Mode After Pool Creation

After a desktop pool is created, you can customize, modify, or test individual machines by placing them in maintenance mode. When a machine is in maintenance mode, users cannot access the virtual machine desktop.

You place existing machines in maintenance mode one at a time. You can remove multiple machines from maintenance mode in one operation.

When you create a desktop pool, you can start all the machines in the pool in maintenance mode if you specify machine names manually.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Click the link for the pool.
- 3 Select the **Machines** tab.
- 4 Select a machine.
- 5 Select **Enter Maintenance Mode** from the **More Commands** drop-down menu.
- 6 Customize, modify, or test the virtual machine desktop.
- 7 Repeat steps to select a machine and customize, modify, or test the virtual machine desktop.
- 8 Select the customized machines and select **Exit Maintenance Mode** from the **More Commands** drop-down menu.

Results

The modified virtual machine desktops are available to users.

Customize Machines by Starting Them in Maintenance Mode During Pool Creation

You can customize individual machines after a pool is created by starting the machines in maintenance mode.

Procedure

- 1 In Horizon Console, begin creating an automated desktop pool by starting the **Add Pool** wizard.
- 2 On the Provisioning Settings page, select **Specify names manually**.
- 3 Select **Start machines in maintenance mode**.
- 4 Complete the **Add Pool** wizard to finish creating the desktop pool.
- 5 In vCenter Server, log in, customize, and test the individual virtual machines.
You can customize the machines manually or by using standard Windows systems-management software such as Altiris, SMS, LanDesk, or BMC.
- 6 In Horizon Console, select **Inventory > Machines**.
- 7 Select specific machines to release to your users.
- 8 Click **More Commands > Exit Maintenance Mode**.

What to do next

Notify your users that they can log in to their desktops.

Desktop Settings for Automated Full-Clone Desktop Pools

You must specify desktop pool settings when you configure automated pools that contain full-clone virtual machines. Different settings apply to pools with dedicated user assignments and floating user assignments.

Settings for Automated Pools That Contain Full-Clone Virtual Machines lists the differences in settings.

Table 5-2. Settings for Automated Pools That Contain Full-Clone Virtual Machines

Setting	Automated Pool, Dedicated Assignment	Automated Pool, Floating Assignment
State	Yes	Yes
Connection Server restrictions	Yes	Yes
Remote machine power policy	Yes	Yes
Automatic logoff after disconnect	Yes	Yes
Allow users to reset/restart their machines	Yes	Yes

Table 5-2. Settings for Automated Pools That Contain Full-Clone Virtual Machines (continued)

Setting	Automated Pool, Dedicated Assignment	Automated Pool, Floating Assignment
Allow user to initiate separate sessions from different client devices		Yes
Delete machine after logoff		Yes
Default display protocol	Yes	Yes
Allow users to choose protocol	Yes	Yes
3D Renderer	Yes	Yes
Max number of monitors	Yes	Yes
Max resolution of any one monitor	Yes	Yes
Override global Mirage settings	Yes	Yes
Mirage Server configuration	Yes	Yes
Enable Multi-User Assignment	Yes	
Display Assigned Machine Name	Yes	

Configuring 3D Rendering for Full-Clone Virtual Machine Pools

When you create or edit a desktop pool of virtual machines, you can configure 3D graphics rendering for your desktops.

End users can take advantage of 3D applications for design, modeling, and multimedia, which typically require GPU hardware to perform well. For users that do not require physical GPU, a software option provides graphics enhancements that can support less demanding applications such as Windows AERO, Microsoft Office, and Google Earth. Following are brief descriptions of the 3D graphics options:

NVIDIA GRID vGPU (shared GPU hardware acceleration)

This feature allows a physical GPU on an ESXi host to be shared among virtual machines and offers flexible hardware-accelerated 3D profiles ranging from lightweight 3D task workers to high-end workstation graphics power users.

AMD MxGPU

This feature allows multiple virtual machines to share an AMD GPU by making the GPU appear as multiple PCI passthrough devices and offers flexible hardware-accelerated 3D profiles, ranging from lightweight 3D task workers to high-end workstation graphics power users.

Virtual Dedicated Graphics Acceleration (vDGA)

This feature dedicates a single physical GPU on an ESXi host to a single virtual machine. Use this feature if you require high-end, hardware-accelerated workstation graphics.

Note See the VMware Hardware Compatibility List at <http://www.vmware.com/resources/compatibility/search.php>. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

Virtual Shared Graphics Acceleration (vSGA)

This feature allows multiple virtual machines to share the physical GPUs on ESXi hosts and is suitable for mid-range 3D design, modeling, and multimedia applications.

Soft 3D

Software-accelerated graphics allow you to run DirectX 9 and OpenGL 2.1 applications without requiring a physical GPU. Use this feature for less demanding 3D applications such as Windows Aero themes, Microsoft Office 2010, and Google Earth.

AMD MxGPU and vDGA solutions do not support VMotion. NVIDIA GRID vGPU, vSGA and Soft 3D support VMotion.

In some cases, if an application such as a video game or 3D benchmark forces the desktop to display in full screen resolution, the desktop session can be disconnected. Possible workarounds include setting the application to run in Windowed mode or matching the Horizon 8 session desktop resolution to the default resolution expected by the application.

3D Renderer Options for Full-Clone Virtual Machine Pools

The **3D Renderer** setting for full-clone virtual machine pools provides options that let you configure graphics rendering in different ways.

The following table describes the differences between the various types of 3D rendering options available in Horizon 8, but does not provide complete information for configuring virtual machines and ESXi hosts for Virtual Shared Graphics Acceleration (vSGA), Virtual Dedicated Graphics Acceleration (vDGA), AMD MxGPU, and NVIDIA GRID vGPU. These tasks must be done with vSphere Client before you attempt to create desktop pools in Horizon Console. For instructions about these tasks for vSGA and vDGA, see the [VMware white paper](#) about graphics acceleration. For instructions about NVIDIA GRID vGPU, see the [NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1](#). For instructions about AMD MxGPU Using vDGA, see the [Preparing for AMD MxGPU for Full-Clone Virtual Machines](#).

Table 5-3. 3D Renderer Options

Option	Description
Manage using vSphere Client	<p>The 3D Renderer option that is set in vSphere Web Client for a virtual machine determines the type of 3D graphics rendering that takes place. Horizon 8 does not control 3D rendering.</p> <p>In the vSphere Client, you can configure the Automatic, Software, or Hardware options. These options have the same effect as they do when you set them in Horizon Console.</p> <p>Use this setting when configuring vDGA and AMD MxGPU. This setting is also an option for vSGA.</p> <p>When you select the Manage using vSphere Client option, the Configure VRAM for 3D Guests, Max number of monitors, and Max resolution of any one monitor settings are inactive in Horizon Console. You can configure the amount of memory in vSphere Client.</p>
Automatic	<p>3D rendering is enabled. The ESXi host controls the type of 3D rendering that takes place.</p> <p>For example, the ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. If all GPU hardware resources are already reserved when a virtual machine is powered on, ESXi uses the software renderer for that machine.</p> <p>This setting is an option when configuring vSGA.</p> <p>The ESXi host allocates VRAM to a virtual machine based on the value that is set in the Configure VRAM for 3D Guests dialog box.</p>
Software	<p>3D rendering is enabled. The ESXi host uses software 3D graphics rendering. If a GPU graphics card is installed on the ESXi host, this pool will not use it.</p> <p>Use this setting to configure Soft 3D.</p> <p>The ESXi host allocates VRAM to a virtual machine based on the value that is set in the Configure VRAM for 3D Guests dialog box.</p>
Hardware	<p>3D rendering is enabled. The ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on.</p> <p>This setting is an option when configuring vSGA.</p> <p>The ESXi host allocates VRAM to a virtual machine based on the value that is set in the Configure VRAM for 3D Guests dialog box.</p> <p>Important If you configure the Hardware option, consider these potential constraints:</p> <ul style="list-style-type: none"> ■ If a user tries to connect to a machine when all GPU hardware resources are reserved, the virtual machine will not power on, and the user will receive an error message. ■ If you use vMotion to move the machine to an ESXi host that does not have GPU hardware configured, the virtual machine will not power on. <p>When you configure hardware-based 3D rendering, you can examine the GPU resources that are allocated to each virtual machine on an ESXi host. For details, see Examining GPU Resources on an ESXi Host.</p>

Table 5-3. 3D Renderer Options (continued)

Option	Description
NVIDIA GRID vGPU	<p>3D rendering is enabled for NVIDIA GRID vGPU. The ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. If a user tries to connect to a machine when all GPU hardware resources are being used by other virtual machines on the host, Connection Server will attempt to move the virtual machine to another ESXi host in the cluster before powering on.</p> <p>Use this setting when configuring NVIDIA GRID vGPU.</p> <p>When you select the NVIDIA GRID vGPU option, the Configure VRAM for 3D Guests, Max number of monitors, and Max resolution of any one monitor settings are inactive in Horizon Console. When you configure the golden image virtual machine or virtual machine template with vSphere Web Client, you are prompted to reserve all memory.</p> <hr/> <p>Important If you configure the NVIDIA GRID vGPU option, consider these potential constraints:</p> <ul style="list-style-type: none"> ■ The virtual machine cannot be suspended or resumed. Therefore the Remote Machine Power Policy option for suspending the virtual machine is not available. ■ If you use vMotion to move the machine to an ESXi host that does not have GPU hardware configured, the virtual machine will not power on. Live vMotion is not available. ■ All ESXi hosts in the cluster must be version 6.0 or later, and the virtual machines must be hardware version 11 or later. ■ If an ESXi cluster contains a host that is NVIDIA GRID vGPU enabled and a host that is not NVIDIA GRID vGPU enabled, the hosts display a yellow (warning) status in the Horizon Console Dashboard. If a user tries to connect to a machine when all GPU hardware resources are being used by other virtual machines on the host, Connection Server will attempt to move the virtual machine to another ESXi host in the cluster before powering on. In this case, hosts that are not NVIDIA GRID vGPU enabled cannot be used for this type of dynamic migration. <hr/>
Disabled	3D rendering is inactive.

Best Practices for Configuring 3D Rendering For Full-Clone Virtual Machine Pools

The 3D rendering options and other pool settings offer various advantages and drawbacks. Select the option that best supports your vSphere hardware infrastructure and your users' requirements for graphics rendering.

Note For detailed information about all the various choices and requirements for 3D rendering, see the [VMware white paper](#) about graphics acceleration.

When to Choose the Automatic Option

The **Automatic** option is the best choice for many Horizon 8 deployments that require 3D rendering. vSGA (Virtual Shared Graphics Acceleration)-enabled virtual machines can dynamically switch between software and hardware 3D rendering, without your having to reconfigure. This option ensures that some type of 3D rendering takes place even when GPU resources are completely reserved.

The only drawback with the **Automatic** option is that you cannot easily tell whether a virtual machine is using hardware or software 3D rendering.

When to Choose the Hardware Option

The **Hardware** option guarantees that every virtual machine in the pool uses hardware 3D rendering, provided that GPU resources are available on the ESXi hosts. This option might be the best choice when all your users run graphically intensive applications. You can use this option when configuring vSGA (Virtual Shared Graphics Acceleration).

With the **Hardware** option, you must strictly control your vSphere environment. All ESXi hosts must have GPU graphics cards installed.

When all GPU resources on an ESXi host are reserved, Horizon 8 cannot power on a virtual machine for the next user who tries to log in to a desktop. You must manage the allocation of GPU resources and the use of vMotion to ensure that resources are available for your desktops.

When to Choose the Option to Manage Using vSphere Client

When you select the **Manage using vSphere Client** option, you can use vSphere Client to configure individual virtual machines with different options and VRAM values.

- For vSGA (Virtual Shared Graphics Acceleration), you can support a mixed configuration of 3D rendering and VRAM sizes for virtual machines in a pool.
- For vDGA (Virtual Dedicated Graphics Acceleration), each virtual machine must be individually configured to share a specific PCI device with the ESXi host and all memory must be reserved. For more information, see [Preparing for vDGA Capabilities for Full-Clone Virtual Machines](#).

All ESXi hosts must have GPU graphics cards installed.

Note See the VMware Hardware Compatibility List at <http://www.vmware.com/resources/compatibility/search.php>. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

- For AMD MxGPU, each virtual machine must be individually configured to share a specific PCI device with the ESXi host and all memory must be reserved. This feature allows a PCI device to appear to be multiple separate physical PCI devices so that the GPU can be shared between 2 to 15 users. For more information, see [Preparing for AMD MxGPU for Full-Clone Virtual Machines](#).

All ESXi hosts must be version 6.0 or later and must have GPU graphics cards installed.

You might also choose this option if you want to explicitly manage graphics settings of clones by having the clones inherit settings from the golden image virtual machine.

When to Choose the NVIDIA GRID vGPU Option

With the **NVIDIA GRID vGPU** option, you can achieve a higher consolidation ratio of virtual machines on an NVIDIA GRID vGPU-enabled ESXi host than is possible by using vDGA, while maintaining the same performance level. As with vDGA (Dedicated Virtual Graphics), the ESXi and virtual machine also use GPU pass-through for NVIDIA GRID vGPU.

Note To improve virtual machine consolidation ratios, you can set the ESXi host to use consolidation mode. Edit the `/etc/vmware/config` file on the ESXi host and add the following entry:

```
vGPU.consolidation = "true"
```

By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is called performance mode. If you would rather have the ESXi host assign virtual machines to the same physical GPU until the maximum number of virtual machines is reached before placing virtual machines on the next physical GPU, you can use consolidation mode.

Because a GPU does not need to be dedicated to one specific virtual machine, with the **NVIDIA GRID vGPU** option, you can create and configure a golden image virtual machine or virtual machine template to be NVIDIA GRID vGPU-enabled and then create a desktop pool of virtual machines that can share the same physical GPU.

If all GPU resources on an ESXi host are being used by other virtual machines, when the next user tries to log in to a desktop, Horizon 8 can move the virtual machine to another NVIDIA GRID vGPU-enabled ESXi server in the cluster and then power on the virtual machine. All ESXi hosts must be version 6.0 or later and must have GPU graphics cards installed.

For more information, see [Preparing for NVIDIA GRID vGPU Capabilities for Full-Clone Virtual Machines](#).

When to Choose the Software Option

Select the **Software** option if your ESXi hosts do not have GPU graphics cards, or if your users only run applications such as AERO and Microsoft Office, which do not require hardware graphics acceleration.

Configuring Desktop Settings to Manage GPU Resources

You can configure other desktop settings to ensure that GPU resources are not wasted when users are not actively using them.

For floating pools, set a session timeout so that GPU resources are freed up for other users when a user is not using the desktop.

For dedicated pools, you can configure the **Automatically logoff after disconnect** setting to **Immediately** and a **Suspend** power policy if these settings are appropriate for your users. For example, do not use these settings for a pool of researchers who execute long-running simulations. Note that the **Suspend** power policy is not available if you use the **NVIDIA GRID vGPU** option.

Preparing for NVIDIA GRID vGPU Capabilities for Full-Clone Virtual Machines

NVIDIA GRID vGPU provides direct access to the physical GPU on an ESXi host, allowing multiple VMs to share a single GPU using vendor graphics card drivers.

Follow these instructions to configure VMs and ESXi hosts to create NVIDIA GRID vGPU-enabled desktop pools in Horizon 8. For complete information and detailed procedures, see the *NVIDIA vGPU Deployment Guide for VMware Horizon 7.5 on vSphere 6.7* document.

- 1 Verify the host machine is supported in the [VMware Compatibility Guide](#), and check with the vendor to verify the host meets power and configuration requirements. Install the graphics card in the ESXi host.
- 2 Verify that the guest virtual machines run with virtual hardware version 11 or later. Configure the virtual machine template to use a shared PCI device before you create the desktop pool in Horizon 8. For detailed instructions, see the *NVIDIA vGPU Deployment Guide for VMware Horizon 7.5 on vSphere 6.7* document.
- 3 Download the NVIDIA vSphere Installation Bundle (VIB) for the appropriate version of ESXi. VIBs are compatible with major version releases. For instance, the NVIDIA ESXi 6.5 VIB works with ESXi 6.5U2, but will not work with ESXi 6.7.
- 4 Update VMware Tools and Virtual Hardware (vSphere Compatibility) for the template or each VM that will use vGPU.
- 5 In the vSphere Web Client, edit the VM settings and add a shared PCI device. PCI devices require reserving guest memory. Expand **New PCI Device** and click **Reserve all guest memory**. You can also modify this setting in the VM Memory settings.
- 6 Select the appropriate GPU Profile for your use case. For sizing guidelines, see the *NVIDIA vGPU Deployment Guide for VMware Horizon 7.5 on vSphere 6.7* document.
- 7 Download the NVIDIA Guest Driver installer package to the VM. Make sure it matches the version of the installed NVIDIA VIB on ESXi.
- 8 Choose one of the following methods to install the NVIDIA Guest Driver. After the NVIDIA driver is installed, vCenter Server console will display a black screen.
 - Desktop Pool
 - View Agent Direct-Connection Plug-in
 - RDP

vMotion of vGPU Virtual Machines

- vMotion of vGPU Virtual Machines is supported starting with vSphere 6.7. See [here](#) for details on how to configure this and more information.
- vSphere Distributed Resource Scheduler (DRS) in vSphere 6.7 Update 1 and later supports initial placement of vGPU VMs without load balancing support.
- DRS in vSphere 6.7 or vSphere 7.0 versions earlier than vSphere 7.0 U3f will not automatically vMotion vGPU VMs when ESXi hosts are placed in maintenance mode. An administrator is required to manually initiate vMotion of vGPU VMs in order to allow ESXi hosts to enter maintenance mode.
- DRS in vSphere 7.0 U3f and later can be configured to allow automatic vMotion when hosts are placed in maintenance mode. See <https://kb.vmware.com/s/article/88271> for instructions. DRS load balancing remains unsupported for vGPU VMs.

Desktop Pool

This method is for creating a template VM.

- 1 Install Horizon Agent.
- 2 Configure domain and other network settings, as needed.
- 3 Configure the VMs as desktops in the pool.
- 4 Assign admin level access to accounts.
- 5 Connect Horizon Client to Horizon Console to access desktops.
- 6 Install NVIDIA driver, reboot, and reconnect.
- 7 Access NVIDIA Control Panel and enter license server information.

View Agent Direct-Connection Plug-in

This method is for a quick environment verification, or a simple user level access.

- 1 Install Horizon Agent.
- 2 Install the matching View Agent Direct-Connection Plug-in. You need local administrator account access.
- 3 Log in with Horizon Client. Use the VM IP address as Connection Server.
- 4 Install NVIDIA driver, reboot, and reconnect.
- 5 Access NVIDIA Control Panel and enter license server information.

RDP

This method is for creating a template VM before installing Horizon Agent.

- 1 Enable Remote Desktop access in the VMs.
- 2 Log in using Microsoft Remote Desktop Connection.

- 3 Install NVIDIA driver, reboot, and reconnect.
- 4 Access NVIDIA Control Panel and enter license server information.
- 5 Install Horizon Agent.
- 6 Configure domain and other network settings, as needed.

In the **Add Desktop Pool** wizard, select the NVIDIA GRID vGPU option for 3D Renderer and only NVIDIA GRID vGPU-enabled ESXi hosts and NVIDIA GRID vGPU-enabled virtual machine templates appear for selection in the wizard. VMware recommends using the default Blast settings for the pool protocol. For additional protocol options and other advanced configuration settings, consult the following guides:

- *NVIDIA vGPU Deployment Guide for VMware Horizon 7.5 on vSphere 6.7*
- *NVIDIA GRID vGPU User Guide*

You can use the same vGPU profile for a mix of full clones and instant clones. If you use different vGPU profiles for a mix of full clones and instant clones, avoid creating or powering on full clones and instant clones at the same time. See the VMware Knowledge Base (KB) article <https://kb.vmware.com/s/article/57297> to set the host assignment policy to GPU consolidation.

Preparing for vDGA Capabilities for Full-Clone Virtual Machines

Virtual Dedicated Graphics Acceleration (vDGA) provides direct pass-through to a physical GPU, providing a user with unrestricted, dedicated access to a single GPU. Before you attempt to create a desktop pool that has vDGA capabilities, you must perform certain configuration tasks on the virtual machines and ESXi hosts.

This overview is an outline of tasks you must perform in vSphere before you can create or configure desktop pools in Horizon Console.

Note See the VMware Hardware Compatibility List at <http://www.vmware.com/resources/compatibility/search.php>. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

- 1 Install the graphics card on the ESXi host.
- 2 Verify that VT-d or AMD IOMMU is enabled on the ESXi host.
- 3 Enable pass-through for the GPU in the ESXi host configuration and reboot.
- 4 Add a PCI device to the virtual machine and select the appropriate PCI device to enable GPU pass-through on the virtual machine.
- 5 Reserve all memory when creating the virtual machine.
- 6 Configure virtual machine video card 3D capabilities.
- 7 Obtain the GPU drivers from the GPU vendor and install the GPU device drivers in the guest operating system of the virtual machine.
- 8 Install VMware Tools and Horizon Agent in the guest operating system and reboot.

- 9 The virtual machines must be virtual hardware version 9 or later.
- 10 Enable GPU pass-through on the ESXi hosts and configure the individual virtual machines to use dedicated PCI devices after the desktop pool is created in Horizon 8. You cannot configure the golden image virtual machine or template for vDGA and then create a desktop pool, because the same physical GPU would be dedicated to every virtual machine in the pool. See "vDGA Installation" in the [VMware white paper](#) about graphics acceleration.
- 11 Set the 3D Renderer option to **Manage using vSphere Client**.

After you perform these tasks, you must add the virtual machine to a manual desktop pool so that you can access the guest operating system using PCoIP or VMware Blast Extreme. In a PCoIP or VMware Blast session, you can then activate the NVIDIA, AMD, or Intel display adapter in the guest operating system.

Preparing for AMD MxGPU for Full-Clone Virtual Machines

With AMD MxGPU, multiple virtual machines to share an AMD GPU by making the GPU appear as multiple PCI passthrough devices. AMD MxGPU provides direct pass-through to a physical GPU, providing a user with unrestricted, dedicated access to a single GPU.

Before you attempt to create a desktop pool that has capabilities to use AMD MxGPU, you must perform certain configuration tasks on the virtual machines and ESXi hosts.

This overview is an outline of tasks you must perform in vSphere before you can create or configure desktop pools in Horizon 8. For information about enabling GPU device pass-through and adding a PCI device to a virtual machine, see the [VMware white paper](#) about graphics acceleration.

- 1 Install the graphics card on the ESXi host.
- 2 Install the GPU vSphere Installation Bundle (VIB).
- 3 Verify that SR-IOV and VT-d or AMD IOMMU are enabled on the ESXi host.
- 4 Use the `esxcfg-module` command to configure the graphics card for SR-IOV (Single Root I/O Virtualization) .

See [Configuring AMD MxGPU](#).

- 5 Reboot the ESXi host.
- 6 Add a PCI device to the virtual machine and select the appropriate PCI device to enable GPU pass-through on the virtual machine.
- 7 Verify that the guest virtual machines have virtual hardware version 11 or later.
- 8 Reserve all memory when creating the virtual machine.
- 9 Configure virtual machine video card 3D capabilities.
- 10 Obtain the GPU drivers from the GPU vendor and install the GPU device drivers in the guest operating system of the virtual machine.
- 11 Install VMware Tools and Horizon Agent in the guest operating system and reboot.

12 Set the 3D Renderer option to **Manage using vSphere Client**.

After you perform these tasks, you must add the virtual machine to a manual desktop pool so that you can access the guest operating system using PCoIP or VMware Blast Extreme. If you attempt to access the virtual machine using a vSphere, the display will show a black screen.

Configuring AMD MxGPU

You use the `esxcfg-module` command-line command to configure such parameters as the number of users who can share the GPU, the amount of frame buffer allocated to each user, and some performance control.

Syntax

```
esxcfg-module -s "adapter1_conf=bus#,device#,function#,number_of_VFs,FB_size,time_slice,mode"
amdgpuv
```

Usage Notes

The `vicfg-module` command supports setting and retrieving VMkernel module options on an ESXi host. For general reference information about this command, see the *vSphere Command-Line Interface Reference* documentation at <https://code.vmware.com>.

Required Flags

You must specify several flags when configuring AMD MxGPU. If the command does not include all the required flags, no error message is provided, but the configuration defaults to a simple 4 SR-IOV device configuration.

Table 5-4. Flags for Configuring AMD SR-IOV

Flag	Description
<code>bus#</code>	Bus number in decimal format.
<code>device#</code>	<p>PCIe device ID for the supported AMD card, in decimal format. To see a list, use the command <code>lspci grep -i display</code>.</p> <p>For example, for a system that has two AMD GPU cards, you might see the following output when you run this command:</p> <pre>[root@host:~] lspci grep -i display 0000:04:00.0 Display controller: 0000:82:00.0 Display controller:</pre> <p>In this example, the PCIe device IDs are 04 and 82. Note that these IDs are listed in hexadecimal format and must be converted to decimal format for use in the <code>vicfg-module</code> command.</p> <p>AMD S7150 cards support only a single GPU per card, and so the device ID and function ID are 0 for these cards.</p>
<code>function#</code>	Function number in decimal format.
<code>number_of_VFs</code>	Number of VFs (virtual functions), from 2 to 15. This number represents the number users who will share the GPU.

Table 5-4. Flags for Configuring AMD SR-IOV (continued)

Flag	Description
<i>FB_size</i>	Amount of frame buffer memory, in MB, allocated to each VF. To determine the size, take the overall amount of video memory on the card and divide that amount by the number of VFs. Then round that number to the nearest number that is a multiple of 8. For example, for an AMD S7150 card, which has 8000 MB, you could use the following settings; <ul style="list-style-type: none"> ■ For 2 VFs, use 4096. ■ For 4 VFs, use 2048. ■ For 8 VFs, use 1024. ■ For 15 VFs, use 544.
<i>time_slice</i>	Interval between VF switches, in microseconds. This setting adjusts the delay in queuing and processing commands between the SR-IOV devices. Use a value between 3000 and 40000. Adjust this value if you see significant stuttering when multiple SR-IOV desktops are active.
<i>mode</i>	Following are the valid values: 0 = reclaimed performance; 1 = fixed percentage performance.

Important After you run the `esxcfg-module` command, you must reboot the ESXi host for the settings to take effect.

Examples

- 1 For a single AMD S7150 card on PCI ID 4 shared between 8 users:

```
esxcfg-module -s "adapter1_conf=4,0,0,8,1024,4000" amdgpv
```

- 2 For a single server with two AMD S7150 cards on PCI ID 4 and PCI ID 82 shared between 4 power users:

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,2,4096,4000" amdgpv
```

- 3 For a single server with two AMD S7150 cards, you can set each card with different parameters. For instance if your View environment needs to support 2 power users and 16 task workers:

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,15,544,7000" amdgpv
```

- 4 Enable the SR-IOV option on the ESXi host.

Some hosts have SR-IOV as a configurable option in the BIOS.

Preparing to Use vSGA for Full-Clone Virtual Machines

vSGA allows multiple virtual machines to share the physical GPUs on ESXi hosts.

To support vSGA, a pool must meet these additional requirements:

- GPU graphics cards and the associated vSphere Installation Bundles (VIBs) must be installed on the ESXi hosts. For a list of supported GPU hardware, see the VMware Hardware Compatibility List at <http://www.vmware.com/resources/compatibility/search.php>.
- The virtual machines must be virtual hardware version 10 or later.
- You can set the 3D Renderer option to any of the following settings: **Manage using vSphere Client**, **Automatic**, or **Hardware**. See [Video RAM Configuration Options for the 3D Renderer](#). **Automatic** uses hardware acceleration if there is a capable and available hardware GPU in the ESXi host. If a hardware GPU is not available, the virtual machine uses software 3D rendering for any 3D tasks.

Preparing to Use Soft 3D for Full-Clone Virtual Machines

When you enable Soft 3D, ESXi host uses software 3D graphics rendering.

To support software 3D rendering, a pool must meet these additional requirements:

- The machines must be virtual hardware version 8 or later.
- You must set the 3D Renderer option to **Software**. See [Video RAM Configuration Options for the 3D Renderer](#).

Video RAM Configuration Options for the 3D Renderer

With video RAM configuration, you can configure the amount of VRAM that is assigned to the virtual machines in the pool.

When you enable the 3D Renderer setting and select the **Automatic**, **Software**, or **Hardware** option, you can configure the amount of VRAM that is assigned to the virtual machines in the pool by moving the slider in the **Configure VRAM for 3D guests** box. The maximum VRAM size is 512MB. The default VRAM size is 96MB.

The VRAM settings that you configure in Horizon Console take precedence over the VRAM settings that can be configured for the virtual machines in vSphere Client or the vSphere Web Client, unless you select the **Manage using vSphere Client** option.

Configure Full Clones with vSphere Virtual Machine Encryption

You can configure full clones to use the vSphere Virtual Machine Encryption feature. You can create full-clone desktops that have the same encryption keys or, full-clone desktops with different keys.

Prerequisites

- Create the Key Management Server (KMS) cluster with key management servers.

- To create a trust between KMS and vCenter Server, accept the self signed CA certificate or create a CA signed certificate.
- In vSphere Client, create the `VMcrypt/VMEncryption` storage profile.

Note For details about the Virtual Machine Encryption feature in vSphere, see the *vSphere Security* document in the vSphere documentation.

Procedure

- 1 To configure full clones that use the same encryption keys, create a VM template for all desktops to have the same encryption keys.

The clone inherits the parent encryption state including keys.

- a In vSphere Client, create a VM with the `vmencrypt` storage policy.
- b Convert the VM to a virtual machine template.
- c Create full-clone desktops that point to the template VM so that all desktops have the same encryption keys.

Note VM Encryption and Content Based Read Cache (CBRC) are not compatible. To use VM Encryption, you must disable CBRC globally by disabling View Storage Accelerator in Horizon Console by navigating to **Settings > Servers**.

- 2 To configure full clones that use different encryption keys, you must change the storage policy for each full-clone desktop.

- a In vSphere Client, create the full-clone desktop pool and then edit the full-clone desktops.

You can also edit existing full-clone desktops.

- b Navigate to each full-clone desktop and edit the storage policy and change the storage policy to `vmencrypt`.

Each full-clone desktop gets a different encryption key.

Rebuild a Virtual Machine in a Full-Clone Desktop Pool

Rebuild a virtual machine in a full-clone desktop pool if you want to replace the virtual machine with a new virtual machine and want to reuse the machine name. You can rebuild a virtual machine that is in an error state to replace the virtual machine with an error free virtual machine of the same name. When you rebuild a virtual machine, the virtual machine is deleted and then cloned with the same virtual machine name and the AD computer accounts are reused. All user data or settings from the previous virtual machine are lost and the new virtual machine is created using the desktop pool template.

Prerequisites

- Create an automated full-clone desktop pool. See [Create an Automated Full-Clone Desktop Pool](#).

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Select the desktop pool that contains the virtual machine you want to rebuild and click the **Inventory** tab.
- 3 Select the virtual machine that you want to rebuild and click **Rebuild**.

In vCenter Client, you can view the virtual machine as it is deleted and cloned again with the same name. In Horizon Console, the status of the rebuilt virtual machine goes through the following states: **Deleting > Provisioning > Customizing > Available**.

Creating and Managing Manual Desktop Pools

6

Use a manual desktop pool if you have pre-existing groups of desktops that you want to manage with Horizon 8. Compared to an automated desktop pool, a manual desktop pool has limited features. For example, Horizon 8 does not manage the lifecycle of the desktops in a manual desktop pool. Instant clones are not applicable to manual desktop pools.

You can create manual desktop pools for both virtual desktops and published desktops, which provide users with desktop sessions on RDS hosts. For more information about creating published desktops pools, see the *Windows Desktops and Applications in Horizon* document. For information about creating a manual desktop pool that uses Linux virtual machines, see the *Linux Desktops and Applications in Horizon* document.

Horizon 8 supports the following types of manual desktop pools.

Manual Desktop Pool of vSphere Machines

This type of manual desktop pool contains the following type of virtual machine:

- Independent virtual machines that are managed by vCenter Server.

These vSphere virtual machines are not created by Horizon 8. For example, these machines were created in vSphere by another virtual desktop infrastructure software and now you want to migrate them to Horizon 8. To create a manual desktop pool of vSphere virtual machines, you must install Horizon Agent on each machine, and then select the **vCenter virtual machines** option as part of the manual desktop pool creation workflow

Instant clone technology is not supported on this type of manual desktop pool. This type of manual desktop pool is also different from automated full-clone desktop pools in which Horizon 8 creates a pool of virtual machines that are cloned from a template VM as part of the pool creation process.

Manual Desktop Pool of Non-vSphere Machines

This type of manual desktop pool contains the following types of machines:

- Non-vSphere virtual machines. Virtual machines that run on a virtualization platform other than vCenter Server.
- Physical machines.

When these machines get registered with Connection Server as part of the Horizon Agent installation process, these machines are called registered machines. To create a manual desktop pool that contains non-vSphere VMs or physical machines in Horizon Console, you must select the **Other sources** option as part of the manual desktop pool creation workflow.

After you create this type of manual desktop pool, you can view these non-vSphere virtual machines or physical computers in Horizon Console by navigating to **Settings > Registered Machines > Others**.

RDS hosts are also registered machines that are not managed by vSphere. For more information on RDS hosts, see the *Windows Desktops and Applications in Horizon*.

Note After the virtual machine is added to a manual pool in Horizon 8, you need to power off the machine so the new display settings can be applied. These settings include monitor count, monitor resolution, and the Screen DMA setting. For more information, see <https://kb.vmware.com/s/article/2144475>.

This chapter includes the following topics:

- [Manual Pool of vSphere Virtual Machines](#)
- [Manual Pool of Registered Non-vSphere Virtual Machines](#)
- [Manual Pool of Registered Physical Machines](#)
- [Prepare a non-vSphere Machine For Horizon 8 Management](#)
- [Worksheet for Creating a Manual Desktop Pool](#)
- [Desktop Pool Settings for Manual Pools in Horizon Console](#)
- [Running Virtual Machines on Hyper-V](#)
- [Create a Manual Desktop Pool](#)
- [Managing non-vSphere Registered Machines](#)

Manual Pool of vSphere Virtual Machines

Complete the following steps in the workflow to create a manual desktop pool that contains vSphere virtual machines.

- Prepare the machines to deliver remote desktop access. In a manual pool that contains vSphere virtual machines, you must prepare each machine individually. Horizon Agent must be installed and running on each machine. To prepare vSphere virtual machines managed by vCenter Server, see [Chapter 3 Creating and Preparing a Virtual Machine for Cloning](#).
- Gather the configuration information that you must provide to create the pool. See [Worksheet for Creating a Manual Desktop Pool](#).
 - Power policies are supported for manual desktop pools that contain vSphere virtual machines. See [Setting Power Policies for Desktop Pools](#).

- 3D rendering options are supported for manual desktop pools that contain vSphere virtual machines. These options are also supported for full-clone desktop pools. For more information, see [Configuring 3D Rendering for Full-Clone Virtual Machine Pools](#).
- Create the manual desktop pool and select the **vCenter virtual machines** option to select the vSphere virtual machine as the desktop pool source. See [Create a Manual Desktop Pool](#).
- Entitle users to access the manual desktop pool. See "Entitling Users and Groups" in the *Horizon Administration* document.

Manual Pool of Registered Non-vSphere Virtual Machines

Non-vSphere virtual machines run on a virtualization platform other than vCenter Server. Since these machines get registered with Connection Server as part of the Horizon Agent installation process, these machines are called registered non-vSphere virtual machines. To create a manual desktop pool that contains non-vSphere virtual machines in Horizon Console, you must select the **Other sources** option as part of the manual desktop pool creation workflow.

Complete the following steps in the workflow to create a manual desktop pool that contains registered non-vSphere virtual machines.

- Prepare the non-vSphere virtual machine to deliver remote desktop access. Before you add this virtual machine to a manual desktop pool, you must prepare each machine individually. Horizon Agent must be installed and running on each machine. To prepare non-vSphere virtual machines, see [Prepare a non-vSphere Machine For Horizon 8 Management](#).
- Gather the configuration information that you must provide to create the pool. See [Worksheet for Creating a Manual Desktop Pool](#).
 - Power policies are not supported for manual desktop pools that contain registered non-vSphere virtual machines because these machines are not directly managed by vSphere.
 - 3D rendering options are not applicable for manual desktop pools that contain registered non-vSphere virtual machines. However, these virtual machines can directly leverage GPU capability available to the Horizon Agent operating system. Verify the graphics support with the third-party virtualization platform vendor.
- Create the manual desktop pool and select the **Other sources** option to select the registered non-vSphere virtual machine as the desktop pool source. See [Create a Manual Desktop Pool](#).
- Entitle users to access the manual desktop pool. See "Entitling Users and Groups" in the *Horizon Administration* document.
- Perform management tasks on non-vSphere registered machines. See [Managing non-vSphere Registered Machines](#).

Manual Pool of Registered Physical Machines

A registered physical machine is a physical computer that has Horizon Agent installed and is then registered with Connection Server.

Creating a manual desktop pool that contains registered physical machines provides end users access to their corporate physical computers remotely in a convenient and secure manner. Teleworkers who need access to their physical machines that reside within the corporate office can also access their machines without requiring to be on VPN and compromising security.

Both floating and dedicated user assignments are supported. With dedicated-assignment, you can also manually assign individual desktops so that each employee is connected to their own physical machine. You can also create a manual desktop pool with a single registered physical machine to enable single user access for the physical machine in the desktop pool.

With dedicated-assignment, you can also assign multiple users to each physical machine in a desktop pool so that shift workers can share the same desktop instead of reserving the dedicated machine for each user.

Physical machines support NVIDIA GPUs and encoders. Physical machines can also directly leverage GPU capability available to the Horizon Agent operating system. For more information, see the VMware Knowledge Base (KB) article <https://kb.vmware.com/s/article/78690>.

The following NVIDIA series have been tested:

- NVIDIA Studio Driver 516.59
- NVIDIA Titan Series
- GeForce 30 series
- GeForce 20 series
- GeForce 16 Series
- GeForce 10 Series
- NVIDIA Quadro Driver 516.59
- NVIDIA RTX Series
- M4000
- P4000
- K620

The following Intel series have been tested:

- Intel Gen10 hardware
- Intel Gen11 hardware
- Intel Graphics DCH Driver 30.0.101.1960
- Intel Graphics DCH Driver 30.0.101.1994

Complete the following steps in the workflow to create a manual desktop pool that contains registered physical machines.

- Prepare the physical machine to deliver remote desktop access. Before you add this physical machine to a manual desktop pool, you must prepare each machine individually. Horizon Agent must be installed and running on each machine. To prepare non-vSphere virtual machines, see [Prepare a non-vSphere Machine For Horizon 8 Management](#).
- Gather the configuration information that you must provide to create the pool. See [Worksheet for Creating a Manual Desktop Pool](#). The following options are not supported for manual desktop pools that contain registered physical machines:
 - Power policies are not supported.
 - PCoIP is not supported.
- Create the manual desktop pool and select the **Other sources** option to select the registered non-vSphere virtual machine as the desktop pool source. See [Create a Manual Desktop Pool](#).
- Entitle users to access the manual desktop pool. See "Entitling Users and Groups" in the *Horizon Administration* document.
- Perform management tasks on non-vSphere registered machines. See [Managing non-vSphere Registered Machines](#).

Note Manual desktop pools that contain registered physical machines supports Wake-on-LAN. This feature enables the entitled user to wake up the physical machine while connecting from Connection Server. Wake-on-LAN is supported with the VMware Blast protocol for dedicated-assignment manual desktop pools that contain registered physical machines. For more information about Wake-on-LAN, see "VMware Blast Extreme" in the *Horizon Overview and Deployment Planning* document.

For more information about using physical machines, see the "Using Horizon 7 to Access Physical Windows Machines" document available at <https://techzone.vmware.com>.

Prepare a non-vSphere Machine For Horizon 8 Management

You must perform certain tasks to prepare a non-vSphere machine to be managed by Horizon 8.

Prerequisites

- Verify that you have administrative rights on the non-vSphere machine.
- To make sure that remote desktop users are added to the local Remote Desktop Users group of the non-vSphere machine, create a restricted Remote Desktop Users group in Active Directory. See the *Horizon Installation and Upgrade* document for more information.

Procedure

- 1 Power on the non-vSphere machine and verify that it is accessible to the Connection Server instance.

- 2 Join the non-vSphere machine to the Active Directory domain for your remote desktops.
- 3 Configure the Windows firewall to allow Remote Desktop connections to the non-vSphere machine.

What to do next

Install Horizon Agent on the non-vSphere machine. See [Install Horizon Agent on a Non-vSphere Machine](#).

Install Horizon Agent on a Non-vSphere Machine

You must install Horizon Agent on all non-vSphere machines. VMware Horizon cannot manage a non-vSphere machine unless Horizon Agent is installed.

To install Horizon Agent on multiple Windows physical computers without having to respond to wizard prompts, you can install Horizon Agent silently.

Prerequisites

- Verify that you have prepared Active Directory. See the *Horizon Installation and Upgrade* document.
- Verify that you have administrative rights on the non-vSphere machine.
- To use a non-vSphere Windows Server machine as a remote desktop rather than as an RDS host, perform the steps described in [Prepare Windows Server Operating Systems for Desktop Use](#).
- Familiarize yourself with the Horizon Agent custom setup options for non-vSphere machines.
- Familiarize yourself with the TCP ports that the Horizon Agent installation program opens on the firewall. See the *Horizon Overview and Deployment Planning* document for more information.
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at <http://www.vmware.com/go/downloadview>.

Procedure

- 1 To start the Horizon Agent installation program, double-click the installer file.

The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

- 2 Accept the VMware license terms.

3 Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.

You must install all VMware Horizon components with the same IP version.

4 Select whether to enable or disable FIPS mode.

This option is available only if FIPS mode is enabled in Windows.

5 Select your custom setup options.**6** Accept or change the destination folder.**7** In the **Server** text box, type the host name or IP address of a Connection Server host.

During installation, the installer registers the non-vSphere machine with this Connection Server instance. After registration, the specified Connection Server instance, and any additional instances in the same Connection Server group, can communicate with the non-vSphere machine.

8 Select an authentication method to register the non-vSphere machine with the Connection Server instance.

Option	Action
Authenticate as the currently logged in user	The Username and Password text boxes are disabled and you are logged in to the Connection Server instance with your current username and password.
Specify administrator credentials	You must provide the username and password of a Connection Server administrator in the Username and Password text boxes.

Provide the username in the following format: **Domain\User**.

The user account must be a domain user with access to Horizon Directory on the Connection Server instance. A local user does not work.

9 Follow the prompts in the Horizon Agent installation program and finish the installation.**10** If you selected the USB redirection option, restart the non-vSphere machine to enable USB support.

In addition, the **Found New Hardware** wizard might start. Follow the prompts in the wizard to configure the hardware before you restart the non-vSphere machine.

Results

The Horizon Agent service is started on the non-vSphere machine and the machine is registered with Horizon 8.

What to do next

Use the registered non-vSphere machine to create a manual desktop pool. See [Create a Manual Desktop Pool](#).

After the pool is created, you can edit the pool.

Note When you reconfigure a pool setting that affects a registered machine, it can take up to 10 minutes for the new setting to take effect. For example, if you change the **Automatically logoff after disconnect** setting for a pool, Horizon 8 might take up to 10 minutes to reconfigure the affected machines.

Horizon Agent Custom Setup Options for Non-vSphere Machines

When you install Horizon Agent on a non-vSphere machine, you can select or deselect certain custom setup options. In addition, Horizon Agent installs certain features automatically on all guest operating systems on which they are supported. These features are not optional.

To change custom setup options after you install the latest Horizon Agent version, you must uninstall and reinstall Horizon Agent. For patches and upgrades, you can run the new Horizon Agent installer and select a new set of options without uninstalling the previous version.

Table 6-1. Horizon Agent Features That Are Installed Automatically on Non-vSphere Machines in an IPv4 Environment (Not Optional)

Feature	Description
PCoIP Agent	Lets users connect to the remote desktop with the PCoIP display protocol. The PCoIP Agent feature is supported on physical machines that are configured with a Teradici TERA host card.
Lync	Provides support for Microsoft Lync 2013 Client on remote desktops.
Unity Touch	Allows tablet and smart phone users to interact easily with Windows applications that run on the remote desktop. Users can browse, search, and open Windows applications and files, choose favorite applications and files, and switch between running applications, all without using the Start menu or Taskbar.

Table 6-2. Horizon Agent Custom Setup Options for Non-vSphere Machines in an IPv4 Environment (Optional)

Option	Description
USB Redirection	<p>Gives users access to locally connected USB devices on their desktops.</p> <p>USB redirection is supported on remote desktops that are deployed on single-user machines. In addition, redirection of USB flash drives and hard disks is supported on RDS desktops and applications.</p> <p>This setup option is not selected by default. You must select the option to install it.</p> <p>For guidance on using USB redirection securely, see the <i>Horizon Security</i> document. For example, you can use group policy settings to disable USB redirection for specific users.</p>
Client Drive Redirection	<p>Allows Horizon Client users to share local drives with their remote desktops.</p> <p>After this setup option is installed, no further configuration is required on the remote desktop.</p> <p>Client Drive Redirection is also supported on VDI desktops that run on managed, single-user virtual machines and on RDS desktops and applications.</p>
Smartcard Redirection	<p>Lets users authenticate with smart cards when they use the PCoIP or Blast Extreme display protocol.</p> <p>Smartcard Redirection is supported on remote desktops that are deployed on single-user machines but is not supported on RDS host-based remote desktops.</p>
Virtual audio driver	Provides a virtual audio driver on the remote desktop.

In an IPv6 environment, the only optional feature is Smartcard Redirection.

In an IPv6 environment, the only automatically installed feature is PCoIP Agent.

Worksheet for Creating a Manual Desktop Pool

When you create a manual desktop pool, you can configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

Note In a manual pool, you must prepare each machine to deliver remote desktop access. Horizon Agent must be installed and running on each machine before you can add the machine to the manual desktop pool.

Table 6-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool

Option	Description	Enter Your Value Here
vCenter Server	The vCenter Server that manages the machines. This option appears only if the machines are virtual machines that are managed by vCenter Server.	
User assignment	Choose the type of user assignment: <ul style="list-style-type: none"> ■ In a dedicated-assignment pool, each user is assigned to a machine. After a user is assigned a desktop, no other user can use the desktop. Users receive the same machine each time they log in. ■ In a floating-assignment pool, users receive different machines each time they log in. For details, see Assign a Machine to a User in a Dedicated-Assignment Pool .	
Enable automatic assignment	In a dedicated-assignment pool, a machine is assigned to a user when the user first logs in to the pool. You can also explicitly assign machines to users. If you do not enable automatic assignment, you must explicitly assign a machine to each user. You can assign machines manually even when automatic assignment is enabled.	
Enable Multi-User Assignment	In a dedicated-assignment pool, you can assign multiple users to each machine in the pool. Multi-user assignment is not supported for automatic user assignment desktop pools. If an assigned user has a connected or disconnected session on a multi-user assignment machine, other assigned users will be unable to launch a session on that machine.	

Table 6-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Machine Source	<p>The virtual machines or physical computers that you want to include in the desktop pool.</p> <ol style="list-style-type: none"> 1 Decide which type of machine you want to use. You can use either virtual machines that are managed by vCenter Server, or virtual machines that are managed by another virtualization platform, and physical computers. 2 Prepare a list of the machines that you want to include in the desktop pool. 3 Install Horizon Agent on each machine that you want to include in the desktop pool. <p>To use PCoIP with machines that are unmanaged virtual machines or physical computers, you must use Teradici hardware.</p> <hr/> <p>Note When you enable Windows Server desktops in the Horizon console, The console displays all available Windows Server machines, including machines on which Connection Server and other Horizon 8 servers are installed, as potential machine sources.</p> <p>You cannot select machines for the desktop pool if Horizon 8 server software is installed on the machines. Horizon Agent cannot coexist on the same virtual or physical machine with any other Horizon 8 software component, including Connection Server or Horizon Client.</p>	
Desktop Pool ID	<p>The pool name that users see when they log in and that identifies the pool in the Horizon console.</p> <p>If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID.</p> <p>A Connection Server configuration can be a standalone Connection Server instance or a pod of replicated instances that share a common LDAP configuration.</p>	
Display name	<p>The pool name that users see when they log in from a client. If you do not specify a name, the pool ID is used.</p>	

Table 6-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Access group	<p>Select an access group for the pool or leave the pool in the default root access group.</p> <p>If you use an access group, you can delegate managing the pool to an administrator who has a specific role.</p> <hr/> <p>Note Access groups are different from vCenter Server folders that store desktop VMs.</p>	
State	<ul style="list-style-type: none"> ■ Enabled. After being created, the desktop pool is enabled and ready for immediate use. ■ Disabled. After being created, the desktop pool is disabled and unavailable for use. This is an appropriate setting if you want to conduct activities such as testing or other forms of baseline maintenance. <p>When this state is in effect, remote desktops are unavailable for use.</p>	
Connection Server restrictions	<ul style="list-style-type: none"> ■ None. The desktop pool can be accessed by any Connection Server instance. ■ With tags. Select one or more Connection Server tags to make the desktop pool accessible only to Connection Server instances that have those tags. You can use the check boxes to select multiple tags. <p>If you intend to provide access to your desktops through VMware Workspace ONE Access, and you configure Connection Server restrictions, the VMware Workspace ONE Access app might display desktops to users when those desktops are actually restricted. VMware Workspace ONE Access users will be unable to launch these desktops.</p>	
Category Folder	<p>Specifies the name of the category folder that contains a Start menu shortcut for the desktop pool entitlement on Windows client devices. For more information, see "Configuring Shortcuts for Entitled Pools" in the <i>Horizon Administration</i> document.</p>	
Client Restrictions	<p>Select whether to restrict access to entitled desktop pools from certain client computers. You must add the names of the computers that are allowed to access the desktop pool in an Active Directory security group. You can select this security group when you add users or groups to the desktop pool entitlement.</p>	

Table 6-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Session Types	<p>You can enable the VM Hosted Applications feature by selecting the supported session type for the desktop pool:</p> <ul style="list-style-type: none"> ■ Desktop. Select this option to use the pool as a regular desktop pool. All the virtual machines in the pool can only be used to host desktops. ■ Application. Select this option to use all the virtual machines in the pool to host applications. ■ Desktop and Application. When this option is selected, the virtual machine in the pool can either host a regular desktop session or host an application session. The first connection to the particular virtual machine will determine the session type of the virtual machine. <p>For more information about the VM Hosted Applications feature, see the technical marketing white paper "Best Practices for Published Applications and Desktops in VMware Horizon and VMware Horizon Apps" available at https://techzone.vmware.com.</p>	
Remote machine power policy	<p>Determines how a virtual machine behaves when the user logs off of the associated desktop. This option is only available for a manual pool of vSphere virtual machines.</p> <p>For descriptions of the power-policy options, see Power Policies for Desktop Pools.</p> <p>For more information about how power policies affect automated pools, see "setting Power Policies for Desktop Pools," in the <i>Windows Desktops and Applications in Horizon</i> document.</p>	
Logoff after disconnect	<ul style="list-style-type: none"> ■ Immediately. Users are logged off as soon as they disconnect. ■ Never. Users are never logged off. ■ After. The time after which users are logged off when they disconnect. Type the duration in minutes. <p>The log off time applies to future disconnections. If a desktop session was already disconnected when you set a log off time, the log off duration for that user starts when you set the log off time, not when the session was originally disconnected. For example, if you set this value to five minutes, and a session was disconnected 10 minutes earlier, Horizon will log off that session five minutes after you set the value.</p>	

Table 6-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Empty session timeout (Applications only)	<p>Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log out from empty application sessions. Select Never, Immediate, or set the number of minutes as the timeout value. The default is After 1 minute. If you select Immediate, the session logs you out or disconnects within 30 seconds.</p> <p>You can further reduce the time the session logs out or disconnects by editing a registry key on the RDS Host on which Horizon Agent is installed. Navigate to <code>HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params</code> and set a value for <code>WindowCheckInterval</code>. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session logout to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session logout to 5 seconds.</p>	
Pre-launch session timeout (Applications only)	Determines the timeout for the application session before the session is disconnected or logged off.	
When timeout occurs	Determines whether an empty application session is disconnected or logged off after the Empty session timeout limit is reached. Select Disconnect or Log off . A session that is logged off frees up resources, but opening an application takes longer. The default is Disconnect .	

Table 6-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Bypass Session Timeout (Application and Desktop and Application session types)	<p>Enable this setting to allow application sessions to run forever. When enabled, all the application sessions belonging to the desktop pool will never be disconnected automatically, neither when reaching the max session timeout nor when reaching the global idle timeout.</p> <p>This setting is available when you select session types Application and Desktop or Application.</p> <p>Application sessions that run forever are supported on Windows and Linux clients.</p> <p>You cannot enable this setting if any of the applications belonging to the desktop pool is part of Global Application Entitlement as local pools.</p> <p>This setting is not available for application pools in a cloud pod architecture environment.</p> <p>Application sessions that run forever are not supported for unauthenticated users.</p> <p>Do not enable this setting if the max session timeout value is set to Never.</p> <p>When you restart Connection Server, existing forever running application sessions no longer run indefinitely.</p>	
Allow users to reset/restart their machines	Allow users to reset or restart their own desktops.	
Show Assigned Machine Name	<p>Displays the host name of the assigned machine instead of the desktop pool display name when you log in to Horizon Client.</p> <p>If no machine is assigned to the user then, Display Name (No Machine Assigned) appears for the desktop pool when you log in to Horizon Client.</p>	
Show Machine Alias Name	<p>Displays the machine alias name set for the assigned users of the machine instead of the desktop display name for the desktop pool in Horizon Client. Applies only to dedicated desktop entitlements.</p> <p>If no machine alias name is set but the Show Assigned Machine Name is set, then the machine host name appears for the desktop pool in Horizon Client. Otherwise, the desktop display name appears for the desktop pool in Horizon Client.</p>	

Table 6-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Default Display Protocol	<p>VMware Blast. The VMware Blast Extreme protocol is built on the H.264 protocol and supports the broadest range of client devices, including smart phones, tablets, ultra-low-cost PCs, and Macs, across any network.</p> <p>PCoIP. PCoIP is supported as the display protocol for virtual and physical machines that have Teradici hardware. PCoIP provides an optimized PC experience for the delivery of images, audio, and video content for a wide range of users on the LAN or across the WAN.</p> <p>Microsoft RDP. Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data. RDP is a multichannel protocol that allows a user to connect to a computer remotely.</p>	
Allow Users to Choose Protocol	Allow users to override the default display protocol for their desktops in Horizon Client.	
3D Renderer	<p>You can configure the 3D Renderer to use software rendering or hardware rendering based on physical GPU graphics cards installed on hosts. If you select RDP as the Default Display Protocol, you must enable the Allow users to choose protocol setting (select Yes) to enable 3D rendering. If the default display protocol is RDP and you disable the Allow users to choose protocol setting (select No), the 3D rendering option is disabled.</p> <p>With the hardware-based 3D Renderer options, users can take advantage of graphics applications for design, modeling, and multimedia. With the software 3D Renderer option, users can take advantage of graphics enhancements in less demanding applications such as AERO, Microsoft Office, and Google Earth. For more details, see Configuring 3D Rendering for Full-Clone Virtual Machine Pools.</p> <p>When you edit this setting, you must power off existing virtual machines, verify that the machines are reconfigured in vCenter Server, and power on the machines to cause the new setting to take effect. Restarting a virtual machine does not cause the new setting to take effect.</p>	

Table 6-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Max Number of Monitors	<p>If you select PCoIP or VMware Blast as the display protocol, you can select the maximum number of monitors on which users can display the desktop. You can select up to four monitors.</p> <p>When the 3DRenderer setting is not selected, the Max number of monitors setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the number of monitors, more memory is consumed on the associated ESXi hosts.</p> <p>Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution.</p> <p>When you edit the pool, you must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.</p>	
Max Resolution of Any One Monitor	<p>If you select PCoIP or VMware Blast as the display protocol, you should specify the maximum resolution of any one monitor.</p> <p>The maximum resolution of any one monitor is set to 1920 x 1200 pixels by default, but you can configure this value.</p> <p>When the 3D Renderer setting is not selected, the Max resolution of any one monitor setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the resolution, more memory is consumed on the associated ESXi hosts.</p> <p>Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution.</p> <p>When you edit the pool, you must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.</p>	

Table 6-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
HTML Access	<p>Select Enabled to allow users to connect to remote desktops from within their Web browsers. When a user logs in through the VMware Horizon Web portal page or the VMware Workspace ONE Access app and selects a remote desktop, the HTML Access agent enables the user to connect to the desktop over HTTPS. The desktop is displayed in the user's browser. Other display protocols, such as PCoIP or RDP, are not used. Horizon Client software does not have to be installed on the client devices.</p> <p>To use HTML Access, you must install HTML Access in your Horizon 8 deployment. For more information, see <i>Using HTML Access</i>, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.</p> <p>To use HTML Access with VMware Workspace ONE Access, you must pair Connection Server with a SAML Authentication server, as described in the <i>Horizon Administration</i> document. VMware Workspace ONE Access must be installed and configured for use with Connection Server.</p>	
Allow Session Collaboration	<p>Select Enabled to allow users of the pool to invite other users to join their remote desktop sessions. Session owners and session collaborators must use the VMware Blast display protocol.</p>	
Allow user to initiate separate sessions from different client devices	<p>Allow user to initiate separate sessions from different client devices</p>	

Table 6-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Use View Storage Accelerator	<p>Determine whether ESXi hosts cache common virtual machine disk data. View Storage Accelerator can improve performance and reduce the need for extra storage I/O bandwidth to manage boot storms and anti-virus scanning I/O storms. This feature is enabled by default.</p> <hr/> <p>Note The Horizon console does not save the blackout times if you add or delete blackout times and then disable View Storage Accelerator. The View Storage Accelerator feature takes effect for new virtual machines of a newly created manual pool only after the new virtual machines are powered off once and powered on.</p> <hr/>	
Transparent Page Sharing Scope	<p>This option is only available for a manual pool of vSphere virtual machines.</p> <p>Select the level at which to allow transparent page sharing (TPS). The choices are Virtual Machine (the default), Pool, Pod, or Global. If you turn on TPS for all the machines in the pool, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications.</p> <p>Page sharing happens on the ESXi host. For example, if you enable TPS at the pool level but the pool is spread across multiple ESXi hosts, only virtual machines on the same host and within the same pool will share pages. At the global level, all machines managed by VMware Horizon on the same ESXi host can share memory pages, regardless of which pool the machines reside in.</p> <hr/> <p>Note The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.</p> <hr/>	

Desktop Pool Settings for Manual Pools in Horizon Console

The desktop pool settings you can configure when you create a manual desktop pool differs depending on the type of machines and user assignments.

Registered machines include registered non-vSphere virtual machines and registered physical machines.

Table 6-4. Settings for Manual Desktop Pools

Setting	vSphere virtual machines, Dedicated Assignment	vSphere virtual machines, Floating Assignment	Registered Machines, Dedicated Assignment	Registered Machines, Floating Assignment
State	Yes	Yes	Yes	Yes
Connection Server restrictions	Yes	Yes	Yes	Yes
Remote machine power policy	Yes	Yes		
Automatically logoff after disconnect	Yes	Yes	Yes	Yes
Allow users to reset/restart their machines	Yes	Yes		
Allow user to initiate separate sessions from different client devices		Yes		Yes
Default display protocol	Yes	Yes	Yes To use PCoIP with a machine that is not managed by vCenter Server, you must install Teradici hardware on the machine.	Yes To use PCoIP with a machine that is not managed by vCenter Server, you must install Teradici hardware on the machine.
Allow users to choose protocol	Yes	Yes	Yes	Yes
3D Renderer	Yes	Yes		
Max number of monitors	Yes	Yes		
Max resolution of any one monitor	Yes	Yes		
Enable automatic user assignment	Yes		Yes	

Table 6-4. Settings for Manual Desktop Pools (continued)

Setting	vSphere virtual machines, Dedicated Assignment	vSphere virtual machines, Floating Assignment	Registered Machines, Dedicated Assignment	Registered Machines, Floating Assignment
Enable Multi-User Assignment	Yes		Yes	
Display Assigned Machine Name	Yes		Yes	

Running Virtual Machines on Hyper-V

VMware Horizon supports virtual machines running on Hyper-V hypervisor version 2012R2 UR12, Hyper-V Server 2016, and Hyper-V Server 2019.

The following operating systems are supported:

- VDI: Windows 10 20H2 64-bit, Windows 10 21H1 64-bit, Windows 10 21H2 64-bit, Windows 11 21H2 64-bit
- RDS Hosts: Windows Server 2016 Standard 64-bit, Windows Server 2012 R2 Standard 64-bit, and Windows Server 2019 (Hyper-V Server 2016, Hyper-V Server 2019)

Running Horizon Agent in virtual machines on Hyper-V has the following limitations and known issues:

- Horizon Agent installation in Desktop mode is not supported on Windows Server OS.
- When you click the CAD button on the Hyper-V console, the CAD window also displays on the remote desktop session.
- Hyper-V does not support GPU-related features: vGPU, 3D RDSH, HEVC.

Note Hyper-V based virtual machines can directly leverage GPU capability available to the Horizon Agent operating system. Verify the graphics support with the third-party virtualization platform vendor (Microsoft).

Create a Manual Desktop Pool

You can create a manual desktop pool that provisions desktops from vSphere virtual machines or registered machines that include non-vSphere virtual machines and physical computers.

Prerequisites

- Prepare the machines to deliver remote desktop access. In a manual pool, you must prepare each machine individually. Horizon Agent must be installed and running on each machine.

To prepare vSphere virtual machines managed by vCenter Server, see [Chapter 3 Creating and Preparing a Virtual Machine for Cloning](#).

To prepare non-vSphere virtual machines or physical computers, see [Managing non-vSphere Registered Machines](#).

- Gather the configuration information that you must provide to create the pool. See [Worksheet for Creating a Manual Desktop Pool](#).

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Click **Add**.
- 3 Select **Manual Desktop Pool**.
- 4 Choose virtual machines managed by vCenter Server or other virtual machines that are not managed by vCenter Server and click **Next**.

Option	Description
vCenter virtual machines	vSphere virtual machines that are managed by vCenter Server. Select the vCenter Server on which the virtual machines reside.
Other Sources	Physical computers or virtual machines that are not managed by vCenter Server.

- 5 Follow the prompts in the wizard to create the pool.

Use the configuration information that you gathered in the worksheet. You can go directly back to any wizard page that you completed by clicking the page name in the navigation panel.

When you select the vSphere virtual machines for inclusion into the manual desktop pool, Horizon 8 ensures that a spare machine is powered on so that users can connect to it. The spare machine is powered on regardless of which power policy is in effect for the desktop pool.

Results

In Horizon Console, you can view the machines as they are added to the pool by selecting **Inventory > Desktops**.

What to do next

Entitle users to access the pool. See "Entitling Users and Groups" in the *Horizon Administration* document.

Managing non-vSphere Registered Machines

In Horizon Console, you can manage non-vSphere registered machines from VMware Horizon.

Remove a Registered Machine from a Manual Desktop Pool

You can reduce the size of a desktop pool by removing registered machines from the pool.

Procedure

- 1 In Horizon Console, select **Inventory > Machines**.
- 2 Select the **Others** tab.
- 3 Select the unmanaged machines to remove.
- 4 Click **Remove**.
- 5 Click **OK**.

Results

The unmanaged machines are removed from the pool.

Remove Registered Machines From Horizon 8

If you do not plan to use a registered machine again, you can remove it from Horizon 8.

After you remove a registered machine, it becomes unavailable in Horizon 8. To make the machine available again, you must reinstall Horizon Agent.

Prerequisites

Verify that the registered machines that you want to remove are not being used in any desktop pool.

Procedure

- 1 In Horizon Console, select **Settings > Registered Machines**.
- 2 Click the **RDS Hosts** tab.
- 3 Select one or more machines and click **Remove**.

You can select only machines that are not being used by a desktop pool.

- 4 Click **OK** to confirm.

Configuring All Virtual Desktop Pool Types

7

When you create a virtual desktop pool, you select configuration options that determine how the pool is managed and how users interact with the desktops.

These tasks apply to virtual desktop pools that are deployed on single-user machines including full clones, instant clones, and manual desktop pools, unless otherwise noted.

If you have connected your pod to Horizon Cloud and want information on configuring virtual desktop pools for use in a Universal Broker environment, see the *Administration of Your Horizon Cloud Tenant Environment and Pod Fleet* document.

This chapter includes the following topics:

- Using a Naming Pattern for Desktop Pools
- Machine-Naming Example
- Change the Size of a Desktop Pool Provisioned by a Naming Pattern
- Naming Machines Manually or Providing a Naming Pattern in Horizon Console
- Assign a Machine to a User in a Dedicated-Assignment Pool
- Unassign a User from a Dedicated Machine in Horizon Console
- Update Machine Aliases for Assigned Users
- Setting Power Policies for Desktop Pools
- Configure Desktop Session Timeouts in Horizon Console
- Managing Desktop Pools
- Export Horizon 8 Information to External Files
- Examining GPU Resources on an ESXi Host
- Creating Desktop Pools on a Single Host SDDC on VMware Cloud on AWS
- Prevent Access to VMware Horizon Desktops Through RDP

Using a Naming Pattern for Desktop Pools

You can provision the machines in a pool by providing a naming pattern and the total number of machines you want in the pool. By default, Horizon 8 uses your pattern as a prefix in all the machine names and appends a unique number to identify each machine.

Length of the Naming Pattern in a Machine Name

Machine names have a 15-character limit, including your naming pattern and the automatically generated number.

Table 7-1. Maximum Length of the Naming Pattern in a Machine Name

If You Set This Number of Machines in the Pool	This Is the Maximum Prefix Length
1-99	13 characters
100-999	12 characters
1,000 or more	11 characters

Names that contain fixed-length tokens have different length limits.

Using a Token in a Machine Name

You can place the automatically generated number anywhere else in the name by using a token. When you type the pool name, type **n** surrounded by curly brackets to designate the token.

For example: **amber-{n}-desktop**

When a machine is created, Horizon 8 replaces **{n}** with a unique number.

You can generate a fixed-length token by typing **{n:fixed=number of digits}**.

Horizon 8 replaces the token with numbers containing the specified number of digits.

For example, if you type **amber-{n:fixed=3}**, Horizon 8 replaces **{n:fixed=3}** with a three-digit number and creates these machine names: **amber-001**, **amber-002**, **amber-003**, and so on.

Length of the Naming Pattern When You Use a Fixed-Length Token

Names that contain fixed-length tokens have a 15-character limit, including your naming pattern and the number of digits in the token.

Table 7-2. Maximum Length of the Naming Pattern When You Use a Fixed-Length Token

Fixed-Length Token	Maximum Length of the Naming Pattern
{n:fixed=1}	14 characters
{n:fixed=2}	13 characters
{n:fixed=3}	12 characters

Machine-Naming Example

This example shows how to create two automated desktop pools that use the same machine names, but different sets of numbers. The strategies that are used in this example achieve a specific user objective and show the flexibility of the machine-naming methods.

The objective is to create two pools with the same naming convention such as VDIABC-XX, where XX represents a number. Each pool has a different set of sequential numbers. For example, the first pool might contain machines VDIABC-01 through VDIABC-10. The second pool contains machines VDIABC-11 through VDIABC-20.

You can use either machine-naming method to satisfy this objective.

- To create fixed sets of machines at one time, specify machine names manually.
- To create machines dynamically when users log in for the first time, provide a naming pattern and use a token to designate the sequential numbers.

Specifying the Names Manually

- 1 Prepare a text file for the first pool that contains a list of machine names from VDIABC-01 through VDIABC-10.
- 2 In Horizon Console, create the pool and specify machine names manually.
- 3 Click **Enter Names** and copy your list into the **Enter Machine Names** list box.
- 4 Repeat these steps for the second pool, using the names VDIABC-11 through VDIABC-20.

For detailed instructions, see [Specify a List of Machine Names](#).

You can add machines to each pool after it is created. For example, you can add machines VDIABC-21 through VDIABC-30 to the first pool, and VDIABC-31 through VDIABC-40 to the second pool. See [Add Machines to an Automated Pool Provisioned by a List of Names](#).

Providing a Naming Pattern With a Token

- 1 In Horizon Console, create the first pool and use a naming pattern to provision the machine names.
- 2 In the naming-pattern text box, type **VDIABC-0{n}**.
- 3 Limit the pool's maximum size to 9.
- 4 Repeat these steps for the second pool, but in the naming-pattern text box, type **VDIABC-1{n}**.

The first pool contains machines VDIABC-01 through VDIABC-09. The second pool contains machines VDIABC-11 through VDIABC-19.

Alternatively, you can configure the pools to contain up to 99 machines each by using a fixed-length token of 2 digits:

- For the first pool, type **VDIABC-0{n:fixed=2}**.

- For the second pool, type **VDIABC-1{n:fixed=2}**.

Limit each pool's maximum size to 99. This configuration produces machines that contain a 3-digit sequential naming pattern.

First pool:

```
VDIABC-001
VDIABC-002
VDIABC-003
```

Second pool:

```
VDIABC-101
VDIABC-102
VDIABC-103
```

For details about naming patterns and tokens, see [Using a Naming Pattern for Desktop Pools](#).

Change the Size of a Desktop Pool Provisioned by a Naming Pattern

When you provision an automated desktop pool by using a naming pattern, you can increase or decrease the size of the pool by changing the maximum number of machines.

Prerequisites

- Verify that you provisioned the desktop pool by using a naming pattern.
- Verify that the desktop pool is automated.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Click the desktop pool ID and click **Edit**.
- 3 On the **Provisioning Settings** tab, type the new number of machines in the desktop pool in the **Max number of machines** text box.

Results

If you increase the desktop pool size, new machines can be added to the pool up to the maximum number.

If you decrease the size of a floating-assignment pool, unused machines are deleted. If more users are logged into the pool than the new maximum, the pool size decreases after users log off.

If you decrease the size of a dedicated-assignment pool, unassigned machines are deleted. If more users are assigned to machines than the new maximum, the pool size decreases after you unassign users.

Note When you decrease the size of a desktop pool, the actual number of machines might be larger than **Max number of machines** if more users are currently logged in or assigned to machines than the value that is specified in **Max number of machines**.

Naming Machines Manually or Providing a Naming Pattern in Horizon Console

With an automated desktop pool of full virtual machines or instant clones, you can specify a list of names for the desktop machines or provide a naming pattern.

If you name machines manually, each line must contain a unique machine name.

If you provide a naming pattern, Horizon 8 can dynamically create and assign machines as users need them.

The following table compares the two naming methods, showing how each method affects the way you create and administer a desktop pool.

Table 7-3. Naming Machines Manually or Providing a Machine-Naming Pattern

Feature	Using a Machine-Naming Pattern	Naming Machines Manually
Machine names	<p>The machine names are generated by appending a number to the naming pattern.</p> <p>For details, see Using a Naming Pattern for Desktop Pools.</p>	<p>Enter names that will be used to create new virtual machines.</p> <p>The name can be used for both floating and dedicated-assignment pools. Optionally, for dedicated desktop pools, a user name can be specified. Specific user names will be ignored for floating desktop pools.</p> <p>In a dedicated-assignment pool, you can pair users with machines by listing user names with the machine names.</p> <p>Start machines in maintenance mode is not applicable for dedicated and floating instant clone pools.</p> <p>For details, see Specify a List of Machine Names.</p>
Pool size	You specify a maximum number of machines.	<p>Maximum Machines is not available for dedicated and floating instant clone pools when virtual machines are specified manually. Your list of machine names determines the number of machines.</p>

Table 7-3. Naming Machines Manually or Providing a Machine-Naming Pattern (continued)

Feature	Using a Machine-Naming Pattern	Naming Machines Manually
To add machines to the pool	You can increase the maximum pool size.	You can add machine names to the list. For details, see Add Machines to an Automated Pool Provisioned by a List of Names .
On-demand provisioning	Available. Horizon 8 dynamically creates and provisions the specified minimum and spare number of machines as users first log in or as you assign machines to users. Horizon 8 can also create and provision all the machines when you create the pool.	Not available. Provisioning machines on demand is disabled for virtual machines whose names are specified manually in both dedicated and floating pools.
Initial customization	Available. When a machine is provisioned, Horizon 8 can run a customization specification that you select.	Available. When a machine is provisioned, Horizon 8 can run a customization specification that you select.
Manual customization of dedicated machines	To customize machines and return desktop access to your users, you must remove and reassign the ownership of each machine. Depending on whether you assign machines on first log in, you might have to perform these steps twice. You cannot start machines in maintenance mode. After the pool is created, you can manually put the machines into maintenance mode.	You can customize and test machines without having to reassign ownership. Start machines in maintenance mode is not applicable for dedicated or floating instant clone pools. For details, see Manually Customizing Machines .
Dynamic or fixed pool size	Dynamic. If you remove a user assignment from a machine in a dedicated-assignment pool, the machine is returned to the pool of available machines. If you choose to delete machines on logoff in a floating-assignment pool, the pool size can grow or shrink depending on the number of active user sessions.	Fixed. The pool contains the number of machines you provide in the list of machine names. You cannot select the Delete machine on logoff setting if you name machines manually.

Table 7-3. Naming Machines Manually or Providing a Machine-Naming Pattern (continued)

Feature	Using a Machine-Naming Pattern	Naming Machines Manually
Spare machines	<p>You can specify a number of spare machines that Horizon 8 keeps powered on for new users.</p> <p>Horizon 8 creates new machines to maintain the specified number. Horizon 8 stops creating spare machines when it reaches the maximum pool size.</p> <p>Horizon 8 keeps the spare machines powered on even when the pool power policy is Power off or Suspend, or when you do not set a power policy.</p>	<p>Spare (Powered On) Machines is not available for dedicated and floating instant clone pools when virtual machines are specified manually.</p>
User assignment	<p>You can use a naming pattern for dedicated-assignment and floating-assignment pools.</p>	<p>You can specify machine names for dedicated-assignment and floating-assignment pools.</p> <p>Note In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.</p>

Specify a List of Machine Names

You can provision an automated desktop pool by manually specifying a list of machine names. This naming method lets you use your company's naming conventions to identify the machines in a pool.

When you explicitly specify machine names, users can see familiar names based on their company's organization when they log in to their remote desktops.

Follow these guidelines for manually specifying machine names:

- Type each machine name on a separate line.
- A machine name can have up to 15 alphanumeric characters.
- You can add a user name to each machine entry. Use a comma to separate the user name from the machine name.

In this example, two machines are specified. The second machine is associated with a user:

```
Desktop-001  
Desktop-002,abccorp.com\jdoe
```

Note In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

Prerequisites

Make sure that each machine name is unique. You cannot use the names of existing virtual machines in vCenter Server.

Procedure

- 1 Create a text file that contains the list of machine names.
If you intend to create a desktop pool with only a few machines, you can type the machine names directly in the **Add Pool** wizard. You do not have to create a separate text file.
- 2 In Horizon Console start the **Add Pool** wizard to begin creating an automated desktop pool that contains full virtual machines.
- 3 On the Provisioning Settings page, select **Specify names manually** and click **Enter names**.
- 4 Copy your list of machine names in the **Enter Machine Names** page and click **Next**.
- 5 Click **Submit**.
- 6 (Optional) Select **Start machines in maintenance mode**.
This option lets you customize the machines before users can log in and use them.
- 7 Follow the prompts in the wizard to finish creating the desktop pool.

Results

Horizon 8 creates a machine for each name in the list. When an entry includes a machine and user name, Horizon 8 assigns the machine to that user.

After the desktop pool is created, you can add machines by importing another list file that contains additional machine names and users. See [Add Machines to an Automated Pool Provisioned by a List of Names](#).

Add Machines to an Automated Pool Provisioned by a List of Names

To add machines to an automated desktop pool provisioned by manually specifying machine names, you provide another list of new machine names. This feature lets you expand a desktop pool and continue to use your company's naming conventions.

Follow these guidelines for manually adding machine names:

- Type each machine name on a separate line.

- The name must contain at least one alpha character.
- The name must contain only alphanumerics and dashes. Underscores are not allowed.
- The maximum length is 15 characters.
- You can add a user name to each machine entry. Use a comma to separate the user name from the machine name.

In this example, two machines are added. The second machine is associated with a user:

```
Desktop-001  
Desktop-002,abccorp.com/jdoe
```

Note In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

Prerequisites

Verify that you created the automated desktop pool of full virtual machines by manually specifying machine names. You cannot add machines by providing new machine names if you created the pool by providing a naming pattern.

Procedure

- 1 Create a text file that contains the list of additional machine names.
If you intend to add only a few machines, you can type the machine names directly in the **Add Pool** wizard. You do not have to create a separate text file.
- 2 In Horizon Console, select **Inventory > Desktops**.
- 3 Select the desktop pool to be expanded.
- 4 Click **Edit**.
- 5 Click the **Provisioning Settings** tab.
- 6 Click **Add Machines**.
- 7 Copy your list of machine names in the **Enter Machine Names** page and click **Next**.
- 8 Click **Submit**.
- 9 Click **OK**.

Results

In vCenter Server, you can monitor the creation of the new virtual machines.

In Horizon Console, you can view the machines as they are added to the desktop pool by selecting **Inventory > Desktops**.

Assign a Machine to a User in a Dedicated-Assignment Pool

In a dedicated-assignment pool, you can assign a user or multiple users to the virtual machine that hosts a remote desktop. Only the assigned user can log in and connect to the remote desktop. If a user is connected to session on a remote desktop, another user entitled to use the virtual machine cannot log in and connect to the remote desktop till the previous user logs off from the remote desktop.

Horizon Console assigns machines to users in these situations.

- When you create a dedicated-assignment desktop pool and select the **Enable automatic assignment** setting, Horizon Console automatically assigns machines to users.

Note If you select the **Enable automatic assignment** setting, you can still manually assign machines to users.

- When you create an automated pool, select the **Specify names manually** setting, and provide user names with the machine names, Horizon Console automatically assigns machines to users.
- When you create a dedicated-assignment desktop pool and select the **Enable Multi-User Assignment** setting, you can manually assign multiple users to the same machine.

If you do not select either setting in a dedicated-assignment pool, users do not have access to virtual desktops. You must manually assign a machine to each user.

You can also use the `vdadmin` command to assign machines to users. For more information about the `vdadmin` command, see the *Horizon Administration* guide.

Prerequisites

- Verify that the virtual machine belongs to a dedicated-assignment pool. In Horizon Console, the desktop pool assignment appears in the **User Assignment** column on the **Desktop Pools** page.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**, click a pool ID, and click the **Machines** tab.
- 2 Select the machine.
- 3 Select **Assign User(s)** from the **More Commands** drop-down menu.
- 4 Click **Add** and choose to select a domain, and type a search string in the **Name** or **Description** text box.
- 5 Select the user or users and click **Submit**.

What to do next

Navigate to **Users and Groups** to see the entitled users. After you assign a machine to a user or users and then navigate to **Users and Groups** and click **Find Machines** in the entitled group details, Connection Server searches and finds machines with assigned users for only those users and groups that belong to the same domain in the Active Directory group.

Unassign a User from a Dedicated Machine in Horizon Console

In a dedicated-assignment pool, you can remove a machine assignment to a user. If the dedicated-assignment pool is configured for multiple user assignment, you can remove a machine assignment for multiple users.

You can also use the `vdmadmin` command to remove a machine assignment to a user. For more information about the `vdmadmin` command, see the *Horizon Administration* guide.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**, double-click a pool ID, and click the **Inventory** tab.
- 2 Select the machine.
- 3 Select **Unassign User(s)** from the **More Commands** drop-down menu and select the user or users that you want to remove from the machine assignment.
- 4 Click **OK**.

Results

The machine is available and can be assigned to another user.

Update Machine Aliases for Assigned Users

In a dedicated-assignment pool, you can update the aliases for assigned users to provide a custom desktop name to the end user.

Prerequisites

- Verify that the **Show Machine Alias Name** option is enabled in the desktop pool settings. See [Worksheet for Creating an Instant-Clone Desktop Pool](#) or [Worksheet for Creating a Manual Desktop Pool](#).

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**, select a pool, and click the **Machines** tab.
- 2 Select a machine.

- 3 Select **Update Machine Aliases** from the **More Commands** drop-down menu, and enter a machine alias.
- 4 Click **OK**.

Setting Power Policies for Desktop Pools

You can configure a power policy for the virtual machines in a desktop pool if the virtual machines are managed by vCenter Server.

Power policies control how a virtual machine behaves when its associated desktop is not in use. A desktop is considered not in use before a user logs in and after a user disconnects or logs off.

You configure power policies when you create or edit desktop pools in Horizon Console.

Note You cannot configure power policies for desktop pools that have non-vSphere machines.

Power Policies for Desktop Pools

Power policies control how a virtual machine behaves when the associated remote desktop is not in use.

You set power policies when you create or edit a desktop pool. [Table 7-4. Power Policies](#) describes the available power policies.

Table 7-4. Power Policies

Power Policy	Description
Take no power action	<p>Horizon 8 does not enforce any power policy after a user logs off. This setting has two consequences.</p> <ul style="list-style-type: none"> ■ Horizon 8 does not change the power state of the virtual machine after a user logs off. <p>For example, if a user shuts down the virtual machine, the virtual machine remains powered off. If a user logs off without shutting down, the virtual machine remains powered on. When a user reconnects to the desktop, the virtual machine restarts if it was powered off.</p> <ul style="list-style-type: none"> ■ Horizon 8 does not enforce any power state after an administrative task is completed. <p>For example, a user might log off without shutting down. The virtual machine remains powered on. When a scheduled recomposition takes place, the virtual machine is powered off. After the recomposition is completed, Horizon 8 does nothing to change the power state of the virtual machine. It remains powered off.</p>
Always powered on	<p>The virtual machine remains powered on, even when it is not in use. If a user shuts down the virtual machine, it immediately restarts. The virtual machine also restarts after an administrative task such as refresh, recompose, or rebalance is completed.</p> <p>Select Always powered on if you run batch processes or system management tools that must contact the virtual machines at scheduled times.</p>
Suspend	<p>The virtual machine enters a suspended state when a user logs off, but not when a user disconnects.</p> <p>You can also configure machines in a dedicated pool to be suspended when a user disconnects without logging off. To configure this policy, you must set an attribute in Horizon Directory. See Configure Dedicated Machines To Be Suspended After Users Disconnect.</p> <p>When multiple virtual machines are resumed from a suspended state, some virtual machines might have delays in powering on. Whether any delays occur depends on the ESXi host hardware and the number of virtual machines that are configured on an ESXi host. Users connecting to their desktops from Horizon Client might temporarily see a desktop-not-available message. To access their desktops, users can connect again.</p> <p>This policy is not available for dedicated instant-clone desktop pools created with NVIDIA GRID vGPU.</p>
Power off	<p>The virtual machine shuts down when a user logs off, but not when a user disconnects.</p> <p>This policy is not available for dedicated instant-clone desktop pools created with NVIDIA GRID vGPU.</p>

When you configure a full-clone desktop pool with floating assignments, the machine is not powered off even with the power policy set to **Power off** when the maximum number of machines is equal to the number of spare (power on) machines.

Note When you add a machine to a manual desktop pool, verify that the machine is powered on to ensure that it is fully configured, even when you select the **Power off** or **Take no power** action power policies. After Horizon Agent is configured, it is marked as **Ready**, and the normal power-management settings for the pool apply.

For manual desktop pools that contain vSphere virtual machines, a spare machine is always powered on so that users can connect to it. The spare machine is powered on no matter which power policy is in effect.

Table 7-5. When Horizon 8 Applies the Power Policy describes when Horizon 8 applies the configured power policy to full-clone desktop pools.

Table 7-5. When Horizon 8 Applies the Power Policy

Desktop Pool Type	The power policy is applied ...
Instant-clone desktop pool with dedicated assignment Instant-clone desktop pool that contains vSphere virtual machines with dedicated assignment	<p>To dedicated virtual machines configured with default power policy set to Always powered on.</p> <p>On assigned machines, power operations are initiated by session management. Virtual machines are powered on when a user requests an assigned machine and are powered off or suspended when the user logs off.</p> <p>Note The Always powered on policy applies to assigned and unassigned machines.</p>
Automated full-clone pool with dedicated assignment Manual desktop pool that contains vSphere virtual machines with dedicated assignment	<p>To unassigned machines only.</p> <p>On assigned machines, power operations are initiated by session management. Virtual machines are powered on when a user requests an assigned machine and are powered off or suspended when the user logs off.</p> <p>Note The Always powered on policy applies to assigned and unassigned machines.</p>
Automated full-clone pool with floating assignment Manual desktop pool that contains vSphere virtual machines with floating assignment	<p>When a machine is not in use and after a user logs off.</p> <p>When you configure the Power off or Suspend power policy for a floating-assignment desktop pool, set Automatically logoff after disconnect to Immediately to prevent discarded or orphaned sessions.</p>
Manual desktop pool that contains one vSphere virtual machine with floating or dedicated assignment.	<p>Power operations are initiated by session management. The virtual machine is powered on when a user requests an assigned machine and is powered off or suspended when the user logs off.</p> <p>Note The Always powered on policy applies to assigned and unassigned machines.</p>

How Horizon 8 applies the configured power policy to automated pools depends on whether a machine is available. See [How Power Policies Affect Automated Desktop Pools](#) for more information.

Configure Dedicated Machines To Be Suspended After Users Disconnect

The **Suspend** power policy causes virtual machines to be suspended when a user logs off, but not when a user disconnects. You can also configure machines in a dedicated pool to be suspended when a user disconnects from a desktop without logging off. Using suspend when users disconnect helps to conserve resources.

To enable suspend on disconnect for dedicated machines, you must set an attribute in Horizon Directory.

Procedure

- 1 Start the ADSI Edit utility on your Connection Server host.
- 2 In the console tree, select **Connect to**.
- 3 In the **Select or type a domain or server** field, type the server name as `localhost:389`
- 4 Under **Connection point**, click **Select or type a distinguished name or naming context**, type the distinguished name as `DC=vdi,DC=vmware,DC=int`, and click **OK**.

The ADAM ADSI Edit main window appears.

- 5 Expand the ADAM ADSI tree and expand **OU=Properties**.
- 6 Select **OU=Global** and select **CN=Common** in the right pane
- 7 Select **Action > Properties**, and under the **pae-NameValuePair** attribute, add the new entry **suspendOnDisconnect=1**.
- 8 Restart the Connection Server service or Connection Server.

How Power Policies Affect Automated Desktop Pools

How Horizon 8 applies the configured power policy to automated pools depends on whether a machine is available.

A machine in an automated pool is considered available when it meets the following criteria:

- Is active
- Does not contain a user session
- Is not assigned to a user

The Horizon Agent service running on the machine confirms the availability of the machine to Connection Server.

When you configure an automated pool, you can specify the minimum and maximum number of virtual machines that must be provisioned and the number of spare machines that must be kept powered on and available at any given time.

Power Policy Examples for Automated Pools with Floating Assignments

When you configure an automated pool with floating assignments, you can specify that a particular number of machines must be available at a given time. The spare, available machines are always powered on, no matter how the pool policy is set.

Power Policy Example 1

[Table 7-6. Desktop Pool Settings for Automated Pool with Floating Assignment Example 1](#) describes the floating-assignment, automated pool in this example. The pool uses a machine-naming pattern to provision and name the machines.

Table 7-6. Desktop Pool Settings for Automated Pool with Floating Assignment Example 1

Desktop Pool Setting	Value
Number of machines (minimum)	10
Number of machines (maximum)	20
Number of spare, powered-on machines	2
Remote machine power policy	Power off

When this desktop pool is provisioned, 10 machines are created, two machines are powered on and immediately available, and eight machines are powered off.

For each new user that connects to the pool, a machine is powered on to maintain the number of spare, available machines. When the number of connected users exceeds eight, additional machines, up to the maximum of 20, are created to maintain the number of spare machines. After the maximum number is reached, the machines of the first two users who disconnect remain powered on to maintain the number of spare machines. The machine of each subsequent user is powered off according to the power policy.

Power Policy Example 2

[Table 7-7. Desktop Pool Settings for Automated Pool with Floating Assignments Example 2](#) describes the floating-assignment, automated pool in this example. The pool uses a machine-naming pattern to provision and name the machines.

Table 7-7. Desktop Pool Settings for Automated Pool with Floating Assignments Example 2

Desktop Pool Setting	Value
Number of machines (minimum)	5
Number of machines (maximum)	5

Table 7-7. Desktop Pool Settings for Automated Pool with Floating Assignments Example 2 (continued)

Desktop Pool Setting	Value
Number of spare, powered-on machines	2
Remote machine power policy	Power off

When this desktop pool is provisioned, five machines are created, two machines are powered on and immediately available, and three machines are powered off.

If a fourth machine in this pool is powered off, one of the existing machines is powered on. An additional machine is not powered on because the maximum of number of machines has already been reached.

Power Policy Example for Automated Pools with Dedicated Assignments

Unlike a powered-on machine in an automated pool with floating assignments, a powered-on machine in an automated pool with dedicated assignments is not necessarily available. It is available only if the machine is not assigned to a user.

[Table 7-8. Desktop Pool Settings for Automated Pool with Dedicated Assignments Example](#) describes the dedicated-assignment, automated pool in this example.

Table 7-8. Desktop Pool Settings for Automated Pool with Dedicated Assignments Example

Desktop Pool Setting	Value
Number of machines (minimum)	3
Number of machines (maximum)	5
Number of spare, powered-on machines	2
Remote machine power policy	Always powered on

When this desktop pool is provisioned, three machines are created and powered on. If the machines are powered off in vCenter Server, they are immediately powered on again, according to the power policy.

After a user connects to a machine in the pool, the machine becomes permanently assigned to that user. After the user disconnects from the machine, the machine is no longer available to any other user. However, the **Always powered on** policy still applies. If the assigned machine is powered off in vCenter Server, it is immediately powered on again.

When another user connects, a second machine is assigned. Because the number of spare machines falls below the limit when the second user connects, another machine is created and powered on. An additional machine is created and powered on each time a new user is assigned until the maximum machine limit is reached.

Preventing Horizon 8 Power Policy Conflicts

When you use Horizon Console to configure a power policy, you must compare the power policy to the settings in the guest operating system's Power Options control panel to prevent power policy conflicts.

A virtual machine can become temporarily inaccessible if the power policy configured for the machine is not compatible with a power option configured for the guest operating system. If there are other machines in the same pool, they can also be affected.

The following configuration is an example of a power policy conflict:

- In Horizon Console, the power policy **Suspend** is configured for the virtual machine. This policy causes the virtual machine to enter a suspended state when it is not in use.
- In the Power Options control panel in the guest operating system, the option **Put the Computer to sleep** is set to three minutes.

In this configuration, both Connection Server and the guest operating system can suspend the virtual machine. The guest operating system power option might cause the virtual machine to be unavailable when Connection Server expects it to be powered on.

Configure Desktop Session Timeouts in Horizon Console

You can specify timeout values for user inactivity and disconnected sessions.

Procedure

- ◆ In the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor, enable these settings:

Setting	Properties
Disconnect Session Time Limit (VDI)	<p>Specifies the amount of time after which a disconnected desktop session will automatically log off.</p> <ul style="list-style-type: none"> ■ Never: disconnected sessions on this machine will never log off. ■ Immediately: disconnected sessions will immediately be logged off. <p>You can also configure the time limit in the desktop pool setting Automatically logoff after disconnect in Horizon Console. If you configure this setting in both places, the GPO value takes precedence.</p> <p>For example, selecting Never here will prevent a disconnected session on this machine from ever logging off, regardless of what is set in Horizon Console.</p>
Idle Time Until Disconnect (VDI)	<p>Specifies the amount of time after which a desktop session will disconnect due to user inactivity.</p> <p>If disabled, unconfigured, or enabled with the setting Never, then the desktop sessions will never be disconnected.</p> <p>If the desktop pool or machine is configured to log off automatically after a disconnect, then that setting will be honored.</p> <p>The internal idle timer has a margin of error of 38 seconds. If you select 1 minute as the idle timeout, then the user will be disconnected automatically after 1 minute to 1 minute and 38 seconds of inactivity. If you select 5 minutes, then the user will be disconnected after 5 minutes to 5 minutes 38 seconds of inactivity.</p>

Changes take effect the next time the user connects to the session.

For more information on group policy settings, see VMware View Agent Configuration ADMX Template Settings in the *Horizon Remote Desktop Features and GPOs* document.

Managing Desktop Pools

You can perform administrative tasks on a desktop pool such as editing its properties, enabling, disabling, or deleting the pool.

Edit a Desktop Pool

You can edit an existing desktop pool to configure settings such as the number of spare machines, datastores, and customization specifications.

Prerequisites

Familiarize yourself with the desktop pool settings that you cannot change after a desktop pool is created. See [Fixed Settings in an Existing Desktop Pool](#).

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Select a desktop pool and click **Edit**.
- 3 Click a tab in the Edit dialog box and reconfigure desktop pool options.
- 4 Click **OK**.

Results

The desktop pool settings are updated.

If you change the image of an instant-clone desktop pool, the push image operation is invoked and the image publishing operation starts immediately. In Horizon Console, the summary page for the desktop pool shows the state for the pending image as *Publishing*.

If you change the cluster of an instant-clone desktop pool, new replica and golden image VMs are created in the new cluster. You can initiate a push image using the same image to have new clones created in the new cluster. However, the template VM, which is used in the cloning process, remains in the old cluster. You can put the ESXi host that the template VM is on in maintenance mode but you cannot migrate the template VM. To completely remove all infrastructure VMs including the template VM from the old cluster, you can initiate a push image using a new image.

Fixed Settings in an Existing Desktop Pool

After you create a desktop pool, you cannot change certain configuration settings.

Table 7-9. Fixed Settings in an Existing Desktop Pool

Setting	Description
Pool type	After you create an automated, manual, or RDS desktop pool, you cannot change the pool type.
User assignment	You cannot switch between dedicated assignments and floating assignments.
Type of virtual machine	You cannot switch between full virtual machines and instant-clone virtual machines.
Pool ID	You cannot change the pool ID.
vCenter settings	You cannot change vCenter settings for existing virtual machines. You can change vCenter settings in the Edit dialog box, but the values affect only new virtual machines that are created after the settings are changed.

Disable or Enable a Desktop Pool

When you disable a desktop pool, the pool is no longer presented to users and pool provisioning is stopped. Users have no access to the pool. After you disable a pool, you can enable it again.

Prerequisites

You can disable a desktop pool to prevent users from accessing their remote desktops while you prepare the desktops for use. If a desktop pool is no longer needed, you can use the disable feature to withdraw the pool from active use without having to delete the desktop pool definition from Horizon Console.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Select a desktop pool and change the status of the pool.

Option	Action
Disable the pool	Select Disable Desktop Pool from the Status drop-down menu.
Enable the pool	Select Enable Desktop Pool from the Status drop-down menu.

- 3 Click **OK**.

Disable or Enable Provisioning in a Desktop Pool

When you disable provisioning in an automated desktop pool, Horizon 8 stops provisioning new virtual machines for the pool. After you disable provisioning, you can enable provisioning again.

Before you change a desktop pool's configuration, you can disable provisioning to ensure that no new machines are created with the old configuration. You also can disable provisioning to prevent Horizon 8 from using additional storage when a pool is close to filling up the available space.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Select a desktop pool and change the status of the pool.

Option	Action
Disable provisioning	Select Disable Provisioning from the Status drop-down menu.
Enable provisioning	Select Enable Provisioning from the Status drop-down menu.

- 3 Click **OK**.

Duplicate an Automated Desktop Pool

You can duplicate an automated desktop pool from an existing pool. When you duplicate a pool, the existing desktop pool's settings are copied into the duplicate desktop pool, allowing you to create a new pool without having to fill in each setting manually.

With this feature, you can streamline pool creation because you do not have to type every option in the wizard to add a desktop pool. You can ensure that desktop pool attributes are standardized by using the pre-filled values in the wizard.

You can duplicate automated desktop pools that contain full virtual machines or instant clones. You cannot duplicate manual desktop pools, or published desktop pools.

When you duplicate an instant-clone desktop pool that has the golden image virtual machine and its snapshot configured with NVIDIA Grid vGPU, the Suspend and Power Off power policies will not be available for selection in the duplicate pool wizard. Suspend and Power Off power policies will be available only when the selected golden image and its snapshot are not configured with NVIDIA Grid vGPU.

When you duplicate a full-clone desktop pool that has the virtual machine template configured with NVIDIA Grid vGPU, the Suspend power policy will not be available for selection in the duplicate pool wizard. Suspend power policy will be available only when the selected virtual machine template is not configured with NVIDIA Grid vGPU.

Prerequisites

- Verify that the prerequisites for creating the original desktop pool are still valid.

When you clone a pool, you can use the same virtual machine template, a golden image virtual machine, or you can select another one.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Select the desktop pool that you want to duplicate and click **Duplicate**.

The **Duplicate Pool** wizard appears.

Note You cannot change the settings for the desktop pool on the **Type**, **vCenter Server**, and **User Assignment** pages. You can modify settings on the other pages in the **Duplicate Pool** wizard.

- 3 To uniquely identify the duplicate desktop pool, on the **Desktop Pool Identification** page, type a unique pool ID.
- 4 On the **Provisioning Settings** page, provide unique names for the virtual machines.

Option	Description
Use a naming pattern	Type a virtual machine naming pattern.
Specify names manually	Provide a list of unique names for the virtual machines.

- 5 Click **Submit** or follow the other prompts in the wizard to complete and create the pool.
Change desktop pool settings and values as needed.

Results

In Horizon Console, you can view the machines as they are added to the pool by selecting **Inventory > Desktops**.

What to do next

Entitle users to access the pool.

Delete a Desktop Pool

When you delete a desktop pool, users can no longer launch new remote desktops in the pool.

By default, you can delete a desktop pool even if desktop machines exist in the pool.

With an automated desktop pool of instant clones, Horizon 8 always deletes the virtual machines from disk.

Important Do not delete the virtual machines in vCenter Server before you delete a desktop pool with Horizon Console. This action could put Horizon 8 components into an inconsistent state.

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Select a desktop pool and click **Delete**.

Results

Horizon 8 deletes all virtual machines from disk and terminates users' sessions to their remote desktops. On the **Desktops** page, the pool status appears as **Deleting**. It can take some time for Horizon 8 to delete the internal VMs from vCenter Server. Do not remove vCenter Server from Horizon Console until you verify that all the internal VMs are deleted.

Delete Virtual-Machine Desktops in a Pool

When you delete a virtual-machine desktop, users can no longer access the desktop.

Note Do not delete the virtual machines in vCenter Server before you delete virtual-machine desktops with Horizon Console. This action could put Horizon 8 components into an inconsistent state.

Procedure

- 1 In Horizon Console, select **Inventory > Machines**
- 2 Select the **vCenter VMs** tab.
- 3 Select one or more machines and click **Remove**.

Results

vCenter Server deletes the instant-clone virtual machines from disk. Users in currently active sessions are disconnected from their remote desktops. With instant clones, vCenter Server always deletes the virtual machines from disk.

Note If you deleted a desktop pool in **Inventory > Desktops** the status of the desktop pool also appears as **Deleting** in **Inventory > Machines**.

Export Horizon 8 Information to External Files

In Horizon Console, you can export Horizon 8 table information to external files. You can export the tables that list users and groups, pools, machines, events, and virtual desktop sessions. You can view and manage the information in a spreadsheet or another tool.

For example, you might collect information about machines that are managed by more than one Connection Server instance or group of replicated Connection Server instances. You can export the Machines table from each Horizon Console interface and view it in a spreadsheet.

When you export a Horizon Console table, it is saved as a Microsoft Excel Open XML Format Spreadsheet (XLSX) file. This feature exports the entire table, not individual pages.

Procedure

- 1 In Horizon Console, display the table you want to export.
For example, click **Inventory > Machines** to display the machines table.
- 2 Click the export icon in the upper right corner of the table.
When you point to the icon, the `Export table contents` tooltip appears.
- 3 Type a filename for the XLSX file in the Select location for download dialog box.
- 4 Browse to a location to store the file.
- 5 Click **Save**.

What to do next

Open a spreadsheet or another tool to view the XLSX format file.

Examining GPU Resources on an ESXi Host

To better manage the GPU resources that are available on an ESXi host, you can examine the current GPU resource reservation. The ESXi command-line query utility, `gpuvmm`, lists the GPUs that are installed on an ESXi host and displays the amount of GPU memory that is reserved for each virtual machine on the host. Note that this GPU memory reservation is not the same as virtual machine VRAM size.

To run the utility, type `gpuvmm` from a shell prompt on the ESXi host. You can use a console on the host or an SSH connection.

For example, the utility might display the following output:

```
~ # gpuvmm
Xserver unix:0, GPU maximum memory 2076672KB
    pid 118561, VM "JB-w7-64-FC3", reserved 131072KB of GPU memory.
    pid 64408, VM "JB-w7-64-FC5", reserved 261120KB of GPU memory.
GPU memory left 1684480KB.
```

Similarly, you can use the `nvidia-smi` command on the ESXi host to see a list of NVIDIA GRID vGPU-enabled virtual machines, the amount of frame buffer memory consumed, and the slot ID of the physical GPU that the virtual machine is using.

Creating Desktop Pools on a Single Host SDDC on VMware Cloud on AWS

VMware Cloud on AWS allows you to deploy a starter configuration containing a single host. The single host SDDC starter configuration is appropriate for test and development or proof of concept (PoC) use cases. Horizon 8 supports creating full clones and instant clones on a single host SDDC for PoCs.

Do not run production workloads on a single host SDDC. Delete any desktop pools created for PoCs before scaling your SDDC to a full production SDDC.

For single host SDDC limitations, see "Deploying a Single Host SDDC Starter Configuration" in *VMware Cloud on AWS Product Documentation*.

Prevent Access to VMware Horizon Desktops Through RDP

In certain VMware Horizon environments, it is a priority to prohibit access to VMware Horizon desktops through the RDP display protocol. You can prevent users and administrators from using RDP to access VMware Horizon desktops by configuring pool settings and a group policy setting.

By default, while a user is logged in to a remote desktop session, you can use RDP to connect to the virtual machine. The RDP connection terminates the remote desktop session, and the user's unsaved data and settings might be lost. The user cannot log in to the desktop until the external RDP connection is closed. To avoid this situation, disable the `AllowDirectRDP` setting.

Note Remote Desktop Services must be started on the virtual machine that you use to create pools and on the virtual machines that are deployed in the pools. Remote Desktop Services are required for Horizon Agent installation, SSO, and other Horizon session-management operations.

Prerequisites

Verify that the Horizon Agent Configuration Administrative Template (ADMX) file is installed in Active Directory.

Procedure

- 1 Select the display protocol that you want Horizon Connection Server to use to communicate with Horizon Client devices.

Option	Description
Create a desktop pool	<ol style="list-style-type: none">a In Horizon Console, start the Add Pool wizard.b On the Remote Display Protocol page, select VMware Blast or PCoIP as the default display protocol.
Edit an existing desktop pool	<ol style="list-style-type: none">a In Horizon Console, select the desktop pool and click Edit.b On the Desktop Pool Settings tab, select VMware Blast or PCoIP as the default display protocol.

- 2 For the **Allow users to choose protocol** setting, select **No**.
- 3 Prevent devices that are not running Horizon Client from connecting directly to Horizon desktops through RDP by disabling the `AllowDirectRDP` group policy setting.
 - a On your Active Directory server, open the Group Policy Management Console and select **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware Horizon Agent Configuration**.
 - b Disable the `AllowDirectRDP` setting.

Managing Storage for Virtual Desktops

8

Deploying desktops on virtual machines that are managed by vCenter Server provides all the storage efficiencies and capabilities enabled by vCenter. Using instant clones as desktop machines increases the storage savings because all virtual machines in a pool share a virtual disk with a base image.

This chapter includes the following topics:

- [Managing Storage with vSphere](#)
- [Reducing Storage Requirements with Instant Clones](#)
- [Storage Sizing for Instant-Clone Desktop Pools](#)
- [Reclaim Disk Space on Instant Clones](#)
- [Enable Periodic Space Reclamation for vSphere 6.7 and Earlier on Non-vSAN Datastores](#)
- [Reclaiming Disk Space for vSphere 6.7 and Later On Non-vSAN Datastores](#)
- [Reclaim Disk Space for vSphere 6.7U1 and later on vSAN datastores](#)
- [Set Storage Accelerator and Space Reclamation Blackout Times](#)

Managing Storage with vSphere

vSphere lets you virtualize disk volumes and file systems so that you can manage and configure storage without having to consider where the data is physically stored.

Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are widely used storage technologies supported by vSphere to meet different data center storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning them to virtual machines.

Instead of external arrays, you can use vSAN, which virtualizes the local physical solid-state disks and hard disk drives available on ESXi hosts into a single datastore shared by all hosts in a cluster. vSAN provides high-performance storage with policy-based management, so that you specify only one datastore when creating a desktop pool, and the various components, such as virtual machine files, replicas, user data, and operating system files, are placed on the appropriate solid-state drive (SSD) disks or direct-attached hard disks (HDDs).

vSAN also lets you manage virtual machine storage and performance by using storage policy profiles. If the policy becomes noncompliant because of a host, disk, or network failure, or workload changes, vSAN reconfigures the data of the affected virtual machines and optimizes the use of resources across the cluster.

Note vSAN is compatible with the View storage accelerator feature but not with the space-efficient disk format feature, which reclaims disk space by wiping and shrinking disks.

With vSphere, you can optionally use Virtual Volumes (vVols). This feature maps virtual disks and their derivatives, clones, snapshots, and replicas, directly to objects, called virtual volumes, on a storage system. This mapping allows vSphere to offload intensive storage operations such as snapshotting, cloning, and replication to the storage system.

Virtual Volumes also lets you manage virtual machine storage and performance by using storage policy profiles in vSphere. These storage policy profiles dictate storage services on a per-virtual-machine basis. This type of granular provisioning increases capacity utilization.

Note Virtual Volumes is compatible with the View storage accelerator feature but not with the space reclamation feature.

Note Instant clones do not support Virtual Volumes.

Using VMware vSAN for High-Performance Storage and Policy-Based Management

VMware vSAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of vSphere hosts. You specify only one datastore when creating an automated desktop pool or an automated farm, and the various components, such as virtual machine files, replicas, user data, and operating system files, are placed on the appropriate solid-state drive (SSD) disks or direct-attached hard disks (HDDs).

vSAN implements a policy-based approach to storage management. When you use vSAN, Horizon 8 defines virtual machine storage requirements, such as capacity, performance, and availability, in the form of default storage policy profiles and automatically deploys them for virtual desktops onto vCenter Server. The policies are automatically and individually applied per disk (vSAN objects) and maintained throughout the life cycle of the virtual desktop. Storage is provisioned and automatically configured according to the assigned policies. You can modify these policies in vCenter. Horizon 8 creates vSAN policies for instant-clone desktop pools, full-clone desktop pools, or an automated farm per Horizon 8 cluster.

You can enable encryption for a vSAN cluster to encrypt all data-at-rest in the vSAN datastore. vSAN encryption is available with vSAN version 6.6 or later. For more information about encrypting a vSAN cluster, see the *VMware vSAN* documentation.

Each virtual machine maintains its policy regardless of its physical location in the cluster. If the policy becomes noncompliant because of a host, disk, or network failure, or workload changes, vSAN reconfigures the data of the affected virtual machines and load-balances to meet the policies of each virtual machine.

While supporting VMware vSphere features that require shared storage, such as HA, vMotion, and DRS, vSAN eliminates the need for an external shared storage infrastructure and simplifies storage configuration and virtual machine provisioning activities.

vSAN Workflow in Horizon 8

- 1 When creating an automated desktop pool or an automated farm in Horizon Console, under **Storage Policy Management**, select **Use VMware vSAN**, and select the vSAN datastore to use.

After you select **Use VMware vSAN**, only the vSAN datastore is displayed.

Default storage policy profiles are created according to the clone type you choose.

- 2 (Optional) Use vCenter Server to modify the parameters of the storage policy profiles, which include things like the number of failures to tolerate and the amount of SSD read cache to reserve. For specific default policies and values, see [Default Storage Policy Profiles for vSAN Datastores](#).
- 3 Use vCenter Server to monitor the vSAN cluster and the disks that participate in the datastore. For more information, see the *Administering VMware vSAN* document.

Requirements and Limitations

The vSAN feature has the following requirements and limitations when used in a Horizon 8 deployment:

- vSAN does not support VVOLs.
- vSAN is compatible with the View Storage Accelerator feature. vSAN provides a caching layer on SSD disks, and the View Storage Accelerator feature provides a content-based cache that reduces IOPS and improves performance during boot storms.
- Use appropriate hardware with vSAN. For specifics, see the [VMware Compatibility Guide](#).
- Be mindful of cluster size and the vSAN maximum limit. For more information on storage requirements and sizing limits, see [VMware Configuration Maximums](#).

For more information about vSAN requirements, see the *Administering VMware vSAN* document. For guidance on sizing and designing the key components of Horizon 8 virtual desktop infrastructures for VMware vSAN, see the white paper at <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.

Default Storage Policy Profiles for vSAN Datastores

When you use vSAN, Horizon 8 defines virtual machine storage requirements, such as capacity, performance, and availability, in the form of default storage policy profiles, which you can modify. Storage is provisioned and automatically configured according to the assigned policies. The default policies that are created during desktop pool creation depend on the type of pool you create.

vSAN offers a storage policy framework so that you can control the behavior of various virtual machine objects that reside on the vSAN datastore. An example of an object in vSAN is a virtual disk (VMDK) file, and there are four characteristics of each object that are controlled through policy:

- **Stripes:** Number of disk stripes per object. The number of disk stripes affects how many magnetic disks you have (HDDs).
- **Resiliency:** Number of failures to tolerate. The number of host failures to tolerate depends, of course, on the number of hosts you have.
- **Storage Reservation:** Object space reservation. Controls how much storage is set aside.
- **Cache Reservation:** Flash read-cache reservation.

The stripes and cache reservation settings are used to control performance. The resiliency setting controls availability. The storage provisioning setting control capacity. These settings, taken together, affect how many vSphere hosts and magnetic disks are required.

For example, if you set the number of disk stripes per object to 2, vSAN will stripe the object across at least 2 HDDs. In conjunction with this setting, if you set the number of host failures to tolerate to 1, vSAN will create an additional copy for resiliency and therefore require 4 HDDs. Additionally, setting the number of host failures to tolerate to 1 requires a minimum of 3 ESXi hosts, 2 for resiliency and the third to break the tie in case of partitioning.

Note If you are deploying Horizon 8 on VMware Cloud on AWS and require guidance on how to set the FTT value to meet the VMware Cloud on AWS SLA requirement, see the VMware Knowledge Base article <https://kb.vmware.com/s/article/76366>.

Table 8-1. Horizon Default Policies and Settings

Policy (as it appears in vCenter Server)	Description	Number of disk stripes per object	Number of failures to tolerate	Flash read-cache reservation	Object space reservation
FULL_CLONE_DISK_<guid>	Dedicated full-clone virtual disk	1	1	0	0
FULL_CLONE_DISK_FLOATING_<guid>	Floating full-clone virtual disk	1	0	0	0
OS_DISK_FLOATING_<guid>	Floating instant-clone OS and disposable disks	1	1	0	0
REPLICA_DISK_<guid>	Instant-clone replica disk	1	1	0	0
VM_HOME_<guid>	VM home directory	1	1	0	0

Note <guid> indicates the UUID of the Horizon 8 cluster.

Once these policies are created for the virtual machines, they will never be changed by Horizon 8. An administrator can edit the policies created by Horizon 8 by going into vCenter through the vSphere client or the vSphere Command-Line Interface (`esxcli`), with the option to make the changes effective across all existing VMs or to any new VMs. Any new default policies enacted by Horizon 8 will not impact existing desktops pools. Each virtual machine maintains its policy regardless of its physical location in the cluster. If the policy becomes non-compliant because of a host, disk, network failure, or workload changes, vSAN reconfigures the data of the affected virtual machines and load-balances to meet the policies of each virtual machine.

Note If you inadvertently attempt to use settings that contradict each other, when you attempt to apply the settings, the operation will fail, and an error message might inform you that you do not have enough hosts.

Using Virtual Volumes for Virtual-Machine-Centric Storage and Policy-Based Management

With Virtual Volumes (VVols), an individual virtual machine, not the datastore, becomes a unit of storage management. The storage hardware gains control over virtual disk content, layout, and management. Horizon 8 only supports VVols with full-clone virtual machines. Virtual Volumes datastores are not supported for instant clone desktop pools.

With Virtual Volumes, abstract storage containers replace traditional storage volumes based on LUNs or NFS shares. Virtual Volumes maps virtual disks and their derivatives, clones, snapshots, and replicas, directly to objects, called virtual volumes, on a storage system. With this mapping, vSphere can offload intensive storage operations such as snapshotting, cloning, and replication to the storage system. The result, for example, is that a cloning operation that previously took an hour might now take a few minutes using Virtual Volumes.

Important One of the key benefits of Virtual Volumes is the ability to use Software Policy-Based Management (SPBM). However, Horizon 8 does not create the default granular storage policies that vSAN creates. Instead, you can set a global default storage policy in vCenter Server that applies to all Virtual Volume datastores.

Virtual Volumes has the following benefits:

- Virtual Volumes supports offloading a number of operations to storage hardware. These operations include taking snapshots, cloning, and Storage DRS.
- With Virtual Volumes, you can use advanced storage services that include replication, encryption, deduplication, and compression on individual virtual disks.
- Virtual Volumes supports such vSphere features as vMotion, Storage vMotion, snapshots, Flash Read Cache, and DRS.

- You can use Virtual Volumes with storage arrays that support vSphere APIs for Array Integration (VAAI).

Note Virtual Volumes is compatible with the View Storage Accelerator feature. vSAN provides a caching layer on SSD disks, and the View Storage Accelerator feature provides a content-based cache that reduces IOPS and improves performance during boot storms.

The Virtual Volumes feature has the following requirements:

- Appropriate hardware. Certain storage vendors are responsible for supplying storage providers that can integrate with vSphere and provide support for Virtual Volumes. Every storage provider must be certified by VMware and properly deployed.
- All virtual disks that you provision on a virtual datastore must be an even multiple of 1 MB.

Virtual Volumes is a vSphere feature. For more information about the requirements, functionality, background, and setup requirements, see the topics about Virtual Volumes in the *vSphere Storage* document.

Reducing Storage Requirements with Instant Clones

Instant clones leverage vSphere vmFork technology to quiesce a running base image, or parent VM, and rapidly create and customize a pool of virtual desktops.

Instant clones share the virtual disks with the parent VM at the time of creation. Each instant clone acts like an independent desktop with a unique host name and IP address, yet the instant clone requires significantly less storage. Instant clones reduce the required storage capacity by 50 to 90 percent.

Storage for Instant Clones

Instant clones support the use of all standard vSphere storage options: VMFS, NFS, vSAN, and local datastores.

You can store instant clones on spinning media-backed (HDDs) datastores or on datastores backed by solid-state drives (SSDs). HDDs provide lower performance, but are less expensive and provide higher storage capacity. SSDs have low storage capacity and high read performance, typically supporting tens of thousands of I/Os per second (IOPS).

One way to lower the storage cost is through the tiered use of HDDs and SSDs. When you create an instant-clone desktop pool, Horizon 8 creates a series of internal VMs for managing instant clones. One such internal VM is a replica, which is essentially a full clone made from the golden image. The replica and the subsequent instant clones made from it can be placed on the same datastore/LUN (logical unit number), or separate datastores with different performance characteristics. For example, you can store the replica VMs on a SSD-backed datastore. A typical environment has only a small number of replica VMs, so replicas do not require much storage. You can then store instant clones on HDDs. They are inexpensive and provide high storage capacity, which makes them suited for storing a large number of clones.

Configuring replicas and clones in this way can reduce the impact of I/O storms that occur when many clones are created at once. For example, if you deploy a floating-assignment pool with a delete-machine-on-logoff policy, and your users start work at the same time, Horizon 8 must concurrently provision new machines for them.

Important This feature is designed for specific storage configurations provided by vendors who offer high-performance disk solutions. Do not store replicas on a separate datastore if your storage hardware does not support high-read performance.

You must follow certain requirements when you store the replica and clones in a pool on separate datastores:

- You can specify only one separate replica datastore for a pool.
- The replica datastore must be accessible from all ESXi hosts in the cluster.
- This feature is not available if you use vSAN datastores. These types of datastores use Software Policy-Based Management, so that storage profiles define which components go on which types of disks.

Availability Considerations for Storing Replicas on a Separate Datastore

You can store replica VMs on a separate datastore or on the same datastores as the clones. These configurations affect the availability of the pool in different ways.

When you store replicas on the same datastores as the clones to enhance availability, a separate replica is created on each datastore. If a datastore becomes unavailable, only the clones on that datastore are affected. Clones on other datastores continue to run.

When you store replicas on a separate datastore, all clones in the pool are anchored to the replicas on that datastore. If the datastore becomes unavailable, the entire pool is unavailable.

To enhance the availability of the desktop pool, you can configure a high-availability solution for the datastore on which you store the replicas.

Storage Sizing for Instant-Clone Desktop Pools

Horizon 8 provides high-level guidelines that can help you determine how much storage an instant-clone desktop pool requires.

During the instant clone pool creation process, Horizon 8 displays a storage-sizing table with the free space on the datastores that you select for storing OS disks. You can decide which datastores to use by comparing the actual free space with the estimated requirements for the desktop pool. The formulas used in the table only provide a general estimate of storage use. The clones' actual storage growth depends on many factors:

- Amount of memory assigned to the golden image.
- Size of the guest operating system's paging file.

- Workload on the desktop machines, determined primarily by the types of applications that users run in the guest operating system.

Note In a deployment that includes hundreds or thousands of clones, configure your desktop pool so that particular sets of datastores are dedicated to particular ESXi clusters. Do not configure pools randomly across all the datastores so that most or all ESXi hosts must access most or all LUNs.

When too many ESXi hosts attempt to write to the OS disks on a particular LUN, contention problems can occur, degrading performance and interfering with scalability. For more information about datastore planning in large deployments, see the *Horizon Overview and Deployment Planning* document.

Storage Sizing Guidelines for Instant-Clone Desktop Pools

When you create or edit an instant-clone desktop pool, the **Select Instant Clone Datastores** page displays a table that provides storage-sizing guidelines. The table can help you to decide which datastores to select for the instant-clone disks. The guidelines calculate space needed for new clones.

Sizing Table for OS Disks

Example Sizing Table for OS Disks shows an example of storage-sizing recommendations that might be displayed for a pool of 10 virtual machines if the golden image virtual machine has 1GB of memory and a 10GB replica.

Table 8-2. Example Sizing Table for OS Disks

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	40.00	80.00	130.00

The **Selected Free Space** column shows the total available space on all of the datastores that you selected for a disk type such as OS disks.

The **Min Recommended** column shows the minimum amount of recommended storage for a pool.

The **50% Utilization** column shows the recommended storage when the disks grow to 50% of the golden image.

The **Max Recommended** column shows the recommended storage when the disks approach the full size of the golden image.

Horizon 8 estimates the storage space that is needed for new clones. When you create a desktop pool, the sizing guidelines encompass the entire pool. When you edit an existing desktop pool, the guidelines encompass only the new clones that you add to the pool.

For example, if you add 100 clones to a desktop pool and select a new datastore, Horizon 8 estimates space requirements for the 100 new clones. If you select a new datastore but keep the desktop pool the same size, or reduce the number of clones, the sizing guidelines show 0. The value of 0 reflects that no new clones must be created on the selected datastore. Space requirements for the existing clones are already accounted for.

How Horizon 8 Calculates the Minimum Sizing Recommendations

To arrive at a minimum recommendation for OS disks, Horizon 8 estimates that each clone consumes twice its memory size when it is first created and started up. If no memory is reserved for a clone, an ESXi swap file is created for a clone as soon as it is powered on. The size of the guest operating system's paging file also affects the growth of a clone's OS disk.

In the minimum recommendation for OS disks, Horizon 8 also includes space for two replicas on each datastore. Horizon 8 creates one replica when a pool is created. When the instant-clone pool is patched for the first time by a push image, Horizon 8 creates a second replica on the datastore, anchors the clones to the new replica, and deletes the first replica if no other clones are using original snapshot. The datastore must have the capacity to store two replicas during the recompose operation.

By default, replicas use vSphere thin provisioning, but to keep the guidelines simple, Horizon 8 accounts for two replicas that use the same space as the golden image virtual machine.

To arrive at a minimum recommendation storing replicas on a separate datastore, Horizon 8 allows space for two replicas on the datastore. The same value is calculated for minimum and maximum usage.

For details, see [Storage Sizing Formulas for Instant-Clone Desktop Pools](#).

Storage Sizing Formulas for Instant-Clone Desktop Pools

Storage-sizing formulas can help you estimate how much disk space is required on the datastores that you select for OS disks and replicas.

Storage Sizing Formulas

Storage Sizing Formulas for Clone Disks on Selected Datastores shows the formulas that calculate the estimated sizes of the disks when you create a pool and as the clones grow over time. These formulas include the space for replica disks that are stored with the clones on the datastore.

If you edit an existing pool or store replicas on a separate datastore, Horizon 8 uses a different sizing formula. See [Storage Sizing Formulas for Creating Instant Clones When You Edit a Pool or Store Replicas on a Separate Datastore](#).

Table 8-3. Storage Sizing Formulas for Clone Disks on Selected Datastores

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	Free space on the selected datastores	Number of VMs * (2 * memory of VM) + (2 * replica disk)	Number of VMs * (50% of replica disk + memory of VM) + (2 * replica disk)	Number of VMs * (100% of replica disk + memory of VM) + (2 * replica disk)

Example of a Storage Sizing Estimate

In this example, the golden image is configured with 1GB of memory. The golden image's disk size is 10GB. A pool is created with 10 machines.

The OS disks are configured on a datastore that currently has 184.23GB of available space.

Example of a Sizing Estimate for Clone Disks Deployed on Selected Datastores shows how the sizing formulas calculate estimated storage requirements for the sample desktop pool.

Table 8-4. Example of a Sizing Estimate for Clone Disks Deployed on Selected Datastores

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	10 * (2*1GB) + (2*10GB) = 40.00	10 * (50% of 10GB + 1GB) + (2*10GB) = 80.00	10 * (100% of 10GB + 1GB) + (2*10GB) = 130.00

Storage Sizing Formulas for Creating Instant Clones When You Edit a Pool or Store Replicas on a Separate Datastore

Horizon 8 calculates different sizing formulas when you edit an existing desktop pool, or store replicas on a separate datastore, than when you first create a pool.

If you edit an existing pool and select datastores for the pool, Horizon 8 creates new clones on the selected datastores. The new clones are anchored to the existing snapshot and use the existing replica disk. No new replicas are created.

Horizon 8 estimates the sizing requirements of new clones that are added to the desktop pool. Horizon 8 does not include the existing clones in the calculation.

If you store replicas on a separate datastore, the other selected datastores are dedicated to the OS disks.

Storage Sizing Formulas for Clone Disks When You Edit a Pool or Store Replicas on a Separate Datastore shows the formulas that calculate the estimated sizes of clone disks when you edit a pool or store replicas on a separate datastore.

Table 8-5. Storage Sizing Formulas for Clone Disks When You Edit a Pool or Store Replicas on a Separate Datastore

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	Free space on the selected datastores	Number of new VMs * (2 * memory of VM)	Number of new VMs * (50% of replica disk + memory of VM)	Number of new VMs * (100% of replica disk + memory of VM)

Example of a Storage Sizing Estimate When You Edit a Pool or Store Replicas on a Separate Datastore

In this example, the golden image virtual machine is configured with 1GB of memory. The golden image virtual machine's disk size is 10GB. A pool is created with 10 machines.

The OS disks are configured on a datastore that currently has 184.23GB of available space.

Example of a Sizing Estimate for Clone Disks When You Edit a Pool or Store Replicas on a Separate Datastore shows how the sizing formulas calculate estimated storage requirements for the sample pool.

Table 8-6. Example of a Sizing Estimate for Clone Disks When You Edit a Pool or Store Replicas on a Separate Datastore

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	10 * (2*1GB) = 20.00	10 * (50% of 10GB + 1GB) = 60.00	10 * (100% of 10GB + 1GB) = 110.00

Storing Instant Clones on Local Datastores (non-vSAN)

Instant-clone virtual machines can be stored on local datastores, which are internal spare disks on ESXi hosts. Local storage offers advantages such as inexpensive hardware, fast virtual-machine provisioning, high performance power operations, and simple management. However, using local storage limits the vSphere infrastructure configuration options that are available to you. Using local storage is beneficial in certain Horizon 8 environments but not appropriate in others. Only NVMe, SAS or SATA drives are supported.

Note The limitations described in this topic do not apply to vSAN datastores, which also use local storage disks but turns them into shared storage.

Using local datastores is most likely to work well if the Horizon 8 desktops in your environment are non-persistent. For example, you might use local datastores if you deploy kiosks or classroom and training stations.

Consider using local datastores if your virtual machines have floating assignments, are not dedicated to individual end users, do not require persistent disks for user data, and can be deleted or refreshed at regular intervals such as on user logoff. This approach lets you control the disk usage on each local datastore without having to move or load-balance the virtual machines across datastores.

However, you must consider the restrictions that using local datastores imposes on your Horizon 8 desktop or farm deployment:

- You cannot use VMotion.
- You cannot use VMware vSphere High Availability.
- You cannot use the vSphere Distributed Resource Scheduler (DRS).
- If you are deploying instant clones on a single ESXi host with a local datastore, you must configure a cluster containing that single ESXi host. If you have a cluster of two or more ESXi hosts with local datastores, select the local datastore from each of the hosts in the cluster. Otherwise, instant clone creation fails..
- Local spinning-disk drives and a storage array might have similar capacity, but local spinning-disk drives do not have the same throughput as a storage array. Throughput increases as the number of spindles grows. If you select direct attached solid-state disks (SSDs), performance is likely to exceed that of many storage arrays. Local datastore support for instant clones is available for both virtual desktops and published desktops

Configure View Storage Accelerator for Desktop Pools

You can enable View Storage Accelerator on pools that contain instant clones and on pools that contain full-clone virtual machines. This feature uses the Content Based Read Cache (CBRC) feature in ESXi hosts.

CBRC uses ESXi host memory to cache virtual machine disk data, reduce IOPS, and improve performance during boot storms, when many machines start up or run anti-virus scans at once. By reducing the number of IOPS during boot storms, View Storage Accelerator lowers the demand on the storage array, which lets you use less storage to support your Horizon 8 deployment. The feature is also beneficial when administrators or users load applications or data frequently.

When a virtual machine is created, Horizon 8 indexes the contents of each virtual disk file. The indexes are stored in a virtual machine digest file. At runtime, the ESXi host reads the digest files and caches common blocks of data in memory. To keep the ESXi host cache up to date, Horizon 8 regenerates the digest file at regular intervals. You can modify the regeneration interval.

Native NFS snapshot technology (VAAI) and Vvols are not supported in pools that are enabled for View Storage Accelerator. vSphere VM Encryption is also not supported with View Storage Accelerator.

To enable the View Storage Accelerator feature, you must enable it globally and then enable it for individual desktop pools. For details on how to enable or disable View Storage Accelerator globally, see the *Horizon Installation and Upgrade* document.

After View Storage Accelerator is enabled globally, you can enable or disable it for individual full-clone desktop pools. For instant-clone desktop pools, View Storage Accelerator is only needed for replica VMs and is enabled automatically for individual pools. It cannot be turned off on a pool level. To disable, you must disable View Storage Accelerator globally, and this step will also disable the feature for full clone pools.

Note Disabling View Storage Accelerator globally will not change the existing instant clone pool. The new instant clone pool still needs to be deployed.

View Storage Accelerator is enabled for a full-clone pool by default. The feature can be disabled or enabled when you create or edit a pool. The best approach is to enable this feature when you first create a desktop pool.

Procedure

- 1 In Horizon Console, display the **Advanced Storage Options** tab in the pool creation wizard.

Option	Description
New desktop pool (recommended)	Start the Add Pool wizard to begin creating an automated desktop pool. Follow the wizard configuration prompts until you reach the Advanced Storage Options page.
Existing desktop pool	Select the existing pool, click Edit , and click the Advanced Storage Options tab. If you modify View Storage Accelerator settings for an existing desktop pool, the changes do not take effect until the virtual machines in the desktop pool are powered off.

- 2 To enable View Storage Accelerator for the pool, make sure that the **Use View Storage Accelerator** check box is selected.

This setting is selected by default. To disable the setting, uncheck the **Use View Storage Accelerator** box. You cannot select a disk type. View Storage Accelerator is performed on the whole virtual machine.

- 3 (Optional) In the **Regenerate storage accelerator after** text box, specify the interval, in days, after which the regeneration for View Storage Accelerator digest files take place.

The default regeneration interval is seven days.

What to do next

You can configure blackout days and times during which disk space reclamation and View Storage Accelerator regeneration do not take place. See [Set Storage Accelerator and Space Reclamation Blackout Times](#).

Reclaim Disk Space on Instant Clones

The disk space reclamation feature is for longer-lived instant clones.

Instant clones can be either short-lived or longer-lived. Short-lived instant clones are clones created with floating assignment or dedicated assignment with the **Refresh on Logoff** set to **Always**. Short-lived instant clones are deleted and then recreated whenever a user logs out. Because of the frequent refresh of short-lived instant clones, the clones' OS disks do not get much chance to grow unlike the OS disks for longer-lived instant clones, so it is beneficial to allow ESXi hosts to reclaim unused disk space, thereby reducing the total storage space required.

Horizon 8 creates all instant clone virtual machines in an efficient disk format. As users interact with instant clone desktops, the clones' OS disks grow and can eventually use almost as much disk space as full-clone desktops. Disk space reclamation reduces the size of the OS disks. Space can be reclaimed while the virtual machines are powered on and users are interacting with their remote desktops. With disk space reclamation, Horizon 8 can maintain instant clones at close to the reduced size they start out with when they are first provisioned.

Space reclamation works differently depending on whether you are using vSAN or non-vSAN datastore, and for the specific version of vSphere/vSAN you are running:

- On vSAN storage, there is no support for space reclamation prior to vSphere/vSAN 6.7U1.
- Starting vSphere/vSAN 6.7U1, space reclamation is supported via vCenter TRIM and UNMAP feature on vSAN datastores
- On non-vSAN storage, prior to vSphere 6.7, Horizon 8 implements a periodic space reclamation operations.
- On non-vSAN storage, from vSphere version 6.7 and later, VMFS-6 supports the Automatic UNMAP feature, which reclaims dead blocks automatically and asynchronously if it is not disabled by the vSphere or vCenter Server administrator. Therefore, you no longer need to enable the manual process on Horizon 8.

Disk space reclamation is not applicable for full clones. For more details, see the *Horizon Installation and Upgrade* document.

Enable Periodic Space Reclamation for vSphere 6.7 and Earlier on Non-vSAN Datastores

This task is relevant if you are using a vSphere version earlier than 6.7 on non-vSAN datastores.

Enabling periodic space reclamation on Horizon 8 is a two-step process.

- You must enable or disable space reclamation globally for each vCenter Server. You can configure space reclamation in Horizon Console by navigating to **Settings > Servers**. You can disable this feature on all desktop pools that are managed by the vCenter Server instance. Disabling the feature at this level overrides the setting at the desktop pool level.
- After you enable space reclamation globally, you can enable or disable space reclamation at individual pool level.

Prerequisites

Verify the following prerequisites for individual desktop pools.

- Verify that the golden image has virtual hardware version 9 or later.
- Verify that the storage for the pool uses SCSI controllers. Disk space reclamation is not supported on virtual machines with IDE controllers.
- Verify that disk space reclamation is enabled globally. This option ensures that the virtual machines in the pool are created in the efficient disk format that is required to reclaim disk space. It is available for instant clones and recommended for longer lived instant clone pools where the desktop is never refreshed on user logout. For other types of instant clones, the benefit from space reclamation may be insignificant.

Procedure

- 1 Complete these steps to set up space reclamation globally.

- a In Horizon Console, navigate to **Settings > Servers**.
- b On the **vCenter Server** tab, click **Add**, and navigate to the **Storage Settings** page.
- c On the **Storage Settings** page, select **Reclaim VM Disk Space**.

This option is selected by default if you perform a fresh installation of Horizon 8. You must select this option if you upgrade to a later release of Horizon 8.

- 2 Complete these steps to set up space reclamation for individual desktop pools.

- a In Horizon Console, navigate to the **Desktop Pool Settings** page of the instant clone pool creation wizard.
- b Select the **Reclaim VM disk space** check box.
- c In the **Initiate reclamation when unused space on VM exceeds** text box, type the minimum amount of unused disk space, in gigabytes, that must accumulate on an instant clone OS disk before ESXi starts reclaiming space on that disk.

For example: 2 GB.

The default value is 1 GB.

What to do next

You can configure blackout days and times during which disk space reclamation and regeneration for View Storage Accelerator do not take place. See [Set Storage Accelerator and Space Reclamation Blackout Times](#).

In Horizon Console, you can select **Inventory > Desktops** and select a machine to display the last time space reclamation occurred and the last amount of space reclaimed on the machine.

You can use the `vmadmin -M` option to initiate disk space reclamation on a particular virtual machine for demonstration or troubleshooting purposes. See the *Horizon Administration* document.

Reclaiming Disk Space for vSphere 6.7 and Later On Non-vSAN Datastores

This topic is relevant if you are using vSphere 6.7 and later, on non-vSAN datastores. In vSphere version 6.7 and later, VMFS-6 supports the Automatic UNMAP feature, which reclaims dead blocks automatically and asynchronously (if it is not disabled by the vSphere or vCenter Server administrator). Therefore, the periodic space reclaim operations by Horizon 8 do not reclaim significant space.

In Horizon Console, the option **Space reclaimed in the latest run over the last 7 days** typically shows a value of 0.00 GB, since this is an indication of the specific Horizon 8 periodic space reclamation operations.

Unless you have disabled automatic UNMAP feature on vSphere or vCenter, no action is needed on Horizon 8 to reclaim space.

Reclaim Disk Space for vSphere 6.7U1 and later on vSAN datastores

This topic is relevant if you are using vSAN datastores. Prior to vSphere with vSAN 6.7U1, there is no space reclamation support. Starting with 6.7U1, vSAN space reclamation is supported with the vCenter UNMAP feature on vSAN datastores. It is disabled by default.

Procedure

- 1 Check that the UNMAP feature is enabled in the ESXi host.

Run the following commands from the command line:

```
esxcfg-advcfg -g /VSAN/GuestUnmap
```

The value of the "GuestUnmap" option is 0.

```
esxcfg-advcfg -g /VSAN/Unmap
```

The value of the "Unmap" option is 1.

- 2 Enable guest UNMAP in all ESXi hosts.

Run the following command:

```
esxcfg-advcfg -s 1 /VSAN/GuestUnmap
```

Then, check the UNMAP feature for the guest operating system. Run the following command:

```
esxcfg-advcfg -g /VSAN/GuestUnmap
```

The value of the GuestUnmap option is 1.

3 Enable the UNMAP feature in vCenter Server.

Run the following RVC command:

```
vsan.unmap_support <cluster> -e
```

Set Storage Accelerator and Space Reclamation Blackout Times

Regenerating digest files for View Storage Accelerator and reclaiming virtual machine disk space can use ESXi resources. To ensure that ESXi resources are dedicated to foreground tasks when necessary, you can prevent the ESXi hosts from performing these operations during specified periods of time on specified days.

For example, you can specify a blackout period during weekday morning hours when users start work, and boot storms and anti-virus scanning I/O storms take place. You can specify different blackout times on different days.

Disk space reclamation and View Storage Accelerator digest file regeneration do not occur during blackout times that you set. You cannot set separate blackout times for each operation.

Horizon 8 allows View Storage Accelerator digest files to be created for new machines during the provisioning stage, even when a blackout time is in effect.

Note The following procedure applies to full-clone desktop pools only.

Prerequisites

- Verify that **Enable View Storage Accelerator**, **Enable space reclamation**, or both features are selected for vCenter Server.
- Verify that **Use View Storage Accelerator**, **Reclaim VM disk space**, or both features are selected for the desktop pool.

Procedure

- 1 On the **Advanced Storage Options** page in the Add Pool wizard, go to **Blackout Times** and click **Add**.
If you are editing an existing pool, click the **Advanced Storage Options** tab.
- 2 Check the blackout days and specify the starting and ending times.
The time selector uses a 24-hour clock. For example, 10:00 is 10:00 a.m., and 22:00 is 10:00 p.m.
- 3 Click **OK**.
- 4 To add another blackout period, click **Add** and specify another period.
- 5 To modify or remove a blackout period, select the period from the Blackout times list and click **Edit** or **Remove**.

Monitoring Virtual Desktops and Desktop Pools

9

In Horizon Administrator, you can monitor the status of virtual desktops, unmanaged machines, or the status of vCenter Server virtual machines in your Horizon 7 deployment.

This chapter includes the following topics:

- [Monitor Virtual-Machine Desktop Status](#)
- [Status of vCenter Server Virtual Machines](#)
- [Recover Instant-Clone Desktops](#)
- [Status of Unmanaged Machines](#)

Monitor Virtual-Machine Desktop Status

You can quickly survey the status of virtual-machine desktops in your Horizon 7 deployment by using the Horizon Administrator dashboard. For example, you can display all disconnected virtual machines or virtual machines that are in maintenance mode.

Prerequisites

Familiarize yourself with the virtual machine states. See [Status of vCenter Server Virtual Machines](#).

Procedure

- 1 In Horizon Administrator, click **Dashboard**.
- 2 In the Machine Status pane, expand a status folder.

Option	Description
Preparing	Lists the machine states while the virtual machine is being provisioned, deleted, or in maintenance mode.
Problem Machines	Lists the machine error states.
Prepared for use	Lists the machine states when the virtual machine is ready for use.

- 3 Locate the machine status and click the hyperlinked number next to it.

Results

The Machines page displays all virtual machines with the selected status.

What to do next

You can click a machine name to see details about the virtual machine or click the Horizon Administrator back arrow to return to the dashboard page.

Status of vCenter Server Virtual Machines

Virtual machines that are managed by vCenter Server can be in various states of operation and availability. In Horizon Administrator, you can track the status of machines in the right-hand column of the Machines page.

[Table 9-1. Status of Virtual Machines That Are Managed by vCenter Server](#) shows the operational state of virtual-machine desktops that are displayed in Horizon Administrator. A desktop can be in only one state at a time.

Table 9-1. Status of Virtual Machines That Are Managed by vCenter Server

Status	Description
Provisioning	The virtual machine is being provisioned.
Customizing	The virtual machine in an automated pool is being customized.
Deleting	The virtual machine is marked for deletion. Horizon 7 will delete the virtual machine soon.
Waiting for Agent	Horizon Connection Server is waiting to establish communication with View Agent or Horizon Agent on a virtual machine in a manual pool.
Maintenance mode	The virtual machine is in maintenance mode. Users cannot log in or use the virtual machine.
Startup	View Agent or Horizon Agent has started on the virtual machine, but other required services such as the display protocol are still starting. For example, View Agent cannot establish an RDP connection with client computers until RDP has finished starting. The agent startup period allows other processes such as protocol services to start up as well.
Agent disabled	<p>This state can occur in two cases. First, in a desktop pool with the Delete or refresh machine on logoff or Delete machine after logoff setting enabled, a desktop session is logged out, but the virtual machine is not yet refreshed or deleted. Second, View Connection Server disables View Agent or Horizon Agent just before sending a request to power off the virtual machine.</p> <p>This state ensures that a new desktop session cannot be started on the virtual machine.</p>
Agent unreachable	Horizon Connection Server cannot establish communication with View Agent or Horizon Agent on a virtual machine.
Invalid IP	The subnet mask registry setting is configured on the virtual machine, and no active network adapters have an IP address within the configured range.
Agent needs reboot	An Horizon 7 component was upgraded, and the virtual machine must be restarted to allow View Agent or Horizon Agent to operate with the upgraded component.

Table 9-1. Status of Virtual Machines That Are Managed by vCenter Server (continued)

Status	Description
Protocol failure	<p>A display protocol did not start before the View Agent or Horizon Agent startup period expired.</p> <p>Note View Administrator can display machines in a Protocol failure state when one protocol failed but other protocols started successfully. For example, the Protocol failure state might be displayed when HTML Access failed but PCoIP and RDP are working. In this case, the machines are available and Horizon Client devices can access them through PCoIP or RDP.</p>
Domain failure	The virtual machine encountered a problem reaching the domain. The domain server was not accessible, or the domain authentication failed.
Already used	<p>In a desktop pool with the Delete or refresh machine on logoff or Delete machine after logoff setting enabled, there is no session on the virtual machine, but the session was not logged off.</p> <p>This condition might occur if a virtual machine shuts down unexpectedly or the user resets the machine during a session. By default, when a virtual machine is in this state, Horizon 7 prevents any other Horizon Client devices from accessing the desktop.</p>
Configuration error	The display protocol such as RDP or PCoIP is not enabled.
Provisioning error	An error occurred during provisioning.
Error	An unknown error occurred in the virtual machine.
Unassigned user connected	<p>A user other than the assigned user is logged in to a virtual machine in a dedicated pool.</p> <p>For example, this state can occur if an administrator starts vSphere Client, opens a console on the virtual machine, and logs in.</p>
Unassigned user disconnected	A user other than the assigned user is logged in and disconnected from a virtual machine in a dedicated-assignment pool.
Unknown	The virtual machine is in an unknown state.
Provisioned	The virtual machine is powered off or suspended.
Available	The virtual machine is powered on and ready for a connection. In a dedicated pool, the virtual machine is assigned to a user and will start when the user logs in.
Connected	The virtual machine is in a session and has a remote connection to the Horizon Client device.
Disconnected	The virtual machine is in a session, but it is disconnected from the Horizon Client device.
In progress	The virtual machine is in a transitional state during a maintenance operation.

While a machine is in a particular state, it can be subject to further conditions. Horizon Administrator displays these conditions as suffixes to the machine state. For example, Horizon Administrator might display the `Customizing (missing)` state.

Table 9-2. [Machine Status Conditions](#) shows these additional conditions.

Table 9-2. Machine Status Conditions

Condition	Description
Missing	The virtual machine is missing in vCenter Server. Typically, the virtual machine was deleted in vCenter Server, but the Horizon LDAP configuration still has a record of the machine.
Task halted	An instant clone task such as push image or a View Composer operation such as refresh, recompose, or rebalance was stopped. The <code>Task halted</code> condition applies to all virtual machines that were selected for the operation, but on which the operation has not yet started. Virtual machines in the pool that are not selected for the operation are not placed in the <code>Task halted</code> condition.

A machine state can be subject to both conditions, (`missing`, `task halted`), if a View Composer task was stopped and the virtual machine is missing in vCenter Server.

Recover Instant-Clone Desktops

When an instant-clone desktop is in an error state, you have the option to recover it. The desktop is recreated from the current base image.

Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**, double-click a pool's ID, and click the **Inventory** tab.
- 2 Select one or more machines and click **Recover**.

Status of Unmanaged Machines

Unmanaged machines, which are physical computers or virtual machines that are not managed by vCenter Server, can be in various states of operation and availability. In View Administrator, you can track the status of unmanaged machines in the right-hand column of the Machines page under the **Others** tab.

[Table 9-3. Status of Unmanaged Machines](#) shows the operational state of unmanaged machines that are displayed in View Administrator. A machine can be in only one state at a time.

Table 9-3. Status of Unmanaged Machines

Status	Description
Startup	View Agent or Horizon Agent has started on the machine, but other required services such as the display protocol are still starting. The agent startup period allows other processes such as protocol services to start up as well.
Validating	This state occurs after View Connection Server first becomes aware of the machine, typically after View Connection Server is started or restarted, and before the first successful communication with View Agent or Horizon Agent on the machine. Typically, this state is transient. It is not the same as the Agent unreachable state, which indicates a communication problem.

Table 9-3. Status of Unmanaged Machines (continued)

Status	Description
Agent disabled	This state can occur if View Connection Server disables View Agent or Horizon Agent. This state ensures that a new desktop session cannot be started on the machine.
Agent unreachable	View Connection Server cannot establish communication with View Agent or Horizon Agent on the machine. The machine might be powered off.
Invalid IP	The subnet mask registry setting is configured on the machine, and no active network adapters have an IP address within the configured range.
Agent needs reboot	A View component was upgraded, and the machine must be restarted to allow View Agent or Horizon Agent to operate with the upgraded component.
Protocol failure	<p>A display protocol did not start before the View Agent or Horizon Agent startup period expired.</p> <p>Note View Administrator can display machines in a Protocol failure state when one protocol failed but other protocols started successfully. For example, the Protocol failure state might be displayed when HTML Access failed but PCoIP and RDP are working. In this case, the machines are available and Horizon Client devices can access them through PCoIP or RDP.</p>
Domain failure	The machine encountered a problem reaching the domain. The domain server was not accessible, or the domain authentication failed.
Configuration error	The display protocol such as RDP or another protocol is not enabled.
Unassigned user connected	<p>A user other than the assigned user is logged in to a machine in a dedicated-assignment pool.</p> <p>For example, this state can occur if an administrator logs in to the unmanaged machine without using Horizon Client.</p>
Unassigned user disconnected	A user other than the assigned user is logged in and disconnected from a machine in a dedicated-assignment pool.
Unknown	The machine is in an unknown state.
Available	The desktop-source computer is powered on and the desktop is ready for a connection. In a dedicated pool, the desktop is assigned to a user. The desktop starts when the user logs in.
Connected	The desktop is in a session and has a remote connection to a Horizon Client device.
Disconnected	The desktop is in a session, but it is disconnected from the Horizon Client device.

Troubleshooting Machines and Desktop Pools

10

You can use a variety of procedures to diagnose and fix problems that you encounter when you create and use machines and desktop pools.

Users might experience difficulty when they use Horizon Client to access desktops and applications. You can use troubleshooting procedures to investigate the causes of such problems and attempt to correct them yourself, or you can obtain assistance from VMware Technical Support.

This chapter includes the following topics:

- [Display Problem Machines in Horizon Console](#)
- [Verify User Assignment for Desktop Pools](#)
- [Restart Desktops and Reset Virtual Machines in Horizon Console](#)
- [Send Messages to Desktop Users in Horizon Console](#)
- [Manage Machines and Policies for Unentitled Users in Horizon Console](#)

Display Problem Machines in Horizon Console

You can display a list of the machines whose operation Horizon 8 has detected as being suspect.

Horizon Console displays machines that exhibit the following problems:

- Are powered on, but which are not responding.
- Remain in the provisioning state for a long time.
- Are ready, but which report that they are not accepting connections.
- Appear to be missing from a vCenter Server.
- Have active logins on the console, logins by users who are not entitled, or logins not made from a Connection Server instance.

Procedure

- 1 In Horizon Console, select **Inventory > Machines**.
- 2 On the **vCenter** tab, click **Problem Machines** from the Machines drop-down menu.

What to do next

The action that you should take depends on the problem that Horizon Console reports for a machine.

- If a machine is powered on, but does not respond, restart its virtual machine. If the machine still does not respond, verify that the version of the Horizon Agent is supported for the machine operating system. You can use the `vdadmin` command with the `-A` option to display the Horizon Agent version. For more information, see the *Horizon Administration* document.
- If a machine remains in the provisioning state for a long time, delete its virtual machine, and clone it again. Verify that there is sufficient disk space to provision the machine.
- If a machine reports that it is ready, but does not accept connections, check the firewall configuration to make sure that the display protocol is not blocked.
- If a machine appears to be missing from a vCenter Server, verify whether its virtual machine is configured on the expected vCenter Server, or if it has been moved to another vCenter Server.
- If a machine has an active login, but this is not on the console, the session must be remote. If you cannot contact the logged-in users, you might need to restart the virtual machine to forcibly log out the users.

Verify User Assignment for Desktop Pools

For dedicated user assignments, you can verify if the user that is assigned to the virtual machine is the user that connects to the virtual desktop or not.

Prerequisites

- Verify that the virtual machine belongs to a dedicated-assignment pool. In Horizon Console, the desktop pool assignment appears in the **User Assignment** column on the **Desktop Pools** page.
- Verify that you have entitled users to the desktop pool.

Procedure

- 1 In Horizon Console, select **Inventory > Machines**.

- 2 On the **vCenter** tab, choose to view the assigned user or connected user.

Option	Description
Assigned User	The Assigned User column displays the user who is assigned to the desktop pool. Note The Assigned User column does not display any user for a floating desktop pool.
Connected User	The Connected User column displays the user who is connected to the virtual machine. Most of the time, the Connected User is the same as the Assigned User when the assigned user is connected to the desktop. At other times, when an administrator is connected to the virtual machine, the Connected User column displays the administrator.

Restart Desktops and Reset Virtual Machines in Horizon Console

You can perform a restart operation on a virtual desktop, which performs a graceful operating system restart of the virtual machine. You can perform a reset operation on a virtual machine without the graceful operating system restart, which performs a hard power-off and power-on of the virtual machine.

Table 10-1. Reset and Restart Functionality

Pool Type	Reset Functionality (Pools, Machines, Sessions, and Horizon Clients)	Restart Functionality (Pools, Machines, Sessions, and Horizon Clients)
Full-clone pool (dedicated pool and floating pool without delete on logOff option enabled)	Reset the VM (Power Off and Power On VM)	Restart the VM (Graceful OS restart)
Instant-clone pool (floating pool)	Power Off VM > Delete VM > Create new VM > Power On	Graceful OS shut down > Delete VM > Create new VM > Power On
Published desktop pools	NA (Not Supported)	NA (Not Supported)

Procedure

- 1 In Horizon Console, select **Inventory > Machines**.
- 2 On the **vCenter** tab, choose to restart a virtual desktop or reset a virtual machine.

Option	Description
Restart Desktop	Restarts the virtual machine with a graceful operating system restart. This action applies only to an automated pool or a manual pool that contains vCenter Server virtual machines.
Reset Virtual Machine	Resets the virtual machine without a graceful operating system restart. This action applies only to an automated pool or a manual pool that contains vCenter Server virtual machines.

- 3 Click **OK**.

Send Messages to Desktop Users in Horizon Console

You might sometimes need to send messages to users who are currently logged into desktops. For example, if you need to perform maintenance on machine, you can ask the users to log out temporarily, or warn them of a future interruption of service. You can send a message to multiple users (there is no set limit on the number of users).

Procedure

- 1 In Horizon Console, click **Inventory > Desktops**.
- 2 Click a pool ID and click the **Sessions** tab.
- 3 Select one or more machines and click **Send Message**.
- 4 Type the message, select the message type, and click **OK**.

A message type can be **Info**, **Warning**, or **Error**.

Results

The message is sent to all selected machines in active sessions.

Manage Machines and Policies for Unentitled Users in Horizon Console

You can display the machines that are allocated to users whose entitlement has been removed, and you can also display the policies that have been applied to unentitled users.

A user who is unentitled might have left the organization permanently, or you might have suspended their account for an extended period of time. These users are assigned a machine but they are no longer entitled to use the machine pool.

You can also use the `vdadmin` command with the `-o` or `-p` option to display unentitled machines and policies. For more information, see the *Horizon Administration* document.

Procedure

- 1 In Horizon Console, select **Inventory > Machines**.
- 2 Select **More Commands > View Unentitled Machines**.
- 3 Remove the machine assignments for unentitled users.
- 4 Select **More Commands > View Unentitled Machines** or **More Commands > View Unentitled Policies** as appropriate.
- 5 Change or remove the policies that are applied to unentitled users.

Setting Up Published Desktops and Applications in Horizon

11

This section describes how to create and deploy pools of desktops and applications that run on Microsoft Remote Desktop Services (RDS) hosts.

It includes information about configuring policies, entitling users and groups, and configuring remote application features.

Introduction to Published Desktops and Applications

12

With Horizon 8, you can create published desktops associated with a farm, which is a group of Windows Remote Desktop Services (RDS) hosts. You can also deliver a published application to many users by creating application pools. The published applications in application pools run on a farm of RDS hosts.

This chapter includes the following topics:

- [Farms, RDS Hosts, and Published Desktops and Applications](#)
- [Configure Horizon 8 for Published Desktops Delivery](#)
- [Configure Horizon 8 for Published Applications Delivery](#)

Farms, RDS Hosts, and Published Desktops and Applications

You can use Microsoft Remote Desktop Services (RDS) to provide desktop sessions on RDS hosts and deliver applications to many users.

RDS Host

RDS hosts are server computers that have Windows Remote Desktop Services and Horizon Agent installed. These servers host applications that users can access remotely.

Farms

Farms are collections of RDS hosts and facilitate the management of those hosts. Farms can have a variable number of RDS hosts and provide a common set of published applications or RDS published desktops to users. When you create an RDS application pool, you must specify a farm. The RDS hosts in the farm provide application sessions to users. See [VMware Configuration Maximums](#) for the maximum number of RDSH host servers supported per farm.

Published Desktops

Published desktops are desktop pools, which provide users with desktop sessions on RDS hosts. Multiple users can have desktop sessions on an RDS host simultaneously. You can create a published desktop pool from a physical system such as an RDS host. Use published desktop pools to provide multiple users with desktop sessions on an RDS host.

Published Applications

Published applications are application pools that run on a farm of RDS hosts. Published applications let you deliver seamless applications to many users, giving them access to published applications that run on servers in a data center instead of on their personal computers or devices.

Configure Horizon 8 for Published Desktops Delivery

You can enable Horizon 8 to deliver published desktops on existing or new RDS hosts.

Procedure

- 1 To configure Horizon 8 to deliver published desktops on existing RDS hosts, complete the following tasks:
 - a Prepare existing RDS hosts for Horizon 8. The RDS hosts can be physical or virtual machines. See [Chapter 13 Setting Up Remote Desktop Services Hosts](#)
 - b Create a manual farm. A manual farm consists of RDS hosts that already exist. You manually add the RDS hosts when you create the farm. See [Create a Manual Farm in Horizon](#).
 - c Create a published desktop pool for the manual farm you created. See [Create a Published Desktop Pool](#).
 - d Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon Administration* document.
- 2 To configure Horizon 8 to deliver published desktops on new RDS hosts, complete the following tasks:
 - a Prepare an RDS host golden image virtual machine. Horizon 8 clones the RDS hosts from this machine as part of the farm creation process. See [Prepare an RDS Host Golden Image Virtual Machine](#).
 - b Create an automated farm. An automated farm consists of RDS hosts that Horizon create as instant-clone virtual machines in vCenter Server. See [Create an Automated Instant-Clone Farm in Horizon](#).
 - c Create a published desktop pool for the automated farm you created. See [Create a Published Desktop Pool](#).
 - d Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon Administration* document.

Configure Horizon 8 for Published Applications Delivery

You can enable Horizon 8 to deliver published applications on existing or new RDS hosts.

Procedure

- 1 To configure Horizon 8 to deliver published applications on existing RDS hosts, complete the following tasks:
 - a Prepare existing RDS hosts for Horizon 8. The RDS hosts can be physical or virtual machines. See [Chapter 13 Setting Up Remote Desktop Services Hosts](#)
 - b Create a manual farm. A manual farm consists of RDS hosts that already exist. You manually add the RDS hosts when you create the farm. See [Create a Manual Farm in Horizon](#).
 - c Create a published application pool for the manual farm you created. See [Create an Application Pool](#).
 - d Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon Administration* document.
- 2 To configure Horizon 8 to deliver published desktops on new RDS hosts, complete the following tasks:
 - a Prepare an RDS host golden image virtual machine. Horizon 8 clones the RDS hosts from this machine as part of the farm creation process. See [Prepare an RDS Host Golden Image Virtual Machine](#).
 - b Create an automated farm. An automated farm consists of RDS hosts that Horizon create as instant-clone virtual machines in vCenter Server. See [Create an Automated Instant-Clone Farm in Horizon](#).
 - c Create a published application pool for the automated farm you created. See [Create an Application Pool](#).
 - d Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon Administration* document.

Setting Up Remote Desktop Services Hosts

13

Microsoft Remote Desktop Services (RDS) hosts provide desktop sessions and applications that users can access from client devices. If you plan to create published desktop pools or application pools, you must first set up RDS hosts.

This chapter includes the following topics:

- [Remote Desktop Services Hosts](#)
- [Prepare Windows Server Operating Systems for Remote Desktop Services \(RDS\) Host Use](#)
- [Install Remote Desktop Services on Windows Server 2012 R2, 2016, or 2019](#)
- [Install Desktop Experience on Windows Server 2012 R2, 2016, or 2019](#)
- [Restrict Users to a Single Session](#)
- [Install Horizon Agent on a Remote Desktop Services Host](#)

Remote Desktop Services Hosts

An RDS host is a server computer that hosts applications and desktop sessions for remote access. An RDS host can be a virtual machine or a physical server.

An RDS host has the Microsoft Remote Desktop Services role, the Microsoft Remote Desktop Session Host service, and Horizon Agent installed. Remote Desktop Services was previously known as Terminal Services. The Remote Desktop Session Host service allows a server to host applications and remote desktop sessions. With Horizon Agent installed on an RDS host, users can connect to applications and desktop sessions by using the display protocol PCoIP or Blast Extreme. Both protocols provide an optimized user experience for the delivery of remote content, including images, audio and video.

To set up an RDS host, you must complete the following tasks:

- 1 Prepare Windows Server operating systems for RDS host use. See [Prepare Windows Server Operating Systems for Remote Desktop Services \(RDS\) Host Use](#).
- 2 Install Remote Desktop Services on Windows Server operating systems. See [Install Remote Desktop Services on Windows Server 2012 R2, 2016, or 2019](#).
- 3 Install desktop experience on Windows Server operating systems. See [Install Desktop Experience on Windows Server 2012 R2, 2016, or 2019](#).

- 4 Restrict users to a single session. See [Restrict Users to a Single Session](#).
- 5 Install Horizon Agent on an RDS host. See [Install Horizon Agent on a Remote Desktop Services Host](#).

Note If smart card authentication is enabled, make sure that the Smart Card service is disabled on RDS hosts. Otherwise, authentication might fail. By default, this service is disabled.

Caution When a user launches an application, for example, a Web browser, it is possible for a user to gain access to the local drives on the RDS host that is hosting the application. This can happen if the application provides functions that cause Windows Explorer to run. Do not create published desktop pools and application pools on the same farm so that desktop sessions are not affected.

Installing Applications

If you plan to create application pools, you must install the applications on the RDS hosts. If you want Horizon 8 to automatically display the list of installed applications, you must install the applications so that they are available to all users from the **Start** menu. You can install an application at any time before you create the application pool. If you plan to manually specify an application, you can install the application at any time, either before or after creating an application pool.

Important When you install an application, you must install it on all the RDS hosts in a farm and in the same location on each RDS host. If you do not, a health warning will appear on the Horizon Console dashboard. In such a situation, if you create an application pool, users might encounter an error when they try to run the application.

When you create an application pool, Horizon 8 automatically displays the applications that are available to all users rather than individual users from the **Start** menu on all of the RDS hosts in a farm. You can choose any applications from that list. In addition, you can manually specify an application that is not available to all users from the **Start** menu. There is no limit on the number of applications that you can install on an RDS host.

Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use

To use a Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 machine as an RDS host, you must perform certain steps before you install Horizon Agent in the virtual machine.

When the Remote Desktop Session Host (RDSH) role is not present, the Horizon Agent installer prompts you to install Horizon Agent in RDS mode or desktop mode. If RDS mode is selected, the installer will install the RDSH role as well as the Desktop Experience role for the supported operating systems and prompt you to reboot the system. At this time the installer has not yet installed Horizon Agent. After rebooting the system you must run the installer again to continue installing Horizon Agent in RDS mode.

When the Remote Desktop Session Host role is present, the Horizon Agent installer does not display these options. The installer treats the Windows Server machine as an RDS host instead of a single-session Horizon desktop and installs Horizon Agent in RDS mode. During this installation, the Horizon Agent installer will not automatically install the Desktop Experience role. If you need the Desktop Experience role, you must install the role manually. See [Install Desktop Experience on Windows Server 2012 R2, 2016, or 2019](#).

Note The Desktop Experience Role is required for the following features:

- HTML Access
- Scanner redirection
- Windows Aero

For Windows Server 2012 R2, if the Horizon Agent installer does not find an RDSH role and you select RDS mode, then the Horizon Agent installer will automatically install the Desktop Experience role with the RDSH role. You do not have to explicitly install the Desktop Experience role. Windows Server 2016 and later do not have a separate installable Desktop Experience role. The Desktop Experience option is available only during the OS installation, so the Horizon Agent installer installs the RDSH role on Windows Server 2016 and later.

Prerequisites

- Verify that the RDS host is part of the Active Directory domain for the Horizon 8 deployment.
- Familiarize yourself with the steps to install the Desktop Experience feature on supported Windows Server operating systems. See [Install Remote Desktop Services on Windows Server 2012 R2, 2016, or 2019](#).
- On Windows Server 2016 machines, familiarize yourself with the steps to configure the Windows Firewall service to restart after failures occur.
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at <http://www.vmware.com/go/downloadview>.

Procedure

- 1 Log in as an administrator.
- 2 To start the Horizon Agent installation program, double-click the installer file.

The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.
- 3 Accept the VMware license terms.

- 4 Select **RDS mode** to install the RDSH role and/or the Desktop Experience role. After it is installed, the installer will prompt you to restart the system. After the system is restarted, launch the installer again to continue installing Horizon Agent in RDS mode.
- 5 On Windows Server 2012 R2 or Windows Server 2016 machines, configure the Windows Firewall service to restart after failures occur.

What to do next

Install Horizon Agent on the remote desktop services host. See [Install Horizon Agent on a Remote Desktop Services Host](#).

Install Remote Desktop Services on Windows Server 2012 R2, 2016, or 2019

Remote Desktop Services is one of the roles that a Windows Server 2012 R2, 2016, or 2019 can have. You must install this role to set up an RDS host.

To use a Windows Server machine as an RDS host, see [Prepare Windows Server Operating Systems for Remote Desktop Services \(RDS\) Host Use](#).

Prerequisites

- Verify that the RDS host is running a supported Windows Server version.
- Verify that the RDS host is part of the Active Directory domain for the Horizon 8 deployment.

Procedure

- 1 Log in to the RDS host as an administrator.
- 2 Start Server Manager.
- 3 Select **Add roles and features**.
- 4 On the Select Installation Type page, select **Role-based or feature-based installation**.
- 5 On the Select Destination Server page, select a server.
- 6 On the Select Server Roles page, select **Remote Desktop Services**.
- 7 On the Select Features page, accept the defaults.
- 8 On the Remote Desktop Services, Role Services page, select the **Remote Desktop Session Host** role and accept the prompts to add in the additional features required to support the Desktop Session Host role.
- 9 Follow the prompts to finish the installation.
- 10 Restart the Windows server.

What to do next

If you plan to use HTML Access or scanner redirection, install the Desktop Experience feature.

Restrict users to a single desktop session. See [Restrict Users to a Single Session](#).

Install Desktop Experience on Windows Server 2012 R2, 2016, or 2019

For published desktops and applications, and for virtual desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

Note A Windows Server 2016 and Windows Server 2019 installation with the Desktop Experience option installs the standard user interface and all tools, including the client experience and the desktop experience features. For Windows Server 2012 RS, the client experience and desktop experience features require a separate installation. For Windows Server 2016 or Windows Server 2019 installation, select **Windows Server 2016** or **Windows Server 2019** or **Windows Server (Server with Desktop Experience)**. If you do not make a choice in the Setup wizard, Windows Server 2016 or Windows Server 2019 is installed as the Server Core installation option. You cannot switch between the installation options. If you install **Windows Server (Server with Desktop Experience)**, and later decide to use **Windows Server 2016** or **Windows Server 2019**, you must perform a fresh installation of Windows Server 2016 or Windows Server 2019.

Procedure

- 1 Log in as an administrator.
- 2 Start Server Manager.
- 3 Select **Add roles and features**.
- 4 On the Select Installation Type page, select **Role-based or feature-based installation**.
- 5 On the Select Destination Server page, select a server.
- 6 On the Select Server Roles page, accept the default selection and click **Next**.
- 7 On the Select Features page, under **User Interfaces and Infrastructure**, select **Desktop Experience**.
- 8 Follow the prompts and finish the installation.

Restrict Users to a Single Session

Horizon 8 supports at most one desktop session and one application session per user on an RDS host. You must configure the RDS host to restrict users to a single session. For Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019, you can restrict users to a single session in a group policy setting.

Procedure

- 1 In the folder `Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections`, Click **Start > Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration**.
- 2 Enable the group policy setting
`Restrict Remote Desktop Services users to a single Remote Desktop Services session`.

What to do next

Install Horizon 8 Agent on the RDS host. See [Install Horizon Agent on a Remote Desktop Services Host](#).

Caution When a user launches an application, for example, a Web browser, it is possible for a user to gain access to the local drives on the RDS host that is hosting the application. This can happen if the application provides functions that cause Windows Explorer to run. Do not create published desktop pools and application pools on the same farm so that desktop sessions are not affected.

Install Horizon Agent on a Remote Desktop Services Host

Horizon Agent communicates with Connection Server and supports the display protocols PCoIP and Blast Extreme. You must install Horizon Agent on an RDS Host.

Prerequisites

- Verify that you have prepared Active Directory. See the *Horizon Installation and Upgrade* document.
- To use a Windows Server virtual machine as an RDS host, see [Prepare Windows Server Operating Systems for Remote Desktop Services \(RDS\) Host Use](#).
- Install the Remote Desktop Services role described in [Install Remote Desktop Services on Windows Server 2012 R2, 2016, or 2019](#).
- Restrict users to a single desktop session. See [Restrict Users to a Single Session](#).
- Familiarize yourself with the Horizon Agent custom setup options. See [Horizon Agent Custom Setup Options for an RDS Host](#).
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at <http://www.vmware.com/go/downloadview>.

Procedure

- 1 Log in as an administrator.

- 2 To start the Horizon Agent installation program, double-click the installer file.

The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number and *xxxxxx* is the build number.

- 3 Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.

You must install all Horizon 8 components with the same IP version.

- 4 Select your custom setup options.

- 5 In the **Server** text box, type the host name or IP address of a Connection Server host.

Horizon Agent installer prompts this step only if you are installing Horizon Agent on an RDS host that will be in a manual farm. During installation, the installer registers the RDS host with this Connection Server instance. After registration, the specified Connection Server instance and any additional instances in the same Connection Server group can communicate with the RDS host.

- 6 Select an authentication method to register the RDS host with the Connection Server instance.

Option	Description
Authenticate as the currently logged in user	The Username and Password text boxes are disabled and you are logged in to the Connection Server instance with your current username and password.
Specify administrator credentials	You must provide the username and password of a Connection Server administrator in the Username and Password text boxes.

The user account must be a domain user with access to View LDAP on the Connection Server instance. A local user does not work.

- 7 Follow the prompts and finish the installation.

What to do next

Create a farm. See [Chapter 14 Creating and Managing Farms](#).

Horizon Agent Custom Setup Options for an RDS Host

When you install Horizon Agent on an RDS host, you can select custom setup options. In addition, Horizon Agent installs certain features automatically on all guest operating systems on which they are supported. These features are not optional.

To change custom setup options after you install the latest Horizon Agent version, see [Modify Installed Components with the Horizon Agent Installer](#).

Table 13-1. Horizon Agent Custom Setup Options for an RDS Host in an IPv4 or IPv6 Environment

Option	Description
USB Redirection	<p>Gives users access to locally connected USB storage devices.</p> <p>This setup option is not selected by default. You must select the option to install it.</p> <p>For information about using USB redirection securely, see the <i>Horizon Security</i> document.</p> <p>For example, you can use group policy settings to disable USB redirection for specific users.</p> <p>For information about using the USB redirection feature, and USB device type limitations, see "Using USB Devices with Remote Desktops and Applications" in the <i>Horizon Remote Desktop Features and GPOs</i> document.</p>
HTML Access	<p>Enables users to connect to published desktops and published applications by using HTML Access. The HTML Access Agent is installed when this setup option is selected. This agent must be installed on RDS hosts to enable users to make connections with HTML Access</p>
3D RDSH	<p>Provides 3D graphics support to applications that run on this RDS host.</p>
Client Drive Redirection	<p>Enables Horizon Client users to share local drives with their published desktops and published applications.</p> <p>After this setup option is installed, no further configuration is required on the RDS host.</p>
Help Desk Plugin for Horizon Agent	<p>You must have a Horizon Enterprise edition license or Horizon Apps Advanced edition license for Horizon to use the Help Desk Tool. This option is installed and enabled by default.</p>
Horizon Monitoring Service Agent	<p>Enables Horizon Monitoring Agent, which is used to provide metrics to Cloud Monitoring Service (CMS).</p>
Scanner Redirection	<p>Redirects scanning devices that are connected to the client system so that they can be used on the published desktop or published application.</p> <p>You must install the Desktop Experience feature in the Windows Server operating system on the RDS hosts to make this option available in the Horizon Agent installer.</p> <p>This setup option is not installed by default on Windows Server guest operating systems. You must select the option to install it.</p>
Serial Port Redirection	<p>Redirects serial COM ports that are connected to the client system so that they can be used on the published desktop or published application.</p> <p>This option is not selected by default. You must select the option to install it.</p>
Instant Clone	<p>Enables the creation of instant-clone virtual machines on a farm of RDS hosts.</p> <p>This setup option is not installed by default on Windows Server guest operating systems. You must select the option to install it.</p>
Horizon Performance Tracker	<p>Monitors the performance of the display protocol and system resource usage. This option is not selected by default. You must select the option to install it. .NET Framework 4.0 or later is required if you install Horizon Performance Tracker.</p>
VMware Integrated Printing	<p>Enables users to print to any printer available on their client machines. Location-based printing is supported.</p> <p>VMware Integrated Printing is supported on the following remote desktops and applications:</p> <ul style="list-style-type: none"> ■ Virtual desktops deployed on Windows Server operating systems or Windows Client operating systems. ■ Published desktops and published applications that are deployed on RDS hosts, where the RDS hosts are virtual machines or physical machines

Table 13-1. Horizon Agent Custom Setup Options for an RDS Host in an IPv4 or IPv6 Environment (continued)

Option	Description
Hybrid Logon	Provides unauthenticated access users access to network resources without the need to enter credentials. This setup option is not installed by default. You must select the option to install it.
Geolocation Redirection	Enables the Geolocation Redirection feature. This option is not selected by default. You must select the option to install it.

Some remote experience features are installed automatically on an RDS host.

Table 13-2. Horizon Agent Features That Are Installed Automatically on an RDS Host

Feature	Description
PCoIP Agent	Enables users to use the PCoIP display protocol to connect to applications and published desktops.
Windows Media Multimedia Redirection (MMR)	Provides multimedia redirection for published desktops. This feature delivers a multimedia stream directly to the client computer, which enables the multimedia stream to be processed on the client hardware instead of on the remote ESXi host.
Unity Touch	Enables tablet and smart phone users to interact with Windows applications that run on the remote desktop. Users can browse, search, and open Windows applications and files, choose favorite applications and files, and switch between running applications without using the Start menu or Taskbar.
PSG Agent	Installs the PCoIP Secure Gateway on RDS hosts to implement the PCoIP display protocol for desktop and application sessions that run on RDS hosts.
VMwareRDS	Provides the VMware implementation of Remote Desktop Services functionality.
HTML5 Multimedia Redirection	Redirects HTML5 multimedia content in a Chrome or Edge browser to the client for performance optimization.
Browser Redirection	Renders a website on the client system instead of the agent system, and displays the website over the remote browser's viewport, when a user uses the Chrome browser in a remote desktop.

In an IPv6 environment, the automatically installed features are PCoIP Agent, PSG Agent, and VMwareRDS.

For additional features that are supported on RDS hosts, see "Feature Support Matrix for Horizon Agent" in the *Horizon Overview and Deployment Planning* document.

Modify Installed Components with the Horizon Agent Installer

Horizon Agent installer allows you to modify already installed components without needing to uninstall and reinstall Horizon Agent.

You can run Horizon Agent installer on a virtual machine where Horizon Agent is already installed to modify, repair, or remove previously installed components. You can also change custom setup options silently using the command line.

Note You cannot switch between installation types, such as managed to unmanaged machines. You also cannot modify Instant Clone Agent (NGVC).

Procedure

- 1 To start the Horizon Agent installation program, double-click the installer file. The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

You can also use the **Uninstall or change a program** in the Control Panel: Click **VMware Horizon Agent**, then click **Change**.

- 2 Select **Modify** from these three options:
 - Modify: add or remove the components that are installed.
 - Repair: fix missing or corrupt files, shortcuts, and registry entries.
 - Remove: remove Horizon Agent from the computer.
- 3 Select or deselect features to add or remove them from the list.
- 4 Follow the prompts to finish the installation.
- 5 Restart the system for the changes to take effect.

What to do next

You can confirm the components that were removed (Absent) or added (Local) in the registry located at `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\Installer\Features_HorizonAgent`.

Silent Installation Properties for Horizon Agent

You can include specific properties when you silently install Horizon Agent from the command line. You must use a `PROPERTY=value` format so that Microsoft Windows Installer (MSI) can interpret the properties and values. A silent upgrade uses the same install commands. You can also modify already installed Horizon Agent components silently.

The following table shows the Horizon Agent silent installation properties that you can use at the command-line.

Table 13-3. MSI Properties for Silently Installing Horizon Agent

MSI Property	Description	Default Value
ENABLE_UNC_REDIRECTION	Specifies whether the UNC Path Redirection feature is installed. A value of 1 installs the feature. You must use group policy settings to configure which UNC's to redirect. See "Configuring UNC Path Redirection" in the <i>Horizon Remote Desktop Features and GPOs</i> document. This MSI property is optional.	0
IGNORE_DOTNET_CHECK	Determines whether the installer checks for a minimum .NET version. By default, when Horizon Performance Tracker is selected, the installer performs a pre-check to confirm that .NET 4.6.2 or later is installed, and stops the install process if it is not. A value of 1 cancels this pre-check. A value of 0 allows the pre-check to proceed.	%ProgramFiles%\VMware\VMware View\Agent
INSTALLDIR	Path and folder in which the Horizon Agent software is installed. For example: <code>INSTALLDIR="D:\abc\my folder"</code> The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path. This MSI property is optional.	
RDP_CHOICE	Determines whether to enable Remote Desktop Protocol (RDP) on the desktop. A value of 1 enables RDP. A value of 0 leaves the RDP setting deactivated. This MSI property is optional.	1
SUPPRESS_RUNONCE_CHECK	Ignores pending Windows Update tasks scheduled at the next operating system reboot in the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce and RunOnceEx keys. Using this flag allows concurrent installation but does not guarantee the installation outcome when the system updates affect the Horizon Agent run-time dependencies. This MSI property is optional.	None
URL_FILTERING_ENABLED	Specifies whether the URL Content Redirection feature is installed. A value of 1 installs the feature. You must use group policy settings to configure which URLs to redirect. See "Configuring URL Content Redirection" in the <i>Horizon Remote Desktop Features and GPOs</i> document. This MSI property is optional.	0
VDM_SKIP_BROKER_REGISTRATION	A value of 1 skips unmanaged desktops.	None

Table 13-3. MSI Properties for Silently Installing Horizon Agent (continued)

MSI Property	Description	Default Value
VDM_VC_MANAGED_AGENT	<p>Determines whether vCenter Server manages the virtual machine on which Horizon Agent is installed.</p> <p>A value of 1 configures the desktop as a vCenter Server-managed virtual machine.</p> <p>A value of 0 configures the desktop as unmanaged by vCenter Server.</p> <p>This MSI property is required.</p> <p>Note The installer repair option is not supported for an unmanaged installation. Repairing such an installation results in an installation of a managed Horizon Agent.</p>	None
VDM_SERVER_NAME	<p>Host name or IP address of the Connection Server instance on which the Horizon Agent installer registers an unmanaged desktop. This property applies to unmanaged desktops only. For example:</p> <p><code>VDM_SERVER_NAME=10.123.01.01</code></p> <p>This MSI property is required for unmanaged desktops.</p> <p>Do not use this MSI property for virtual desktops that are managed by vCenter Server.</p>	None
VDM_SERVER_USERNAME	<p>User name of the administrator on the Connection Server instance. This MSI property applies only to unmanaged desktops. For example:</p> <p><code>VDM_SERVER_USERNAME=domain\username</code></p> <p>This MSI property is required for unmanaged desktops.</p> <p>Do not use this MSI property for virtual desktops managed by vCenter Server.</p>	None
VDM_SERVER_PASSWORD	<p>Connection Server administrator user password. For example:</p> <p><code>VDM_SERVER_PASSWORD=secret</code></p> <p>This MSI property is required for unmanaged desktops.</p> <p>Do not use this MSI property for virtual desktops that are managed by vCenter Server.</p>	None
VDM_IP_PROTOCOL_USAGE	<p>Specifies the IP version that Horizon Agent uses. Valid values are IPv4 and IPv6.</p>	IPv4
VDM_FIPS_ENABLED	<p>Specifies whether to enable or disable FIPS mode. A value of 1 enables FIPS mode. A value of 0 disables FIPS mode. If this property is set to 1 and Windows is not in FIPS mode, the installer will stop.</p>	0
VDM_FORCE_DESKTOP_AGENT	<p>If you install Horizon Agent on a Windows Server machine and configure it as a single-user Horizon desktop rather than as an RDS host, set the value to 1. This requirement applies to machines managed by vCenter Server and unmanaged machines. For non-server Windows guests that host application sessions, set the value to 0.</p> <p>This MSI property is optional.</p>	0

In a silent installation command, you can use the `ADDLOCAL` property to specify options that the Horizon Agent installer configures.

The following table shows the Horizon Agent options that you can enter at the command line. These options have corresponding setup options that you can deselect or select during an interactive installation.

When you do not use the `ADDLOCAL` property at the command line, Horizon Agent installs all of the options that are installed by default during an interactive installation, if they are supported on the guest operating system. When you use `ADDLOCAL=ALL`, Horizon Agent installs all of the following options, both on-by-default and off-by-default, if they are supported on the guest operating system.

For more information, see the `ADDLOCAL` table entry in [Microsoft Windows Installer Command-Line Options](#).

If you use `ADDLOCAL` to specify features individually (you do not specify `ADDLOCAL=ALL`), you must always specify `Core`.

You can modify features by using the `ADDLOCAL` and `REMOVE` MSI properties. Use the following PowerShell command to query the registry of installed components on the system where Horizon Agent is installed for the `ModifyPath` base command line:

```
Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* |
    Select-Object DisplayName, ModifyPath | Where-Object {$_.DisplayName -eq 'VMware
Horizon
    Agent'} | Format-Table -AutoSize
```

The output:

DisplayName	ModifyPath
VMware Horizon Agent	MsiExec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111}

The following example modifies and removes the USB component from an existing installation:
`VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn REMOVE=USB"`

The following example modifies the agent installation by replacing Horizon Performance Tracker with the Horizon Help Desk Tool: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=HelpDesk REMOVE=PerfTracker"`

The following example modifies the agent installation by adding serial port and scanner redirection: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=SerialPortRedirection,ScannerRedirection"`

Table 13-4. Horizon Agent Silent Installation Options and Interactive Custom Setup Options

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When <code>ADDLOCAL</code> Is Not Used
Core	The core Horizon Agent functions. If you specify <code>ADDLOCAL=ALL</code> , the Core features are installed.	Yes
PCoIP	PCoIP Protocol Agent	Yes
USB	USB Redirection	No
NGVC	Instant Clone Agent	No
RTAV	Real-Time Audio-Video	Yes
ClientDriveRedirection	Client Drive Redirection	Yes
SerialPortRedirection	Serial Port Redirection	No
ScannerRedirection	Scanner Redirection	No
GEOREDIR	Geolocation Redirection	No
V4V	Horizon Monitoring Service Agent	Yes
SmartCard	Smartcard This feature is not installed by default in an interactive installation.	No
VmwareAudio	VMware Audio (virtual audio driver)	Yes
VmwareVidd	VMware Indirect Display Driver	<p>Yes</p> <p>Note VmwareVidd is installed and marked as Local in the registry only if:</p> <ul style="list-style-type: none"> ■ Desktop Mode Windows Server is RS4 and above (OS build 17134 - version 1803), or ■ Server is 19H1 and above (OS build 18362 - version 1903) <p>VmwareVidd is installed and set as <code>Absent</code> in the registry in Windows Server 2019 (version 1809) std and datacenter with the RDS role.</p> <p>VmwareVidd will be installed and set as <code>Local</code> in the registry in Windows Server 2022 with the RDS role.</p>
TSMMR	Windows Media Multimedia Redirection (MMR)	Yes

Table 13-4. Horizon Agent Silent Installation Options and Interactive Custom Setup Options (continued)

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When ADDLOCAL Is Not Used
RDP	Enables RDP in the registry if you use the <code>RDP_CHOICE=1</code> property on the command line or select RDP as the default display protocol when you create or edit a desktop pool. This feature is hidden during interactive installations.	Yes
VMWMediaProviderProxy	VMware Virtualization Pack for Skype for Business	No
RDSH3D	3D rendering on RDS hosts	No
BlastUDP	UDP Transport support for Blast	Yes
SdoSensor	SDO Sensor Redirection	No
PerfTracker	Horizon Performance Tracker	No
HelpDesk	Horizon Help Desk Tool	Yes
PrintRedir	VMware Integrated Printing	Yes
PSG	This feature sets a registry entry that tells Connection Server whether Horizon Agent is using IPv4 or IPv6.	Yes

Enable Time Zone Redirection for Published Desktop and Application Sessions

If an RDS host is in one time zone and a user is in another time zone, by default, when the user connects to a published desktop, the desktop displays time that is in the time zone of the RDS host. You can enable the Time Zone Redirection group policy setting to make the published desktop display time in the local time zone. This policy setting applies to application sessions as well.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.
- Verify that the Horizon RDS ADMX files are added to Active Directory. See "Add the Remote Desktop Services ADMX Files to Active Directory" in the *Horizon Remote Desktop Features and GPOs* document.
- Familiarize yourself with the group policy settings. See "RDS Device and Resource Redirection Settings" in the *Horizon Remote Desktop Features and GPOs* document.

Procedure

- 1 On the Active Directory server, open the Group Policy Management Console.

- 2 Expand your domain and **Group Policy Objects**.
- 3 Right-click the GPO that you created for the group policy settings and select **Edit**.
- 4 In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection**.
- 5 Enable the setting **Allow time zone redirection**.

Enable Windows Basic Theme for Applications

If a user has never connected to a desktop on an RDS host, and the user launches an application that is hosted on the RDS host, the Windows basic theme is not applied to the application even if a GPO setting is configured to load the Aero-styled theme. Horizon 8 does not support the Aero-styled theme but supports the Windows basic theme. To make the Windows basic theme apply to the application, you must configure another GPO setting.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.

Procedure

- 1 On the Active Directory server, open the Group Policy Management Console.
- 2 Expand your domain and **Group Policy Objects**.
- 3 Right-click the GPO that you created for the group policy settings and select **Edit**.
- 4 In the Group Policy Management Editor, navigate to **User Configuration > Policies > Administrative Templates > Control Panel > Personalization**.
- 5 Enable the setting **Force a specific visual style file or force Windows classic** and set the Path to Visual Style as `%windir%\resources\Themes\Aero\ aero.msstyles`.

Configure Group Policy to Start Runonce.exe

By default, some applications that rely on the Explorer.exe file may not run in an application session. To avoid this issue, you must configure a GPO setting to start runonce.exe.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.

Procedure

- 1 On the Active Directory server, open the Group Policy Management Console.
- 2 Expand your domain and **Group Policy Objects**.
- 3 Right-click the GPO that you created for the group policy settings and select **Edit**.
- 4 In the Group Policy Management Editor, navigate to **User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff)**.

- 5 Double-click **Logon** and click **Add**.
- 6 In the Script Name box, type **runonce.exe**.
- 7 In the Script Parameters box, type **/AlternateShellStartup**.

RDS Host Performance Options

You can optimize Windows for either foreground programs or background services by setting performance options. By default, Horizon 8 disables certain performance options for RDS hosts for all supported versions of Windows Server.

The following table shows the performance options that are disabled by Horizon 8.

Table 13-5. Performance Options Disabled by Horizon 8

Performance Options Disabled by Horizon 8
Animate windows when minimizing and maximizing
Show shadows under mouse pointer
Show shadows under windows
Use drop shadow for icon labels on the desktop
Show windows contents while dragging

The five performance options that are disabled by Horizon 8 correspond to four Horizon 8 settings in the registry. The following table shows the Horizon 8 settings and their default registry values. The registry values are all located in the registry subkey `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration`. You can re-enable the performance options by setting one or more of the Horizon 8 registry values to **false**.

Table 13-6. Horizon 8 Settings Related to Windows Performance Options

Horizon 8 Setting	Registry Value
Disable cursor shadow	DisableMouseShadows
Disable full window drag	DisableFullWindowDrag
Disable ListView shadow	DisableListViewShadow
Disable Window Animation	DisableWindowAnimation

RDS Host Printing Options

Horizon 8 supports both local printer redirection and native network printers.

Local printer redirection is designed for the following use cases:

- Printers directly connected to USB or serial ports on the client device.

- Specialized printers such as bar code printers and label printers connected to the client.
- Network printers on a remote network that are not addressable from the virtual session.

Network printers are managed using corporate print servers, which allows for greater management and control of printer resources. Native printer drivers for all possible printers need to be installed on the virtual machine or RDSH host. If you consider this challenging, there are third-party options such as advanced versions of ThinPrint that can provide network printing without the need to install additional printer drivers on each virtual machine or RDSH host. The Print and Document Services option included with Microsoft Windows Server is another option for managing your network printers.

When users submit print jobs concurrently from published desktops or applications that are hosted on the same RDS host, the ThinPrint server on the RDS host processes the print requests serially rather than in parallel. This can cause a delay for some users.

Configuring 3D Graphics for RDS Hosts

With 3D graphics configured for RDS hosts, both applications in application pools and applications running on published desktops can display 3D graphics.

Horizon 8 supports several 3D Graphics options for RDS hosts. Note that the options differ based whether your RDS hosts are vSphere virtual machines (automated or manual farm), non-vSphere virtual machines, or physical RDS.

3D graphics is only supported when you use the PCoIP or VMware Blast protocol. Therefore, the farm must use PCoIP or VMware Blast as the default protocol and users must not be allowed to choose the protocol.

For details on 3D graphics support for automated farm of RDS hosts using instant clones, see [Configuring 3D Rendering for Automated Instant Clone Farms](#).

For details on 3D graphics support for manual farm of RDS hosts, see [3D Graphics Options for Manual Farms](#).

Understanding RDS Per-Device Client Access Licensing in Horizon

When a Windows client device connects to a published desktop or application on an RDS host, it receives an RDS Per-Device Client Access License (CAL), if the Per-Device licensing mode is configured on the RDS host.

By default, the CAL is stored only on the client device.

Note Storage of Per-Device CALs is supported only on Windows clients. Windows Zero clients, and non-Windows clients, do not support this feature. For clients that do not support this feature, CALs are stored only on the Connection Server host.

Storing the CAL makes CAL use more efficient in RDS deployments and prevents the following problems.

- If you deploy multiple license servers, and users run multiple sessions from a client device that connects to different RDS hosts that use different license servers, each license server can potentially issue a separate RDS Per-Device CAL to the same client device.

Considerations for Cloud Pod Architecture Environments

A typical Cloud Pod Architecture environment consists of multiple pods. Each pod can point to a different license server, and a single client device can use published desktops and applications on different pods in the pod federation.

If the client device has a license, it always presents that license. If the client device does not present a license, the most up-to-date license that can be found on any pod involved in the published desktop or application launch is used. If a license cannot be found on any pod involved in the launch, the client device's ID is presented to the license server and a license is issued.

Note VMware recommends that you upgrade to the latest Windows client and server software for the best handling of RDS licensing.

Creating and Managing Farms

14

A farm is a group of Windows Remote Desktop Services (RDS) hosts. You can create published desktops associated with a farm. You can also deliver a published application to many users by creating application pools. The published applications in application pools run on a farm of RDS hosts.

Farms simplify the task of managing RDS hosts, published desktops, and applications in an enterprise. You can create manual or automated farms to serve groups of users that vary in size or have different desktop or application requirements.

A manual farm consists of RDS hosts that already exist. The RDS hosts can be physical or virtual machines. You manually add the RDS hosts when you create the farm.

Connection Server creates the instant clone virtual machines based on the parameters that you specify when you create the farm. Instant clones share a virtual disk of an internal parentVM and therefore consume less storage than full virtual machines. In addition, instant clones share the memory of a parentVM and are created using the vmFork technology.

Although helpful in speeding up the provisioning speed, the use of parentVM does increase the memory requirement across the cluster. In some cases when the benefit of having more memory outweighs the increase in provisioning speed, Horizon automatically chooses to provision instant clones directly from replicaVM, without creating any parentVM. This feature is called Smart Provisioning. A single instant clone farm can have both instant clones that are created with parentVMs or without parentVMs.

When you create an application pool or a published desktop pool, you must specify one and only one farm. The RDS hosts in a farm can host published desktops, applications, or both. A farm can support at most one published desktop pool, but it can support multiple application pools. A farm can support both types of pools simultaneously.

For more information on farms, see the *Horizon Administration* document.

This chapter includes the following topics:

- [Creating an Automated Instant-Clone Farm](#)
- [Creating a Manual Farm](#)
- [3D Graphics Options for Manual Farms](#)
- [Managing Farms](#)

Creating an Automated Instant-Clone Farm

An automated farm consists of RDS hosts that are instant-clone virtual machines in vCenter Server. There is no other cloning technology available for automated farms.

An automated instant-clone farm created from a golden image using the vmFork technology (called instant clone API) in vCenter Server. Instant clone technology replaces View Composer linked clone as the process for creating automated farms in Horizon 8. In addition to using the instant clone API from vCenter Server, Horizon 8 also creates several types of internal VMs (Internal Template, Replica VM, and ParentVM) in order to manage these clones in a more scalable way.

Although helpful in speeding up the provisioning speed, the use of parentVM does increase the memory requirement across the cluster. In some cases when the benefit of having more memory outweighs the increase in provisioning speed, Horizon 8 automatically chooses to provision instant clones directly from replicaVM, without creating any parentVM. This feature is called Smart Provisioning. A single instant clone farm can have both instant clones that are created with parentVMs or without parentVMs.

When parentVM is used, instant clones share the virtual disk of the parentVM and therefore consume less storage than full VMs. In addition, instant clones share the memory of the parentVM when they are first created, which contributes to fast provisioning. Once the instant clone VM is provisioned and the machine starts to be used, additional memory is utilized.

An instant-clone desktop farm has the following benefits:

- The provisioning of instant clones is fast, with or without using parentVM.
- Instant clones are always created in a powered-on state, ready for use.
- You can patch a farm of instant clones in a rolling process with zero downtime.

Connection Server creates the instant-clone virtual machines based on the parameters that you specify when you create the farm. Instant clones share a virtual disk of a parentVM and therefore consume less storage than full virtual machines. In addition, instant clones share the memory of a parentVM and are created using the vmFork technology.

Before you create an automated instant-clone farm, you must prepare an RDS host golden image virtual machine. See [Prepare an RDS Host Golden Image Virtual Machine](#).

Instant Clone Image Publishing and Creation Workflow for Farms

Publishing an image is a process by which internal VMs needed for instant cloning are created from a golden image and its snapshot. This process only happens once per image and may take some time.

Horizon 8 performs the following steps to create a pool of instant clones:

- 1 Horizon 8 publishes the image that you select. In vCenter Server, four folders (`ClonePrepInternalTemplateFolder`, `ClonePrepParentVmFolder`,

`ClonePrepReplicaVmFolder`, and `ClonePrepResyncVmFolder`) are created if they do not exist, and some internal VMs that are required for cloning are created. In Horizon Console, you can see the progress of this operation on the **Summary** tab of the desktop pool. During publishing, the Pending Image pane shows the name and state of the image.

Note Do not tamper with the four folders or the internal VMs that they contain. Otherwise, errors might occur. The internal VMs are removed when they are no longer needed. Normally the VMs are removed within 5 minutes of pool deletion or a push-image operation. However, sometimes the removal can take up to 30 minutes. If there are no internal VMs in all four folders, these folders are unprotected and you can delete these folders.

- 2 After the image is published, Horizon 8 creates the instant clones.. This process is fast. During this process, the Current Image pane in Horizon Console shows the name and state of the image.

After the farm is created, you can change the image through the push-image operation. As with the creation of a farm, the new image is first published. Then the clones are recreated.

When an instant clone pool farm is created, Horizon 8 spreads the pool across datastores automatically in a balanced way. If you edit a farm to add or remove datastores, rebalancing of the cloned VMs happens automatically when a new clone is created.

Preparing a Golden Image Virtual Machine for an Automated Farm

To create an automated farm, you must first prepare a golden image virtual machine. Connection Server uses this golden image virtual machine to create instant-clone virtual machines, which are the RDS hosts in the farm.

- [Prepare an RDS Host Golden Image Virtual Machine](#)

Connection Server requires a golden image virtual machine from which you generate a base image for creating instant clones.

- [Disable Windows Hibernation in the Golden Image](#)

The Windows hibernation feature creates a hidden system file, `Hiberfil.sys` and uses this file to store information that is needed for hybrid sleep. Disabling hibernation reduces the size of an instant clone's virtual disk.

Prepare an RDS Host Golden Image Virtual Machine

Connection Server requires a golden image virtual machine from which you generate a base image for creating instant clones.

Prerequisites

- Verify that an RDS host virtual machine is set up. See [Chapter 13 Setting Up Remote Desktop Services Hosts](#). To set up the RDS host, be sure not to use a virtual machine that was previously registered to Connection Server.

- To create an automated instant-clone farm, you must select the **Instant Clone** option when you install Horizon Agent on the golden image virtual machine. See [Install Horizon Agent on a Remote Desktop Services Host](#).
- Verify that the virtual switch that the instant-clone VMs connect to has enough ports to support the expected number of VMs. Each network card on a VM requires one port.
- Verify that you added an instant-clone domain administrator in Horizon Console. See *Add an Instant-Clone DomainAdministrator* in the *Horizon Installation and Upgrade* document.
- To deploy Windows machines, configure a volume license key and activate the golden image virtual machine's operating system with volume activation.
- Familiarize yourself with the procedure for disabling searching Windows Update for device drivers. See the Microsoft Technet article, "Disable Searching Windows Update for Device Drivers" at [http://technet.microsoft.com/en-us/library/cc730606\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx).
- To implement the RDS host load balancing feature, modify the RDS host golden image virtual machine.

Procedure

- ◆ Verify that the system disk contains a single volume.
- ◆ Verify that the virtual machine does not contain an independent disk.
An independent disk is excluded when you take a snapshot of the virtual machine.
- ◆ Before you take a snapshot of the golden image virtual machine, disable searching Windows Update for device drivers.
- ◆ In vSphere Client, disable the vApp Options setting on the golden image virtual machine.
- ◆ On Windows Server 2012 R2 machines, disable the scheduled maintenance task that recovers disk space by removing unused features.

For example: `Schtasks.exe /change /disable /tn
"Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup"`

What to do next

Use vSphere Client to take a snapshot of the golden image virtual machine in its powered-down state.

Important Before you take a snapshot, completely shut down the golden image virtual machine by using the **Shut Down** command in the guest operating system.

Disable Windows Hibernation in the Golden Image

The Windows hibernation feature creates a hidden system file, `Hiberfil.sys` and uses this file to store information that is needed for hybrid sleep. Disabling hibernation reduces the size of an instant clone's virtual disk.

Caution When you make hibernation unavailable, hybrid sleep does not work. Users can lose data if a power loss occurs.

Procedure

- 1 In vSphere Client, select the golden image virtual machine and select **Open Console**.
- 2 Log in as an administrator.
- 3 Disable the hibernation option.
 - a Click **Start** and type `cmd` in the **Start Search** box.
 - b In the search results list, right-click **Command Prompt** and click **Run as Administrator**.
 - c At the **User Account Control** prompt, click **Continue**.
 - d At the command prompt, type `powercfg.exe /hibernate off` and press Enter.
 - e Type `exit` and press Enter.

Worksheet for Creating an Automated Instant-Clone Farm in Horizon

When you create an automated instant-clone farm, you can configure certain settings.

Table 14-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm.	
Description	Description of this farm.	
Access group	Select an access group for the farm, or leave the farm in the default root access group.	
Default display protocol	Select VMware Blast , PCoIP or Microsoft RDP . Microsoft RDP applies to desktop pools only. The display protocol for application pools is always VMware Blast or PCoIP . If you select Microsoft RDP and you plan to use this farm to host application pools, you must set Allow users to choose protocol to Yes . The default is PCoIP .	
Allow users to choose protocol	Select Yes or No . This setting applies to published desktop pools only. If you select Yes , users can choose the display protocol when they connect to a published desktop from Horizon Client. The default is Yes .	
3D Renderer	Select 3D graphics rendering for desktops. NVIDIA GRID vGPU is the only 3D rendering option offered for automated farm of instant clone RDS hosts.	

Table 14-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Pre-launch session timeout (applications only)	<p>Determines the amount of time that an application configured for pre-launch is kept open. The default is 10 minutes.</p> <p>If the end-user does not start any application in Horizon Client, the application session is disconnected if the idle session times out or if pre-launch session times out.</p> <p>If you want to end the pre-launch session after timeout, you must set the Log off disconnected session option to Immediate.</p>	
Empty session timeout (applications only)	<p>Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log out from empty application sessions. Select Never, Immediate, or set the number of minutes as the timeout value. The default is After 1 minute. If you select Immediate, the session logs you out or disconnects within 30 seconds.</p> <p>You can further reduce the time the session logs out or disconnects by editing a registry key on the RDS Host on which Horizon Agent is installed. Navigate to <code>HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params</code> and set a value for <code>WindowCheckInterval</code>. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session logout to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session logout to 5 seconds.</p>	
When timeout occurs	<p>Determines whether an empty application session is disconnected or logged off after the Empty session timeout limit is reached. Select Disconnect or Log off. A session that is logged off frees up resources, but opening an application takes longer. The default is Disconnect.</p>	
Log off disconnected sessions	<p>Determines when a disconnected session is logged off. This setting applies to both desktop and application sessions. Select Never, Immediate, or After ... minutes. Use caution when you select Immediate or After ... minutes. When a disconnected session is logged off, the session is lost. The default is Never.</p>	

Table 14-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Bypass Session Timeout	<p>Enable this setting to allow application sessions to run forever.</p> <p>Application sessions that run forever are supported on Windows and Linux clients.</p> <p>This setting is not available for application pools in a cloud pod architecture environment.</p> <p>Application sessions that run forever are not supported for unauthenticated users.</p> <p>Do not enable this setting if the max session timeout value is set to Never.</p> <p>When you restart Connection Server, existing forever running application sessions no longer run indefinitely.</p>	
Allow Session Collaboration	Select Enabled to allow users of desktop pools based on this farm to invite other users to join their remote desktop sessions. Session owners and session collaborators must use the VMware Blast display protocol.	
Max sessions per RDS Host	<p>Determines the maximum number of sessions that an RDS host can support. Select Unlimited or No More Than</p> <p>The default is Unlimited.</p>	
Load Balancing	See Load Balancing Settings for the list of settings.	
Enable provisioning	Select this checkbox to enable provisioning after you finish this wizard. This box is checked by default.	
Stop provisioning on error	Select this checkbox to stop provisioning when a provisioning error occurs. This box is checked by default.	
Naming pattern	<p>Specify a prefix or a name format. Horizon 8 will append or insert an automatically generated number starting with 1 to form the machine name. If you want the number at the end, simply specify a prefix. Otherwise, specify {n} anywhere in a character string and {n} will be replaced by the number. You can also specify {n:fixed=<number of digits>}, where fixed=<number of digits> indicates the number of digits to be used for the number. For example, specify vm-{n:fixed=3}-sales and the machine names will be vm-001-sales, vm-002-sales, and so on.</p> <p>Note Each machine name, including the automatically generated number, has a 15-character limit.</p>	
Max number of machines	The number of machines to be provisioned.	

Table 14-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Minimum number of ready (provisioned) machines during Instant Clone maintenance operations	This setting lets you keep the specified number of machines available to accept connection requests while Connection Server performs maintenance operations on the machines in the farm. This setting is not honored if you schedule immediate maintenance.	
Use VMware vSAN	Specify whether to use VMware vSAN, if available. vSAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of ESXi hosts.	
Select separate datastores for replica and OS disks	(Available only if you do not use vSAN) You can place replica and OS disks on different datastores for performance or other reasons. If you select this option, you can select the options to select one or more instant-clone datastores or replica disk datastores.	
Golden image	Select a golden image virtual machine from the list.	
Snapshot	Select the snapshot of the golden image virtual machine to use as the base image for the farm. Do not delete the snapshot and golden image virtual machine from vCenter Server, unless no instant clones in the farm use the default image, and no more instant clones will be created from this default image. The system requires the golden image virtual machine and snapshot to provision new instant clones in the farm, according to farm policies. The golden image virtual machine and snapshot are also required for Connection Server maintenance operations.	
VM folder location	Select the folder in vCenter Server in which the farm resides.	
Cluster	Select the ESXi host or cluster on which the desktop virtual machines run. For the maximum limit on the cluster, see the KB article on Sizing Limits and Recommendations .	
Resource pool	Select the vCenter Server resource pool in which the farm resides.	

Table 14-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Datastores	<p>Select one or more datastores on which to store the farm.</p> <p>A table on the Select Instant Clone Datastores page of the Add Farm wizard provides high-level guidelines for estimating the farm's storage requirements. These guidelines can help you determine which datastores are large enough to store the instant-clones. The Storage Overcommit value is always set to Unbounded and is not configurable.</p> <hr/> <p>Note If you use vSAN, there is only one datastore.</p>	
Replica disk datastores	<p>Select one or more replica disk datastores on which to store the instant-clones. This option appears if you select separate datastores for replica and OS disks.</p> <p>A table on the Select Replica Disk Datastores page of the Add Farm wizard provides high-level guidelines for estimate the farm's storage requirements. These guidelines can help you determine which replica disk datastores are enough to store the instant-clones.</p>	

Table 14-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Networks	<p>Note If the selected snapshot has multiple network adapters, the wizard shows a selection grid for each adapter. To change the number of adapters, make the change on the Instant Clone golden image, take a new snapshot, and select that snapshot to use for the new pool.</p> <p>If the selected snapshot has multiple network adapters, the wizard selects the network type of Adapter 1 as the network type. To change the network type for the snapshot, edit the network type on the Instant Clone golden image, take a new snapshot, and select that snapshot to use for the new pool.</p> <p>Select the networks to use for the automated instant-clone farm. You can select multiple vLAN networks to create a larger instant-clone desktop farm. The default setting uses the network from the snapshot selected.</p> <p>The Select Networks wizard provides a list of networks based on the snapshot's preferred network adapter (Network Adapter 1 while the snapshot was taken) network type: DVS, NSX-V, NSX-T (Opaque Network), NSX-T (CVDS), and Standard. To use multiple networks, you must unselect Use network from golden image (which selects the network and network type from the selected snapshot) and then select the networks to use with the instant-clone farm. The Show all networks for each network adapter switch shows or hides (greys out) incompatible networks for all network types. By default, only compatible networks are shown. If you select an incompatible network, such as vmcNetworks, you see this error message: This network belongs to VMC internal network.</p> <p>Note You can select any one available Standard Network per network adapter for Instant Clone farms. It is not supported to use more than one Standard Network per network adapter.</p> <p>The wizard also provides the list of ports and port bindings that are available to use: static (early binding) and ephemeral.</p> <p>All selected NSX-T or VDS network segments must be the same size, such as all /24 networks. Unequal sized segments can result in provisioning errors.</p> <p>The wizard displays error messages for the following incompatible networks:</p> <ul style="list-style-type: none"> ■ vmcNetworks. This network belongs to VMC internal network ■ dvsUplinkPort. Cannot use network because it does not meet the naming standards for a virtual switch uplink port. 	

Table 14-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
	<ul style="list-style-type: none"> ■ notConfiguredOnAllHosts. Cannot use network because it is not configured on all hosts in the cluster. ■ This network is on <network type 1>. Only networks on <network type 2> can be selected.. Cannot use network because it is not the same type as the network in the selected snapshot. 	
CPU	<p>Update the default CPU if desired.</p> <ul style="list-style-type: none"> ■ The default value is taken from the selected snapshot in vCenter. ■ You can update this value again in the future using the Push Image function. <p>Note The CPU value must be a multiple of the Cores per Socket value.</p>	
RAM	<p>Update the default RAM if desired.</p> <ul style="list-style-type: none"> ■ The default value is taken from the selected snapshot in vCenter. ■ You can update this value again in the future using the Push Image function. <p>Note If you set a memory reservation on the Golden Image VM through vSphere Client, use the "Reserve all guest memory (All locked)" option to ensure the correct behavior when creating pools with different amounts of RAM than the Golden Image.</p>	
Cores per Socket	<p>Update the default Cores per Socket if desired.</p> <ul style="list-style-type: none"> ■ The default value is taken from the selected snapshot in vCenter. ■ You can update this value again in the future using the Push Image function. 	
Domain	<p>Select the Active Directory domain and user name.</p> <p>Connection Server requires certain user privileges to farm. The domain and user account are used by ClonePrep to customize the instant-clone machines.</p> <p>You specify this user when you configure Connection Server settings for vCenter Server. You can specify multiple domains and users when you configure Connection Server settings. When you use the Add Farm wizard to create a farm, you must select one domain and user from the list.</p>	
AD container	<p>Provide the Active Directory container relative distinguished name.</p> <p>For example: CN=Computers</p> <p>When you run the Add Farm wizard, you can browse your Active Directory tree for the container. You can cut, copy, or paste in the container name.</p>	

Table 14-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Allow reuse of pre-existing computer accounts	<p>Select this option to use existing computer accounts in Active Directory when the virtual machine names of new instant clones match the existing computer account names.</p> <p>When an instant clone is created, if an existing AD computer account name matches the instant-clone virtual machine name, Horizon 8 uses the existing computer account. Otherwise, a new computer account is created.</p> <p>The existing computer accounts must be located in the Active Directory container that you specify with the AD container setting.</p> <p>When this option is disabled, a new AD computer account is created when Horizon 8 creates an instant clone. This option is disabled by default.</p>	
Image Publish Computer Account	<p>Publishing instant-clones requires an additional computer account in the same AD domain as the clones. If you want to use pre-created computer accounts instead of auto-created computer accounts, you must also create the additional computer account and specify its name here.</p> <p>Then you do not need to delegate Create and Delete of computer objects to the provisioning account.</p>	

Table 14-1. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Use ClonePrep or a customization specification (Sysprep)	<p>Choose whether to use ClonePrep or select a customization specification (Sysprep) to configure licensing, domain attachment, DHCP settings, and other properties on the machines.</p> <ul style="list-style-type: none"> ■ Power-off script name. Name of the customization script that ClonePrep runs on instant-clone machines before they are powered off. Provide the path to the script on the golden image virtual machine. ■ Power-off script parameters. Provide parameters that ClonePrep can use to run a customization script on instant-clone machines before they are powered off. For example, use p1. ■ Post-synchronization script name. Name of the customization script that ClonePrep runs on instant-clone machines after they are created or an image has been pushed to them. Provide the path to the script on the golden image virtual machine. ■ Post-synchronization script parameters. Provide parameters for the script that ClonePrep runs on instant-clone machines after they are created or an image has been pushed to them. For example, use p2. <p>After you use ClonePrep or Sysprep when you create a farm, you cannot switch to the other customization method later on, when you create or recompose machines in the farm.</p> <p>After you use ClonePrep or Sysprep when you create a farm, you can edit the customization type or spec name. Changes to the customization spec are not reflected on the farm until a new push image is scheduled, and the currently published image continues to use the old spec even if it has been edited or deleted. If push image fails, the farm continues using the old unedited spec. However, the farm settings continue to point to the new spec name if it has been changed.</p> <p>For more information about the differences between ClonePrep and Sysprep, see Choosing ClonePrep or Sysprep for Customizing Your Virtual Desktops.</p>	
Ready to Complete	Review the settings for the automated instant-clone farm.	

Create an Automated Instant-Clone Farm in Horizon

You create an automated instant-clone farm as part of the process to give users access to published applications or published desktops.

Prerequisites

- Verify that Connection Server is installed. See the *Horizon Installation and Upgrade* document.
- Verify that Connection Server settings for vCenter Server are configured in Horizon Console. See the *Horizon Administration* document.
- Verify that you have a sufficient number of ports on the ESXi virtual switch that is used for the virtual machines that are used as remote desktops. The default value might not be sufficient if you create large desktop pools.
- Verify that you prepared a golden image virtual machine. Horizon Agent must be installed on the golden image virtual machine. See [Preparing a Golden Image Virtual Machine for an Automated Farm](#).
- Take a snapshot of the golden image virtual machine in vCenter Server. You must shut down the golden image virtual machine before you take the snapshot. Connection Server uses the snapshot as the base image from which the clones are created.
- Gather the configuration information you must provide to create the farm. See [Worksheet for Creating an Automated Instant-Clone Farm in Horizon](#).

Procedure

- 1 In Horizon Console, select **Inventory > Farms**.
- 2 Click **Add**.
- 3 Select **Automated Farm**.
- 4 Select **Instant clone**.
- 5 Follow the prompts in the wizard to create the farm.

Use the configuration information that you gathered in the worksheet. You can go directly back to any wizard page that you completed by clicking the page name in the navigation panel.

Note If you are a VMware Carbon Black customer and select a golden image configured with Carbon Black for the new farm, then the screen displays information from the Carbon Black Scan for each snapshot listed.

- If you select the Show All Images check box, the list might include snapshots that are not compatible and cannot be selected.
 - If no value appears in the Carbon Black Scan (% Complete) column, that indicates that the Carbon Black sensor was not enabled in the Instant Clone golden image when the snapshot was taken. For more information, see the [VMware Carbon Black Cloud Documentation](#).
-

What to do next

Create a published application pool or a published desktop pool. See [Create an Application Pool](#) or [Create a Published Desktop Pool](#).

Configuring 3D Rendering for Automated Instant Clone Farms

When you create or edit a farm of instant clone RDS machines, you can configure 3D graphics rendering for your farm. Instant clone farms support NVIDIA GRID vGPU for 3D rendering.

Horizon 8 does not directly control settings for 3D rendering of an instant-clone farm as it does with full-clone virtual machines. You need to configure 3D settings in the ESXi hosts, and then in your golden image using the vSphere Client. Instant-clone virtual machines will inherit those settings from the golden image. Horizon Console will display some of the settings you configured, but you cannot edit or interact with those settings.

The ESXi host assigns GPU hardware resources to virtual machines on a first-come, first-served basis as virtual machines are created. By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is the **best performance** mode. If you would rather have the ESXi host assign virtual machines to the same physical GPU until the maximum number of virtual machines is reached before placing virtual machines on the next physical GPU, you can use the **GPU consolidation** mode. You can configure this mode in vCenter Server for each ESXi host that has vGPU installed. For more information, see the VMware Knowledge Base (KB) article <https://kb.vmware.com/s/article/55049>.

If you are only using a single vGPU profile per vSphere cluster, set the GPU assignment policy for all GPU hosts within the cluster to the **best performance** mode in order to maximize performance. In this case, you can also have instant-clone pools and full-clone pools that use the same vGPU profile in the same vSphere cluster.

You can have a cluster with some GPU enabled hosts and some non-GPU enabled hosts.

NVIDIA GRID vGPU has these potential constraints:

- RDP is not supported.
- The virtual machines must be hardware version 11 or later.
- vMotion of a VM between vGPU-enabled hosts is supported starting with vSphere 6.7. You cannot use vSphere Distributed Resource Scheduler (DRS) with vGPU.
- Horizon 8 does support creating a vGPU instant-clone farm using a cluster with some vGPU enabled hosts and non-vGPU enabled hosts, and will just ignore the non-vGPU enabled hosts when creating the farm. You can not use vMotion to move an instant-clone from a GPU-enabled ESXi host to an ESXi host that does not have GPU hardware configured.

To enable an instant-clone farm to use NVIDIA GRID vGPU:

Procedure

- 1 Install NVIDIA GRID vGPU in the physical ESXi hosts.
- 2 In vCenter Server hardware graphics configuration, select the Host Graphics tab, and in **Edit Host Graphics Settings**, select **Shared Direct**.

ESXi host uses the NVIDIA GRID card for vGPU.

- 3 Prepare a golden image with NVIDIA GRID vGPU configured, including selecting the vGPU profile you want to use.
- 4 Take a snapshot of the golden image.
- 5 In Horizon Console, when you create an instant-clone farm, select this golden image and snapshot.

Results

Horizon 8 automatically displays **NVIDIA GRID vGPU** in the 3D Render field. Horizon 8 also displays the vGPU profile you chose in the golden image. Instant clones inherit the settings configured in the vSphere Client for the golden image.

The vGPU profile cannot be edited from Horizon Console during the instant-clone farm creation process. To edit the vGPU profile for a farm once the farm has been created, you can create a new image with the updated vGPU profile, take a snapshot, and then do a push-image operation.

Creating a Manual Farm

A manual farm consists of RDS hosts that already exist. The RDS hosts can be physical, vSphere virtual machines (excluding instant clones), or non-vSphere virtual machines. You manually add the RDS hosts when you create the farm.

Before you create a manual farm, you must prepare existing RDS hosts for Horizon 8. See [Chapter 13 Setting Up Remote Desktop Services Hosts](#).

Worksheet for Creating a Manual Farm in Horizon

When you create a manual farm, you can configure certain farm settings.

Table 14-2. Worksheet: Configuration Settings for Creating a Manual Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm.	
Description	Description of this farm.	
Access group	Select an access group for the farm, or leave the farm in the default root access group.	
Default display protocol	Select VMware Blast , PCoIP or Microsoft RDP . Microsoft RDP applies to desktop pools only. The display protocol for application pools is always VMware Blast or PCoIP . If you select Microsoft RDP and you plan to use this farm to host application pools, you must set Allow users to choose protocol to Yes . The default is PCoIP .	
Allow users to choose protocol	Select Yes or No . This setting applies to published desktop pools only. If you select Yes , users can choose the display protocol when they connect to a published desktop from Horizon Client. The default is Yes .	

Table 14-2. Worksheet: Configuration Settings for Creating a Manual Farm (continued)

Setting	Description	Fill in Your Value Here
Pre-launch session timeout (applications only)	<p>Determines the amount of time that an application configured for pre-launch is kept open. The default is 10 minutes.</p> <p>If the end-user does not start any application in Horizon Client, the application session is disconnected if the idle session times out or if pre-launch session times out.</p> <p>If you want to end the pre-launch session after timeout, you must set the Log off disconnected session option to Immediate.</p>	
Empty session timeout (applications only)	<p>Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log out from empty application sessions. Select Never, Immediate, or set the number of minutes as the timeout value. The default is After 1 minute. If you select Immediate, the session logs you out or disconnects within 30 seconds.</p> <p>You can further reduce the time the session logs out or disconnects by editing a registry key on the RDS Host on which Horizon Agent is installed. Navigate to <code>HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params</code> and set a value for <code>WindowCheckInterval</code>. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session logout to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session logout to 5 seconds.</p>	
When timeout occurs	Determines whether an empty application session is disconnected or logged off after the Empty session timeout limit is reached. Select Disconnect or Log off . A session that is logged off frees up resources, but opening an application takes longer. The default is Disconnect .	
Log off disconnected sessions	Determines when a disconnected session is logged off. This setting applies to both desktop and application sessions. Select Never , Immediate , or After ... minutes . Use caution when you select Immediate or After ... minutes . When a disconnected session is logged off, the session is lost. The default is Never .	
Bypass Session Timeout	<p>Enable this setting to allow application sessions to run forever. Application sessions that run forever are supported on Windows and Linux clients.</p> <p>This setting is not available for application pools in a cloud pod architecture environment.</p> <p>Application sessions that run forever are not supported for unauthenticated users.</p> <p>Do not enable this setting if the max session timeout value is set to Never.</p> <p>When you restart Connection Server, existing forever running application sessions no longer run indefinitely.</p>	

Table 14-2. Worksheet: Configuration Settings for Creating a Manual Farm (continued)

Setting	Description	Fill in Your Value Here
Allow Session Collaboration	Select Enabled to allow users of desktop pools based on this farm to invite other users to join their remote desktop sessions. Session owners and collaborators must use the VMware Blast protocol.	
Use custom script	Select this setting to use a custom script for load balancing. If this setting is enabled, Horizon 8 does not consider other load balancing settings and reads the <code>CustomLoadValue</code> registry key in the following location to get the server load index: <code>HKLM\Software\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue</code> . See, Writing a Load Balancing Script for an RDS Host .	
Include session count	Select this setting to include the session count on the RDS host for load balancing. If none of the settings are selected for load balancing and if the custom script setting is not selected, Horizon 8 uses the session count by default. Disable this setting if you do not need to consider the session count for load balancing.	
Select RDS Hosts	Select the RDS host from the list.	
CPU usage threshold	Threshold value for the CPU usage in percentage. Horizon 8 uses the configured CPU threshold to calculate the CPU load index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.	
Memory usage threshold	Threshold value for the memory in percentage. Horizon 8 uses the configured memory threshold to calculate the Memory Load Index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.	
Disk queue length threshold	Threshold of the average number of both read and write requests that were queued for the selected disk during the sample interval. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing.	
Disk read latency threshold	Threshold of the average time of read of data from the disk in milliseconds. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.	
Disk write latency threshold	Threshold of the average time of write of data to the disk in milliseconds. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.	

Create a Manual Farm in Horizon

Create a manual farm as part of the process to give users access to published applications or desktops.

Prerequisites

- Set up the RDS hosts that belong to the farm. See [Chapter 13 Setting Up Remote Desktop Services Hosts](#).
- Verify that all the RDS hosts have the Available status. In Horizon Console, select **Settings > Registered Machines** and check the status of each RDS host on the RDS Hosts tab.
- Gather the configuration information you must provide to create the farm. See [Worksheet for Creating a Manual Farm in Horizon](#).

Procedure

- 1 In Horizon Console, select **Inventory > Farms**.
- 2 Click **Add**.
- 3 Select **Manual Farm**.

- 4 Follow the prompts in the wizard to create the farm.

Use the configuration information you gathered in the worksheet. You can go directly back to any wizard page by clicking the page name in the navigation pane.

- 5 Select the RDS hosts to add to the farm and click **Next**.
- 6 Click **Finish**.

What to do next

Create a published application or desktop pool.

3D Graphics Options for Manual Farms

3D graphics options are available for a manual farm of RDS using vSphere virtual machines.

These options are applicable to vSphere virtual machines. If you have a manual farm of non-vSphere virtual machines or physical servers, you can leverage GPU capabilities that are available to the OS.

NVIDIA GRID vGPU (shared GPU hardware acceleration)

A physical GPU on an ESXi host is shared among multiple virtual machines.

AMD Multiuser GPU using vDGA

A physical GPU on an ESXi host is shared among multiple virtual machines.

Virtual Dedicated Graphics Acceleration (vDGA)

A physical GPU on an ESXi host is dedicated to a single virtual machine.

Note See the VMware Hardware Compatibility List at <http://www.vmware.com/resources/compatibility/search.php>. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

3D graphics is only supported when you use the PCoIP or VMware Blast protocol. Therefore, the farm must use PCoIP or VMware Blast as the default protocol and users must not be allowed to choose the protocol.

With vDGA, you allocate an entire GPU to a single machine for maximum performance. The RDS host must be in a manual farm.

With AMD Multiuser GPU using vDGA, you can share an AMD GPU between multiple RDS hosts by making it appear as multiple PCI passthrough devices. The RDS host must be in a manual farm.

With NVIDIA GRID vGPU, each graphics card can support multiple RDS hosts or virtual machines. If an ESXi host has multiple physical GPUs, you can also configure the way the ESXi host assigns virtual machines to the GPUs. By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is called performance mode. You can also choose consolidation mode, where the ESXi host assign virtual machines to the same physical GPU until the maximum number of virtual machines is reached before placing virtual machines on the next physical GPU. To configure consolidation mode, edit the `/etc/vmware/config` file on the ESXi host and add the following entry:

```
vGPU.consolidation = "true"
```

Overview of Steps for Configuring 3D Graphics

This overview describes tasks that you must perform in vSphere and Horizon 8 to configure 3D graphics. For more information about setting up NVIDIA GRID vGPU, see the document [NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1](#). For more information about setting up vDGA, see the document [Graphics Acceleration in View Virtual Desktops](#). For more information about setting up AMD Multiuser GPU using vDGA, see the *Setting Up Virtual Machine Desktops in Horizon 7* guide.

- 1 Set up an RDS host virtual machine. For more information, see [Chapter 13 Setting Up Remote Desktop Services Hosts](#).
- 2 Add the graphics PCI device to the virtual machine. See "Other Virtual Machine Device Configuration" in the chapter "Configuring Virtual machine Hardware" in the *vSphere Virtual Machine Administration* document. Be sure to click **Reserve all memory** when adding the device.
- 3 On the virtual machine, install the device driver for the graphics card.
- 4 Add the RDS host to a manual farm, create a published desktop pool, connect to the desktop using PCoIP, and activate the display adapter.

You do not need to configure 3D graphics for RDS hosts in Horizon Console. Selecting the option **3D RDSH** when you install Horizon Agent is sufficient. By default, this option is not selected and 3D graphics is disabled.

Managing Farms

In Horizon Console, you can add, edit, delete, enable, and disable farms.

After you create a farm, you can add or remove RDS hosts to support more or fewer users.

Edit a Farm

For an existing farm, you can make changes to the configuration settings.

Prerequisites

Familiarize yourself with the settings of a farm.

Procedure

- 1 In Horizon Console, select **Inventory > Farms**.
- 2 Select a farm and click **Edit**.
- 3 Make changes to the farm settings.
- 4 Click **OK**.

Delete a Farm

You can delete a farm if you no longer need it or if you want to create a new one with different RDS hosts. You can only delete a farm that is not associated with published desktop or application pool.

Prerequisites

Verify that the farm is not associated with any published desktop pool or application pool.

Procedure

- 1 In Horizon Console, select **Inventory > Farms**.
- 2 Select one or more farms and click **Delete**.
- 3 Click **OK** to confirm.

Disable or Enable a Farm

When you disable a farm, users can no longer launch published desktops or applications from the published desktop pools and the application pools that are associated with the farm. Users can continue to use published desktops and applications that are currently open.

You can disable a farm if you plan to do maintenance on the RDS hosts in the farm or on the published desktop and application pools that are associated with the farm. After you disable a farm, some users might still be using published desktops or applications that they opened before you disable the farm.

Procedure

- 1 In Horizon Console, select **Inventory > Farms**.
- 2 Select one or more farms and click **More Commands**.
- 3 Click **Enable** or **Disable**.
- 4 Click **OK** to confirm.

Results

You can view the status of the pools by selecting **Inventory > Desktops** or **Inventory > Applications**.

Schedule Maintenance for an Automated Instant-Clone Farm in Horizon

With the maintenance operation, you can schedule recurring or immediate maintenance of all the RDS hosts in an automated instant-clone farm. During each maintenance cycle, all the RDS hosts are refreshed from the golden image virtual machine. Depending on how you want the golden image to be managed, you can change the golden image and snapshot source in your pool from vCenter to Image Catalog or reverse. For more information on the Image Management Service, see the *Managing Horizon Images from the Cloud* document.

You can make changes to the golden image virtual machine without affecting the RDS host instant clones because the snapshot of the current golden image VM is used for maintenance. The instant clones created in the automated farm use the information in the golden image VM for their system configuration.

If possible, schedule maintenance operations during off-peak hours to ensure all that RDS hosts have finished maintenance and are available during peak hours.

Prerequisites

- Decide when to schedule the maintenance operation. By default, Connection Server starts the operation immediately.

You can schedule an immediate maintenance or recurring maintenance or both for a farm. You can schedule maintenance operations on multiple farms concurrently.

- Decide whether to force all users to log off when the maintenance operation begins or wait for each user to log off before refreshing that user's machine.

If you force users to log off, Horizon 8 notifies users before they are disconnected and allows them to close their applications and log off.

- Decide the minimum farm size. The minimum farm size is the number of RDS hosts that are kept available at all times to allow users to continue to use the farm. For example, if the farm

size is ten and the minimum farm size is two, then maintenance will be performed on eight RDS hosts. As each RDS host becomes available again then the remaining hosts will go through maintenance. All RDS hosts are managed individually, so as one host becomes available then one of the remaining hosts will be put into maintenance.

However, if you schedule immediate maintenance, then all the RDS hosts in the farm will be put into maintenance.

All RDS hosts will also be subject to policy and will wait for logoff or force users to logoff depending upon what policy is configured.

- Decide whether to stop provisioning at first error. If you select this option and an error occurs when Connection Server provisions an instant-clone, provisioning stops. You can select this option to ensure that resources such as storage are not consumed unnecessarily.

Selecting the **Stop at first error** option does not affect customization. If a customization error occurs on an instant-clone, other clones continue to be provisioned and customized.

- Verify that provisioning is enabled. When provisioning is disabled, Horizon 8 stops the machines from being customized after they are refreshed.
- If your deployment includes replicated Connection Server instances, verify that all instances are the same version.

Procedure

- 1 In Horizon Console, select **Inventory > Farms**.
- 2 Click the pool ID of the farm for which you want to schedule a maintenance.
- 3 Click **Maintain > Schedule**.

4 In the **Schedule Recurring Maintenance** wizard, choose a maintenance mode.

◆ Option	Action
Recurring	<p>Schedules periodic maintenance of all the RDS host servers in a farm.</p> <ul style="list-style-type: none"> ■ Select a date and time from which the maintenance is effective. ■ Select a maintenance period. You can select daily, monthly, or weekly maintenance periods. ■ Select a repeat interval in days for the maintenance operation to recur. <p>If an immediate maintenance is scheduled on a farm, then the immediate maintenance date becomes the effective date for any recurring maintenance. If you cancel the immediate maintenance, then the current date becomes the effective date for recurring maintenance.</p>
Immediate	<p>Schedules immediate maintenance of all the RDS host servers in a farm. Immediate maintenance creates a one-time maintenance schedule for immediate or near future maintenance. Use immediate maintenance to refresh the farm from a new image when you want to apply urgent security patches.</p> <p>Select an immediate maintenance configuration.</p> <ul style="list-style-type: none"> ■ Select Start Now to start the maintenance operation instantly. ■ Select Start at to start the maintenance operation at a near future date and time. Enter the date and Web browser local time. <p>Note Recurring maintenance will be put on hold until immediate maintenance is complete.</p>
Publish Secondary Image	<p>The image you used to create a pool is the default image. By default, all maintenance operations use this image to update all machines in the farm.</p> <p>You can optionally publish a secondary image, which you can use to update a subset of the machines in the farm while leaving the rest unchanged.</p> <p>After you have published the secondary image, options are enabled to apply either of the images to selected machines without using the Schedule Recurring Maintenance process.</p> <ul style="list-style-type: none"> ■ To apply the secondary image, select the machines on the RDS Hosts tab of the Farms page and then select More Commands > Apply Secondary Image. ■ To apply the default image, select the machines on the RDS Hosts tab of the Farms page and then select More Commands > Apply Default Image.

Option	Action
	<p>If the new image meets your acceptance criteria, you can promote this secondary image to be your default image. Otherwise, you can cancel the secondary image and the default image will get applied to the desktop pool.</p> <ul style="list-style-type: none"> ■ There is an option on the Summary tab to promote the secondary image. This causes the secondary image to become the new default image on the pool and applies it to all the machines in the pool. To promote the secondary image, select Maintain > Promote Secondary Image. ■ To cancel the secondary image, select Maintain > Cancel on the Summary tab. <ul style="list-style-type: none"> ■ If the pool is set to refresh on logoff, the desktops that are currently on the secondary image will revert to the default image once the user logs off. ■ If the pool is not set to refresh on logoff, the desktops on the secondary image remain on it unless a recover, delete, or refresh is performed on the desktop.

5 Click **Next**.

6 (Optional) Click **Change** to change the golden image virtual machine. You can change the image source from vCenter to Image Catalog or vice versa.

7 Select a snapshot.

You cannot select a different snapshot unless you clear the **Use current parent VM image** checkbox. Click **Snapshot Details** to display details about the snapshot. If the image source is Image Catalog, select the required stream and marker.

Note If you are a VMware Carbon Black customer and select a golden image configured with Carbon Black, then the screen displays information from the Carbon Black Scan for each snapshot listed.

- If you select the Show All Images check box, the list might include snapshots that are not compatible and cannot be selected.
- If no value appears in the Carbon Black Scan (% Complete) column, that indicates that the Carbon Black sensor was not enabled in the Instant Clone golden image when the snapshot was taken. For more information, see the [VMware Carbon Black Cloud Documentation](#).

8 Click **Next**.

9 (Optional) Specify whether to force users to log off or wait for users to log off.

The option to force users to log off is selected by default.

- 10 (Optional) Specify whether to stop provisioning at first error.

This option is selected by default.

- 11 Click **Next**.

The **Ready to Complete** page is displayed.

- 12 Click **Finish**.

Creating Published Desktop Pools

15

One of the tasks that you perform to give users remote access to session-based desktops is to create a published desktop pool. A published desktop pool runs on a farm of RDS hosts and has properties that can satisfy some specific needs of a remote desktop deployment.

This chapter includes the following topics:

- [Understanding Published Desktop Pools](#)
- [Published Desktop Pools Settings](#)
- [Create a Published Desktop Pool](#)
- [Troubleshooting Instant Clones in the Internal VM Debug Mode](#)

Understanding Published Desktop Pools

An published desktop pool is one of three types of desktop pools that you can create. This type of pool was known as a Microsoft Terminal Services pool in previous Horizon 8 releases.

A published desktop pool and a published desktop have the following characteristics:

- A published desktop pool is associated with a farm, which is a group of RDS hosts. The farm can be an automated farm or a manual farm. Each RDS host is a Windows server that can host multiple published desktops.
- A published desktop is based on a session to an RDS host. In contrast, a desktop in an automated desktop pool is based on a virtual machine, and a desktop in a manual desktop pool is based on a virtual or physical machine.
- A published desktop supports the RDP, PCoIP, and VMware Blast display protocols.
- A published desktop pool is only supported on Windows Server operating systems that support the RDS role and are supported by Horizon 8. See "System Requirements for Guest Operating Systems" in the *Horizon Installation and Upgrade* document.
- Horizon 8 provides load balancing of the RDS hosts in a farm by directing connection requests to the RDS host that has the least number of active sessions.

Published Desktop Pools Settings

You can specify certain pool settings when you create an published desktop pool that run on a farm of RDS hosts. Not all pool settings apply to all types of desktop pools. These settings are specific to published desktop pools.

Table 15-1. Settings for a Published Desktop Pool

Setting	Description	Default Value
State	<ul style="list-style-type: none"> ■ Enabled. After being created, the desktop pool is enabled and ready for immediate use. ■ Disabled. After being created, the desktop pool is disabled and unavailable for use, and provisioning is stopped for the pool. This is an appropriate setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance. <p>When this state is in effect, remote desktops are unavailable for use.</p>	Enabled
Connection Server restrictions	<p>You can restrict access to the desktop pool to certain Connection Servers by clicking Browse and selecting one or more Connection Servers.</p> <p>If you intend to provide access to desktops through VMware Identity Manager, and you configure Connection Server restrictions, the VMware Identity Manager application might display desktops to users when those desktops are actually restricted. VMware Identity Manager users will be unable to launch these desktops.</p>	None
Category Folder	Specifies the name of the category folder that contains a Start menu shortcut for the desktop pool entitlement on Windows client devices.	Disabled

Table 15-1. Settings for a Published Desktop Pool (continued)

Setting	Description	Default Value
Client Restrictions	Select whether to restrict access to entitled desktop pools from certain client computers. You must add the names of the computers that are allowed to access the desktop pool in an Active Directory security group. You can select this security group when you add users or groups to the desktop pool entitlement.	Disabled
Allow user to initiate separate sessions from different client devices	<p>When you enable this setting, users that connect to the same desktop pool from different client devices receive different desktop sessions. To reconnect to an existing desktop session, users must use the same device from which that session was initiated. If you do not select this setting, users are always reconnected to their existing desktop sessions, regardless of the client device that they use. The RDP display protocol is not supported if you select this setting.</p> <p>Default is No.</p> <hr/> <p>Note If you enable this policy, all the desktop pools in the global entitlement must also support multiple sessions per user.</p> <hr/> <p>For more information about understanding the multiple sessions per user policy for global desktop entitlements, see the <i>Cloud Pod Architecture in Horizon</i> document.</p>	

Create a Published Desktop Pool

You create a published desktop pool as part of the process to give users access to desktops that run on a farm of RDS hosts.

Prerequisites

- Set up RDS hosts. See [Chapter 13 Setting Up Remote Desktop Services Hosts](#).
- Create a farm that contains the RDS hosts. See [Chapter 14 Creating and Managing Farms](#).
- Decide how to configure the pool settings. See [Published Desktop Pools Settings](#).

Procedure

- 1 In Horizon Console, select **Inventory > Desktops**.
- 2 Click **Add**.
- 3 Select **RDS Desktop Pool** and click **Next**.

- 4 Provide a pool ID, display name, and description.

The pool ID is the unique name that identifies the pool in Horizon Console. The display name is the name of the published desktop pool that users see when they log in to Horizon Client. If you do not specify a display name, it will be the same as the pool ID.

- 5 Select pool settings.
- 6 Select an existing farm or create a farm for this pool.

What to do next

Entitle users to access the pool.

If you have connected your pod to Horizon Cloud and want information on configuring published desktop pools for use in a Universal Broker environment, see [Horizon Pods - Configure RDSH Desktops and Applications for a Universal Broker Environment](#).

Troubleshooting Instant Clones in the Internal VM Debug Mode

You can use the internal VM debug mode to troubleshoot internal virtual machines in instant clone desktop pools. With the internal VM debug mode, you can analyze failed internal virtual machines before these virtual machines are deleted. You must enable the internal VM debug mode before you create an instant clone desktop pool.

Procedure

- 1 In the vSphere Web Client, select the golden VM, and click **Manage > Configure > VM Options > Edit > VM Options > Advanced > Edit Configuration**.

The **Configuration Parameters** window displays a list of parameter names and values.

- 2 In the **Configuration Parameters** window, search for the `cloneprep.debug.mode` parameter.

If the golden VM does not have the `cloneprep.debug.mode` parameter, you must add `cloneprep.debug.mode` as the parameter name and add a value of ON or OFF. If the golden VM has the `cloneprep.debug.mode` parameter, you can change the value of the parameter to ON or OFF.

- 3 Enable or disable the internal VM debug mode for internal VMs.
 - To enable the internal VM debug mode, set the value of `cloneprep.debug.mode` to ON. If you enable the internal VM debug mode, the internal VMs are not locked and cannot be deleted by Connection Server.
 - To disable the internal VM debug mode, set the value of `cloneprep.debug.mode` to OFF. If you disable the internal VM debug mode, the internal VMs are locked and can be deleted by Connection Server.

For instant clone actions such as prime, provision, resync, or unprime, the internal virtual machines use the value set in the golden virtual machine. If you do not disable the internal VM

debug mode, then the VMs remain in vSphere till you delete the VMs. For further debugging on instant clone actions, you can also log in to the internal VM and view the instant clone logs. You can also see the following VMware Knowledge Base articles for further debugging on instant clone actions:

- Differences between VMware ClonePrep, QuickPrep and Microsoft Sysprep (2003797) <https://kb.vmware.com/s/article/2003797>
- Initial publish of an Instant Clone desktop pool image fails and the template VMs are deleted (2144938) <https://kb.vmware.com/s/article/2144938>
- Computer-based Global Policy Objects (GPOs) that require reboot are not applied on Instant Clones (2150495) <https://kb.vmware.com/s/article/2150495>
- How to change SVGA settings for Instant Clone Pools (2151745) <https://kb.vmware.com/s/article/2151745>

Creating Application Pools

16

One of the tasks that you perform to give users remote access to an application is to create an application pool. Users who are entitled to an application pool can access the application remotely from a variety of client devices.

With application pools, you can deliver a single application to many users. The application runs on a farm of RDS hosts or a desktop pool.

When you create an application pool, you deploy an application in the data center that users can access from anywhere on the network.

An application pool has a single application and is associated with a single farm or desktop pool. To avoid errors, you must install the application on all of the RDS hosts in the farm or desktop pool.

When you create an application pool, Horizon 8 automatically displays the applications that are available to all users rather than individual users from the **Start** menu on all the RDS hosts in the farm or desktop pool. You can select one or more applications from the list. If you select multiple applications from the list, a separate application pool is created for each application. You can also manually specify an application that is not on the list. If an application that you want to manually specify is not already installed, Horizon 8 displays a warning message.

When you create an application pool, you cannot specify the access group in which to place the pool. For published application and desktop pools, you specify the access group when you create a farm or desktop pool.

An application supports the PCoIP and VMware Blast display protocols.

This chapter includes the following topics:

- [Worksheet for Creating an Application Pool Manually](#)
- [Create an Application Pool](#)
- [Managing Application Pools](#)

Worksheet for Creating an Application Pool Manually

When you create an application pool and manually specify an application, you can add information about the application. It is not a requirement that the application is already installed on any RDS host.

Table 16-1. Worksheet: Application Properties for Creating an Application Pool Manually

Property	Description	Fill in Your Value Here
Select an RDS Farm or Desktop Pool	Select a farm or a desktop pool from the list of desktops with supported session type Application or Application and Desktop.	
ID	Unique name that identifies the pool in Horizon Console. This field is required.	
Display Name	Pool name that users see when they log in to Horizon Client. If you do not specify a display name, it will be the same as ID .	
Version	Version of the application.	
Publisher	Publisher of the application.	
Path	Full pathname of the application. For example, C:\Program Files\appl.exe. This field is required.	
Start Folder	Full pathname of the starting directory for the application.	
Parameters	Parameters to pass to the application when it starts. For example, you can specify <code>-username user1 -loglevel 3</code> .	
Description	Description of this application pool.	
Pre-launch	<p>Select this option to configure an application so that an application session is launched before a user opens the application in Horizon Client. When a published application is launched, the application opens more quickly in Horizon Client.</p> <p>If you enable this option, the configured application session is launched before a user opens the application in Horizon Client, regardless of how the user connects to the server from Horizon Client.</p> <p>If you enable this option on applications published from a desktop with session type Application and Desktop, the desktop session may not be available.</p> <p>Note Application sessions can be disconnected when the Pre-launch session timeout (applications only) option is set when you add or edit the application farm.</p>	

Table 16-1. Worksheet: Application Properties for Creating an Application Pool Manually (continued)

Property	Description	Fill in Your Value Here
Connection Server Restrictions	<p>You can restrict access to the application pool to certain Connection Servers by clicking Browse and selecting one or more Connection Servers.</p> <p>If you intend to provide access to desktops through VMware Identity Manager, and you configure Connection Server restrictions, the VMware Identity Manager application might display desktops to users when those desktops are actually restricted. VMware Identity Manager users will be unable to launch these desktops.</p>	
Category Folder	Specifies the name of the category folder that contains a Start menu shortcut for the application pool entitlement on Windows client devices.	

Table 16-1. Worksheet: Application Properties for Creating an Application Pool Manually (continued)

Property	Description	Fill in Your Value Here
Client Restrictions	<p>Select whether to restrict access to entitled application pools from certain client computers.</p> <p>You must add the names of the computers that are allowed to access the application pool in an Active Directory security group. You can select this security group when you add users or groups to the application pool entitlement.</p>	
Multi-Session Mode	<p>You can start published application sessions in the following modes:</p> <p>Single-session: If the user opens a published application on client A in single-session mode, and then opens the same published application or another published application based on the same farm on client B then, the session on client A is disconnected and reconnected on client B.</p> <p>Multi-session: If the user opens a published application on client A in multi-session mode, and then opens the same published application or another published application based on the same farm on client B, the published application remains open on client A and a new session of the published application opens on client B. Such sessions are logged off on disconnect. You cannot enable the session pre-launch feature when multi-session mode is enabled.</p> <p>The multi-session mode has the following values:</p> <ul style="list-style-type: none"> ■ Disabled. Multi-session mode is not supported. ■ Enabled (Default Off). Multi-session mode is supported, but it is disabled by default. To use multi-session mode, users must enable the Multi-Launch setting in Horizon Client. ■ Enabled (Default On). Multi-session mode is supported, and it is enabled by default. Users can disable multi-session mode by disabling the Multi-Launch setting in Horizon Client. ■ Enabled (Enforced). Multi-session mode is always enabled. Users cannot disable it in any version of Horizon Client and the application is always launched in multi-session mode. 	

Table 16-1. Worksheet: Application Properties for Creating an Application Pool Manually (continued)

Property	Description	Fill in Your Value Here
	<p>When multi-session mode is enabled you can also configure the max-sessions count setting. This sets the maximum number of concurrent multi-sessions that can be started by a user for the same published application from different client devices.</p> <p>You can open a published application from a client in both the single-session mode and multi-session mode, which is based on the multi-session mode configuration. In this case, the client has one single-session and one multi-session.</p> <p>Enabling multi-session mode affects how HTML Access behaves when it is started from Workspace ONE. For more information, see the Workspace ONE documentation.</p> <p>For more information about using the Multi-Launch setting, see the Horizon Client documentation.</p> <hr/> <p>Note This setting is not supported for applications based on a desktop pool.</p>	

Create an Application Pool

You create an application pool as part of the process to give users access to an application that runs on RDS hosts or a desktop pool.

Prerequisites

- Set up RDS hosts. See [Chapter 13 Setting Up Remote Desktop Services Hosts](#).
- Create a farm that contains the RDS hosts. See [Chapter 14 Creating and Managing Farms](#).
- If you plan to add the application pool manually, gather information about the application. See [Worksheet for Creating an Application Pool Manually](#)

Procedure

- 1 In Horizon Console, select **Inventory > Applications**.
- 2 Click **Add**.
- 3 Follow the prompts in the wizard to create the pool.

If you choose to add an application pool manually, use the configuration information you gathered in the worksheet. If you select applications from the list that Horizon Console displays, you can select multiple applications. A separate pool is created for each application.

What to do next

Entitle users to access the pool. You can also view the number of entitled users that are using a published application in the **User Count** column in the application pools page.

Make sure that your end users have access to Horizon Client 3.0 or later software, which is required to support published applications.

If you need to ensure that Connection Server launches the application only on RDS hosts that have sufficient resources to run the application, configure an anti-affinity rule for the application pool.

Note For applications running on desktop pools, the anti-affinity rule is supported only for applications created from floating desktop pools, and not from dedicated desktop pools.

See [Configure an Anti-Affinity Rule for an Application Pool in Horizon Console](#).

If you have connected your pod to Horizon Cloud and want information on configuring published desktop pools for use in a Universal Broker environment, see [Horizon Pods - Configure RDSH Desktops and Applications for a Universal Broker Environment](#).

Managing Application Pools

You can add, edit, delete, or entitle application pools in Horizon Console.

Edit an Application Pool

You can edit an existing application pool to configure settings such as display name, version, publisher, path, start folder, parameters, and description. You cannot change the ID or access group of an application pool.

Prerequisites

- Familiarize yourself with the settings of an application pool.
- You might need to configure an anti-affinity rule to ensure that Connection Server launches the application only on RDS hosts that have sufficient resources to run the application.

Procedure

- 1 In Horizon Console, select **Inventory > Applications**.
- 2 Select a pool and click **Edit**.
- 3 Make changes to the pool settings.
- 4 Click **OK**.

Delete an Application Pool

When you delete an application pool, users can no longer launch the application in the pool.

You can delete an application pool even if users are currently accessing the application. After the users close the application, they can no longer access the application.

Procedure

- 1 In Horizon Console, select **Inventory > Applications**.
- 2 Select one or more application pools and click **Delete**.
- 3 Click **OK** to confirm.

Duplicate an Application Pool

You can duplicate an application pool to create multiple applications that are similar to each other.

When you duplicate an application pool, you can change the application pool ID and description to create a new application pool.

Note If there is an icon for the original application pool, the icon does not get associated with the duplicate application pool. However, you can assign the original icon to the duplicate application pool.

Note If there are user entitlements for the original application pool, the duplicate application pool does not get these entitlements and you must entitle users to the duplicate application pool again.

Procedure

- 1 In Horizon Console, select **Inventory > Applications**.
- 2 Select an application pools and click **Duplicate**.
- 3 Enter an application pool ID.
- 4 (Optional) Enter a display name and a description.
- 5 Click **OK**.

What to do next

Entitle users to the duplicate application pool. See "Entitling Users and Groups" in the *Horizon Administration* document.

Change the Icon of a Published Application

You can customize the icons for published applications for end users. When you change the icon for a published application, the new application icon is available for the end user to view on the published desktop.

Prerequisites

- Verify that the icon is available in the .PNG file format.

Procedure

- 1 In Horizon Console, select **Inventory > Applications**.

- 2 Select an application pool or multiple application pools and click **Application Icon > Associate Application Icon**.
- 3 To upload an icon, click **Upload Icon File** and browse for an icon in the .PNG format.
The icon file must be between 16x16 pixels and 256x256 pixels.
- 4 Click **OK**.

Results

The icon appears for the published application on the published desktop.

Remove the Icon of a Published Application

You can remove the icon of a published application to replace it with another icon. When you remove the icon for a published application, the published application is replaced with the default icon on the published desktop. You can remove icons from multiple published applications only if all published applications have the same icon. You cannot select multiple published applications that have different icons to remove an icon.

Procedure

- 1 In Horizon Console, select **Inventory > Applications**.
- 2 Select an application pool or multiple application pools and click **Application Icon > Remove Application Icon**.

Results

The published application is replaced with the default icon on the published desktop.

Enable or Disable an Application Pool

When you enable an application pool, entitled users have access to the application pool. When you disable an application pool, entitled users no longer have access to the application pool. You can enable or disable one or multiple application pools.

Prerequisites

- Verify that you have the **Enable Farms, Desktops and Applications Pools** privilege.

Procedure

- 1 In Horizon Console, select **Inventory > Applications**.
- 2 Select one or more application pools.
- 3 Choose to enable or disable an application pool or pools.
 - To enable an application pool or pools, click **More > Enable Pool**.
 - To disable an application pool or pools, click **More > Disable Pool**.
- 4 Click **OK** to confirm.

Configure an Anti-Affinity Rule for an Application Pool in Horizon Console

When you configure an anti-affinity rule for an application pool, Horizon Connection Server attempts to launch the application only on RDS hosts that have sufficient resources to run the application. This feature can be useful for controlling applications that consume large amounts of CPU or memory resources.

An anti-affinity rule consists of an application matching pattern and a maximum count. For example, the application matching pattern might be `autocad.exe` and the maximum count might be 2.

Connection Server sends the anti-affinity rule to Horizon Agent on an RDS host. If any applications running on the RDS host have process names that match the application matching pattern, Horizon Agent counts the current number of instances of those applications and compares the number to the maximum count. If the maximum count is exceeded, Connection Server skips that RDS host when it selects an RDS host to run new sessions of the application.

Prerequisites

- Create the application pool. See [Create an Application Pool](#).
- Become familiar with the constraints of the anti-affinity feature. See [Anti-Affinity Feature Constraints](#).

Procedure

- 1 In Horizon Console, select **Inventory > Applications**.
- 2 Select the pool to modify and click **Edit**.
- 3 In the **Anti-Affinity Patterns** text box, type a comma-separated list of patterns to match against the process names of other applications running on RDS hosts.

The pattern string can include the asterisk (*) and question mark (?) wildcard characters. An asterisk matches zero or more characters and a question mark matches any single character. For example, `*pad.exe, *notepad.???` matches `wordpad.exe`, `notepad.exe`, and `notepad.bat`, but it does not match `wordpad.bat` or `notepad.script`.

Note Horizon 8 counts multiple patterns that match for an application in a single session as a single match.

- 4 In the **Anti-Affinity Count** text box, type the maximum number of other applications that can be running on the RDS host before the RDS host is rejected for new application sessions.
The maximum count can be an integer from 1 to 20.
- 5 Click **Submit** to save your changes.

Anti-Affinity Feature Constraints

The anti-affinity feature has certain constraints.

- Anti-affinity rules affect new application sessions only. An RDS host that contains sessions in which a user has previously run an application is always reused for the same application. This behavior overrides reported load preferences and anti-affinity rules.
- Anti-affinity rules do not affect application launches from within an RDS desktop session.
- RDS session limits prevent application sessions from being created, regardless of anti-affinity rules.
- In certain circumstances, the instances of applications on the RDS host might not be restricted to the maximum count that you specify. For example, Horizon 8 cannot determine the exact instance count if other applications for other pending sessions are in the process of being launched.
- Inter-application anti-affinity rules are not supported. For example, large application classes, such as Autocad and Visual Studio instances, cannot be counted in a single rule.
- Do not use anti-affinity rules in environments where end-users use Horizon Client on mobile clients. Anti-affinity rules can result in multiple sessions in the same farm for an end user. Reconnecting to multiple sessions on mobile clients can result in indeterminate behavior.
- Anti-Affinity rules consider only the connected number of sessions for load balancing. However, load balancing for RDS hosts considers the sum of the connected, pending, and disconnected sessions for load balancing.

Managing RDS Hosts and Sessions

17

In Horizon Console, you can perform management operations such as configuring or deleting RDS hosts or manage sessions for published desktops and applications.

This chapter includes the following topics:

- [Managing RDS Hosts in Horizon Console](#)
- [Monitor RDS Hosts in Horizon Console](#)
- [Manage Published Desktop and Application Sessions in Horizon Console](#)
- [Configuring Load Balancing for RDS Hosts in Horizon Console](#)

Managing RDS Hosts in Horizon Console

You can perform certain management tasks on the manual or automated farm of RDS hosts you have created. Note that some tasks are applicable to both manual and automated farms, whereas others are only applicable to one type of farm.

When you manually set up an RDS host, it automatically registers with Horizon Connection Server. You cannot separately register an RDS host with Connection Server. For a manual farm, you can perform the following management tasks:

- Edit the RDS host.
- Add the RDS host to a manual farm.
- Remove the RDS host from a farm.
- Enable the RDS host.
- Disable the RDS host.

For an automated farm of RDS hosts, you can perform the following management tasks:

- Remove the RDS host from a farm.
- Enable the RDS host.
- Disable the RDS host.

Edit an RDS Host in a Manual Farm

You can change the number of connections that an RDS host can support. You can set it to any positive number, or to unlimited.

You can only edit an RDS host that you set up manually, but not an RDS host that is in an automated farm.

Procedure

- 1 In Horizon Console, select **Settings > Registered Machines**.
- 2 Select an RDS host and click **Edit**.
- 3 Specify a value for the setting **Number of connections**.
- 4 Click **OK**.

Add an RDS Host to a Manual Farm

You can add an RDS host that you set up manually to a manual farm to increase the scale of the farm or for other reasons. You can only add RDS hosts to a manual farm.

Procedure

- 1 In Horizon Console, select **Inventory > Farms**.
- 2 Click the farm ID.
- 3 Select the **RDS Hosts** tab.
- 4 Click **Add**.
- 5 Select one or more RDS hosts.
- 6 Click **OK**.

Remove an RDS Host from a Manual or Automated Farm

You can remove an RDS host from a manual farm to reduce the scale of the farm, to perform maintenance on the RDS host, or for other reasons. As a best practice, disable the RDS host and ensure that users are logged off from active sessions before you remove a host from a farm.

If users have application or desktop sessions on hosts that you remove, the sessions remain active, but Horizon 8 does not track them. A user who disconnects from a session will be unable to reconnect to it, and any unsaved data might be lost.

You can also remove an RDS host from an automated farm. One possible reason might be that the RDS host is in an unrecoverable error state.

Procedure

- 1 In Horizon Console, select **Inventory > Farms**.
- 2 Click the farm ID.

- 3 Select the **RDS Hosts** tab.
- 4 Select one or more RDS hosts.
- 5 Click **Remove from farm**.
- 6 Click **OK**.

Remove a Registered RDS Host from Horizon

You can remove from Horizon 8 an RDS host that you set up manually and that you no longer plan to use. The RDS host must not currently be in a manual farm.

Prerequisites

Verify that the RDS host does not belong to a farm.

Procedure

- 1 In Horizon Console, select **Settings > Registered Machines**.
- 2 Select an RDS host and click **Remove**.
- 3 Click **OK**.

Results

After you remove an RDS host, to use it again, you must reinstall Horizon Agent.

Disable or Enable an RDS Host in a Manual or Automated Farm

When you disable an RDS host, Horizon 8 no longer uses it to host new published desktops or applications. Users can continue to use published desktops and applications that are currently open.

Procedure

- 1 In Horizon Console, select **Inventory > Farms**.
- 2 Click the farm ID.
- 3 Select the **RDS Hosts** tab.
- 4 Select an RDS host and click **More Commands**.
- 5 Click **Enable** or **Disable**.
- 6 Click **OK**.

Results

If you enable the RDS host, a check mark appears in the Enabled column, and Available appears in the Status column. If you disable the RDS host, the Enabled column is empty and Disabled appears in the Status column.

Status of RDS Hosts in Horizon Console

An RDS host can be in various states from the time that it is initialized. As a best practice, check that RDS hosts are in the state that you expect them to be in before and after you perform tasks or operations on them.

Table 17-1. Status of an RDS Host

Status	Description
Startup	Horizon Agent has started on the RDS host, but other required services such as the display protocol are still starting. The agent startup period also allows other processes such as protocol services to start up.
Disable in progress	RDS host is in the process of being disabled while sessions are still running on the host. When the sessions end, the status changes to Disabled.
Disabled	Process of disabling the RDS host is complete.
Validating	Occurs after Connection Server first becomes aware of the RDS host, typically after Connection Server is started or restarted, and before the first successful communication with Horizon Agent on the RDS host. Typically, this state is transient. This state is not the same as the Agent unreachable state, which indicates a communication problem.
Agent disabled	Occurs if Connection Server disables Horizon Agent. This state ensures that a new desktop or application session cannot be started on the RDS host.
Agent unreachable	Connection Server cannot establish communication with Horizon Agent on an RDS host.
Invalid IP	Subnet mask registry setting is configured on the RDS host, and no active network adapters have an IP address within the configured range.
Agent needs reboot	Component was upgraded, and the RDS host must be restarted to allow Horizon Agent to operate with the upgraded component.
Protocol failure	The RDP display protocol is not running correctly. If RDP is not running and PCoIP is running, clients cannot connect using either RDP or PCoIP. However, if RDP is running and PCoIP is not running, clients can connect using RDP.
Domain failure	RDS host encountered a problem reaching the domain. The domain server was not accessible, or the domain authentication failed.
Configuration error	RDS role is not enabled on the server.
Unknown	RDS host is in an unknown state.
Available	RDS host is available. If the host is in a farm, and the farm is associated with a published desktop or application pool, it will be used to deliver published desktops or applications to users.
Drain	RDS host is in drain mode and not accepting new connections.
Drain mode until restart	RDS host is in drain mode and not accepting new connections until it is restarted.

Monitor RDS Hosts in Horizon Console

You can monitor the status and view the properties of RDS hosts in both manual and automated farms in Horizon Console.

Procedure

- ◆ In Horizon Console, navigate to the page that displays the properties that you want to view.

Properties	Action
DNS Name, Type, Image, Pending Image, Task, Max Number of Connections, Sessions, Agent Version, Enabled, Status	<ul style="list-style-type: none"> ■ In Horizon Console, select Inventory > Farms. ■ Select a farm and click the RDS Hosts tab.
RDS Host, Farm, Desktop Pool, Agent Version, Sessions, Status	<ul style="list-style-type: none"> ■ In Horizon Console, select Inventory > Machines. ■ Click the RDS Hosts tab.
DNS Name, Type, RDS Farm, Max Number of Connections, Sessions, Agent Version, Enabled, Status	<ul style="list-style-type: none"> ■ In Horizon Console, select Settings > Registered Machines. ■ Click the RDS Hosts tab.

Results

The properties are displayed and have the following meanings:

Property	Description
RDS Host	Name of the RDS host.
Farm	Farm to which the RDS host belongs.
Desktop Pool	Published desktop pool associated with the farm.
Agent Version	Version of Horizon Agent that runs on the RDS host.
Sessions	Number of client sessions.
DNS Name	DNS name of the RDS host.
Type	Version of Windows Server that runs on the RDS host.
RDS Farm	Farm to which the RDS host belongs.
Image	Image of the RDS host on the farm.
Pending Image	Pending image of the RDS host on the farm.
Task	Task being performed on the RDS host of the farm.
Max Number of Connections	Maximum number of connections that the RDS host can support.
Enabled	Whether the RDS host is enabled.
Status	State of the RDS host. See Status of RDS Hosts in Horizon Console for a description of the possible states.

Manage Published Desktop and Application Sessions in Horizon Console

When a user launches a published desktop or application, a session is created. You can disconnect and log off sessions, send messages to clients, reset, and restart virtual machines.

Procedure

- 1 In Horizon Console, navigate to where session information is displayed.

Session Type	Navigation
Remote desktop sessions	<p>Select Inventory > Desktops, click a pool's ID, and click the Sessions tab. The Sessions column also appears on the Desktop Pools page for all desktops.</p> <p>Select Inventory > Farms, click a farm's ID, and click the Sessions tab.</p> <p>You can also view the published applications associated with a session. The Application Names column displays the published applications associated with a session.</p> <p>The Sessions column also appears on the Farms page for all farms.</p> <p>Select Settings > Registered Machines, and view the Sessions column.</p>
Remote desktop and application sessions	Select Monitor > Sessions .
Sessions associated with a user or user group	<ul style="list-style-type: none"> ■ Select Users and Groups. ■ Click a user's name or a user group's name. ■ Click on the Sessions tab.

- 2 Select a session.

To send a message to users, you can select multiple sessions. You can perform the other operations on only one session at a time. You can perform a log off operation only on a session that is not connected from a vSphere console.

- 3 Choose whether to disconnect, log off, send a message, restart a desktop, or reset a virtual machine.

Option	Description
Disconnect Session	Disconnects the user from the session.
Logoff Session	Logs the user off the session. Data that is not saved is lost.
Send Message	Send a message to Horizon Client. You can label the message as Info , Warning , or Error .

Option	Description
Restart Desktop	Performs a restart operation on a virtual desktop, which performs a graceful operating system restart of the virtual machine. Note This option is not available for instant-clone farms.
Reset Virtual Machine	Performs a reset operation on a virtual machine without the graceful operating system restart, which performs a hard power-off and power-on of the virtual machine. Note This option is not available for instant-clone farms.

4 Click **OK**.

Results

The session properties have the following descriptions:

Property	Description
RDS Host	Name of the RDS host.
Farm	Farm to which the RDS host belongs.
Desktop Pool	RDS desktop pool associated with the farm.
Agent Version	Version of Horizon Agent that runs on the RDS host.
Sessions	Number of client sessions.
DNS Name	DNS name of the RDS host.
Type	Version of Windows Server that runs on the RDS host.
Client ID	Name or the MAC address of the client.
Client Version	Version of Horizon Client for the user's session.
RDS Farm	Farm to which the RDS host belongs.
Max Number of Connections	Maximum number of connections that the RDS host can support.
Enabled	Whether the RDS host is enabled.
Status	State of the RDS host. See Status of RDS Hosts in Horizon Console for a description of the possible states.

Configuring Load Balancing for RDS Hosts in Horizon Console

You can configure load balancing for RDS hosts by configuring load balancing settings in Horizon Console or by creating and configuring load balancing scripts.

By default, Connection Server uses the following formula to balance the placement of published desktop and application sessions on RDS hosts:

$$(\text{connected sessions} + \text{pending sessions} + \text{disconnected sessions}) / (\text{maximum session count})$$

If the maximum session count is configured as unlimited, load balancing falls back to using the absolute number of the total session count which includes connected, pending and disconnected sessions.

Load Balancing Settings in Horizon Console

Horizon calculates the Server Load Index based on the load balancing settings you configure in Horizon Console. The Server Load Index indicates the load on the server. The Server Load Index can range from 0 to 100, where 0 represents no load and 100 represents full load. A Server Load Index of -1 indicates that load balancing is disabled. You can view the Server Load Index in the Horizon Console dashboard. Horizon also offers threshold values in the load balancing settings for logon storm handling. See, [Load Balancing Settings](#).

Load Balancing Scripts

You can also override the default behavior of the load balancing settings and control the placement of new published desktop and application sessions by writing and configuring load balancing scripts.

You can write your own custom load balancing scripts, or you can use one of the sample load balancing scripts provided with Horizon Agent. To use custom load balancing scripts, you must select the **Use Custom Script** load balancing setting in Horizon Console.

You can run these scripts on your own schedule or run these scripts with Horizon 8. For more information on configuring load balancing scripts in Horizon 8, see [Configure a Load Balancing Script on an RDS Host](#).

Configuring load balancing scripts involves enabling the VMware Horizon View Script Host service and setting a registry key on each RDS host in a farm.

Load balancing scripts must write the load index to the `CustomLoadValue` registry key with the `REG_DWORD` registry setting in the following location:

```
HKLM\Software\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue
```

The value must be between 0-100.

Horizon 8 calculates the raw performance metrics that are written to the `Performance Stats` registry key in the following location:

```
HKLM\Software\VMware Inc.\VMware VDM\Performance Stats
```

You can use the raw performance metrics and combine these with your custom index factor for writing custom scripts.

Configure Load Balancing Settings on an RDS Host in Horizon Console

You can configure load balancing settings in Connection Server to control the placement of published desktop and application sessions on RDS hosts.

Procedure

- 1 In Horizon Console, select **Inventory > Farms**.
- 2 Click **Add** and follow the prompts to the **Load Balancing Settings** page.
- 3 Configure the load balancing settings. See, [Load Balancing Settings](#).
- 4 Follow the prompts to complete the wizard and click **Submit**.

Load Balancing Settings

Horizon 8 calculates the Server Load Index based on the load balancing settings you configure in Horizon Console. The Server Load Index indicates the load on the server. The Server Load Index can range from 0 to 100, where 0 represents no load and 100 represents full load. A Server Load Index of -1 indicates that load balancing is disabled. You can view the Server Load Index in the Horizon Console dashboard. Horizon also offers threshold values in the load balancing settings for logon storm handling.

Logon storms occur when a large number of users log into the farm within a short time interval. In these events, the Server Load Index reported by the RDS hosts may be stale, or out of date, because the sampling interval for the CPU, Memory, and Disk statistics is 30 seconds and only updates those metrics after 30 seconds. Horizon provides two methods for mitigating this issue of the stale Server Load Index: the Horizon Connection Server will send session requests to RDS hosts with a lower number of concurrently connecting sessions as well as a lower load index, and the Horizon Agent will be able to reject and redirect sessions based on the number of concurrently connecting sessions on the machine and the load index using thresholds provided in the Horizon Console.

When configuring load balancing settings, follow the best practice of including the session count with other metrics, which allows the load balancing to place session requests on machines with a lower number of total sessions. In addition, follow the best practice of setting a Connecting Session Threshold in the Horizon Console, which helps better load balance during logon storms.

Logon storm handling thresholds, which include Connecting Session Threshold and Load Index Threshold, by best practice should be set only on the Horizon Console. However, they can also be set on each RDS host through Agent Configuration Policy Settings (for more information, see "VMware View Agent Configuration ADMX Template Settings" in the *Horizon Remote Desktop Features and GPOs* document). If both policy settings and Horizon Console settings for logon storm handling thresholds are set, the policy settings will take precedence.

Table 17-2. Load Balancing Settings in Horizon Console

Option	Description
Use custom script	Select this setting to use a custom script for load balancing. If this setting is enabled, Horizon 8 does not consider other load balancing metrics for calculating server load index, but it will consider the Connecting Session Threshold and Load Index Threshold used for logon storm handling. To get the server load index, Horizon reads the <code>CustomLoadValue</code> registry key in the following location: <code>HKLM\Software\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue</code> . See Writing a Load Balancing Script for an RDS Host .
Include session count	Select this setting to include the session count on the RDS host for load balancing. If none of the settings are selected for load balancing and if the custom script setting is not selected, Horizon 8 uses the session count by default. Disable this setting if you do not need to consider the session count for load balancing.
CPU usage threshold	Threshold value for the CPU usage in percentage. Horizon 8 uses the configured CPU threshold to calculate the CPU load index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.
Memory usage threshold	Threshold value for the memory in percentage. Horizon 8 uses the configured memory threshold to calculate the Memory Load Index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.
Disk queue length threshold	Threshold of the average number of both read and write requests that were queued for the selected disk during the sample interval. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing.
Disk read latency threshold	Threshold of the average time of read of data from the disk in milliseconds. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.
Disk write latency threshold	Threshold of the average time of write of data to the disk in milliseconds. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.
Connecting session threshold	Threshold value for connecting sessions, for use in logon storm handling. The configured threshold specifies the maximum number of sessions that can concurrently log into each RDSH agent machine in the farm, exempting reconnecting sessions. This is configurable from 0 to 150. The recommended value is 20, but the value can be lowered to decrease the number of concurrent sessions that can log in to further protect each RDS host. By default, this threshold is disabled and does not deny session logons (default value is 0).
Load index threshold	Threshold value for load index, for use in logon storm handling. The configured threshold specifies the minimum load index at which each RDSH agent machine in the farm will start denying session logins, exempting reconnecting sessions. This is configurable from 0 to 100. The recommended value is 0 (disabled). The value can be set to a higher number (between 90-100) to reject sessions on an RDS host based on an exceedingly high load index. By default, this threshold is disabled and does not deny session logons (default value is 0).

Writing a Load Balancing Script for an RDS Host

You can write a load balancing script to generate a load value based on any RDS host metric that you want to use for load balancing.

Your load balancing script must write the load index value to the `CustomLoadValue` registry key in the following location: `HKLM\Software\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue`. This value must be between 0-100.

If at least one RDS host in the farm returns a valid load value, the Connection Server assumes a load value of 25 for the other RDS hosts in farm until their load balancing scripts return valid values. If no RDS host in the farm returns a valid load value, the load balancing feature is disabled for the farm.

Note The Horizon Console dashboard shows -1 for those RDS hosts that do not report a load index. Connection Server only uses the value of 25 for internal load balancing logic.

If your load balancing script writes an invalid load value to the `CustomLoadValue` registry key, the value is capped at 100 and returned as the load index to the Connection Server. If the script is unable to create the `CustomLoadValue` registry key, the default value of 0 is sent as the load index to the Connection Server. If the custom script does not finish running within 10 seconds, Horizon 8 terminates the script after 10 seconds and uses stale values from the `CustomLoadValue` registry key as the load index.

Copy your load balancing script to the Horizon Agent `scripts` directory (`C:\Program Files\VMware\VMware View\Agent\scripts`) on each RDS host in the farm. You must copy the same script to every RDS host in the farm.

For an example how to write a load balancing script, see the sample scripts in the Horizon Agent `scripts` directory. For more information, see [Sample Load Balancing Scripts for RDS Hosts](#).

Sample Load Balancing Scripts for RDS Hosts

When you install Horizon Agent on an RDS host, the installer places sample load balancing scripts in the Horizon Agent `scripts` directory (`C:\Program Files\VMware\VMware View\Agent\scripts`).

Table 17-3. Sample Load Balancing Scripts

Name	Description
<code>cpuutilisation.vbs</code>	Reads the percentage of CPU that has been utilized from the registry and writes it to the <code>CustomLoadValue</code> registry key.
<code>memoryutilisation.vbs</code>	Reads the percentage of memory that has been utilized from the registry and writes it to the <code>CustomLoadValue</code> registry key.

Enable the VMware Horizon View Script Host Service on an RDS Host

You must enable the VMware Horizon View Script Host service on an RDS host before you configure a load balancing script. The VMware Horizon View Script Host service is disabled by default.

Procedure

- 1 Log in to the RDS host as an administrator.
- 2 Start Server Manager.
- 3 Select **Tools > Services** and navigate to the VMware Horizon View Script Host service.
- 4 Right-click **VMware Horizon View Script Host** and select **Properties**.
- 5 In the Properties dialog box, select **Automatic** from the **Startup type** drop-down menu and click **OK** to save your changes.
- 6 Right-click **VMware Horizon View Script Host** and select **Start** to start the VMware Horizon View Script Host service.

Results

The VMware Horizon View Script Host service restarts automatically each time the RDS host starts.

What to do next

Configure your load balancing script on each RDS host in the farm. See [Configure a Load Balancing Script on an RDS Host](#).

Configure a Load Balancing Script on an RDS Host

You must configure the same load balancing script on every RDS host in the farm. Configuring a load balancing script involves setting a registry key on the RDS host.

If you are using an automated farm, you perform this procedure on the golden image virtual machine for the automated farm.

Important You must configure the load balancing script on all of the RDS hosts in a farm or on none of the RDS hosts in a farm. If you configure a load balancing script on only some of the RDS hosts in a farm, Horizon Console sets the status of the farm to red.

Prerequisites

- Write a load balancing script and copy the same script to the Horizon Agent `scripts` directory on each RDS host in the farm. See [Writing a Load Balancing Script for an RDS Host](#).
- Enable the VMware Horizon View Script Host service on the RDS host. See [Enable the VMware Horizon View Script Host Service on an RDS Host](#).

Procedure

- 1 Log in to the RDS host as an administrator.
- 2 Start Server Manager.
- 3 Select **Tools > System Configuration**, click the **Tools** tab, and launch the Registry Editor.
- 4 In the registry, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents`.
- 5 In the navigation area, select the **RdshLoad** key.

The values for the **RdshLoad** key, if any, appear in the topic area (the right pane).

- 6 Right-click in the topic area for the **RdshLoad** key, select **New > String Value**, and create a new string value.

As a best practice, use a name that represents the load balancing script to be run, for example, **cpuutilisationScript** for the `cpuutilisation.vbs` script.

- 7 Right-click the entry for the new string value you created and select **Modify**.
- 8 In the **Value data** text box, type the command line that invokes your load balancing script and click **OK**.

Type the full path to your load balancing script.

For example: `cscript.exe "C:\Program Files\VMware\VMware View Agent\scripts\cpuutilisation.vbs"`

- 9 Restart the Horizon Agent service on the RDS host to make your changes take effect.

Results

Your load balancing script begins to run on the RDS host.

What to do next

Repeat this procedure on each RDS host in the farm. If you performed this procedure on the golden image virtual machine for an automated farm, provision the automated farm.

To verify that your load balancing script is working correctly, see [Verify a Load Balancing Script](#).

Verify a Load Balancing Script

You can verify that your load balancing script is working correctly by viewing RDS farm and RDS host information in Horizon Console.

Procedure

- 1 In Horizon Console, navigate to **Monitor > Dashboard**.
- 2 In the **Issues** pane, click **View**.

3 Click **RDS Farms** and click the name of each RDS host to view its load index.

The Server load field in the details dialog box shows the server load index reported by Horizon Agent. The value should be between 0-100.

The status of the farm should be green. If a load balancing script is configured on only some of the RDS hosts in a farm, Horizon Console sets the status of the farm to yellow. You must configure the load balancing script on all of the RDS hosts in a farm or on none of the RDS hosts in a farm.

What to do next

If load balancing is not working as you expected, verify the content of your load balancing script. If the script is written correctly, it should update the `CustomLoadValue` registry key on Horizon Agent with the expected load index. The `CustomLoadValue` registry key is located in the following location: `HKLM\Software\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue`. Verify that this registry key is updated correctly. If you use Horizon 8 to run your scripts, verify that the VMware Horizon View Script Host service is running. Also, verify that the same load balancing script is configured on each RDS host in the farm.