# Table of Contents

Lab Overview - HOL-1851-07-ADV - Horizon 7.1 Advanced: Operational Concepts ........2
  Lab Guidance .................................................................................................................. 3
Module 1 - Optimize Windows Images (30 minutes) .......................................................... 9
  Introduction.......................................................................................................................10
  VMware OS Optimization Tool Overview.....................................................................11
  Running the VMware OS Optimization Tool ...............................................................13
  Conclusion.......................................................................................................................29
Module 2 - Management with Group Policies (30 minutes) ............................................31
  Introduction.......................................................................................................................32
  Horizon Group Policy Objects ........................................................................................33
  RDS Host Group Policies..................................................................................................48
  Group Policy Settings for User Environment Manager ...............................................61
  Group Policies Best Practices .......................................................................................66
  Conclusion.......................................................................................................................72
Module 3 - Management using PowerCLI for Horizon (30 Minutes) ..............................74
  Introduction.......................................................................................................................75
  Automating VMware Horizon 7 with VMware PowerCLI 6.5 ...............................76
  Conclusion.......................................................................................................................84
Module 4 - Reporting with vRealize Log Insight (15 minutes) .........................................85
  Introduction.......................................................................................................................86
  vRealize Log Insight and Horizon ................................................................................87
  Conclusion.......................................................................................................................89
Module 5 - vRealize Operations for Horizon (30 minutes) .............................................90
  Module Overview ...........................................................................................................91
  Hands-on Labs Interactive Simulation: vRealize Operations for Horizon .................92
  Conclusion.......................................................................................................................93
Lab Overview - HOL-1851-07-ADV - Horizon 7.1 Advanced: Operational Concepts
Lab Guidance

Note: It will take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

Attendees will go into the operational concepts of VMware Horizon 7.1 by looking at an overview of Optimizing Windows Images with VMware OS Optimization Tool, Management with Group Policies of the Horizon environment, Management using PowerCLI for Horizon, Reporting with Log Insight into the Horizon environment, and working with vRealize Operations Manager for Horizon looking at Horizon specific dashboards.

Lab Module List:

- **Module 1 - Optimize Windows Images** (30 minutes) (Basic) Optimizing for Windows 10 master image with our Optimization tool and the top things to take into consideration.
- **Module 2 - Management with Group Policies** (30 minutes) (Advanced) Using the Horizon Extra’s GPO Bundle to optimize and streamline your virtual environment’s resources.
- **Module 3 - Management using PowerCLI for Horizon** (30 minutes) (Advanced) Making daily task and automation of Horizon functions easier with Horizon PowerCLI 6.5
- **Module 4 - Reporting with vRealize Log Insight** (15 minutes) (Advanced) Making log and events analysis easier and more intuitive with Log Insight.
- **Module 5 - vRealize Operations for Horizon (iSIM)** (30 minutes) (Intermediate) In-depth analysis and proactive investigation of your Horizon environment with vRealize Operations for Horizon. (iSIM)

Lab Captains:

- **Module 1 - Laurel Spadaro, Sr. Systems Engineer, US; Tom Baella, Systems Engineer, US**
- **Module 2 - Laurel Spadaro, Sr. Systems Engineer, US; Tom Baella, Systems Engineer, US**
- **Module 3 - Laurel Spadaro, Sr. Systems Engineer, US; Tom Baella, Systems Engineer, US**
- **Module 4 - Laurel Spadaro, Sr. Systems Engineer, US; Tom Baella, Systems Engineer, US**
• Module 5 - Laurel Spadaro, Sr. Systems Engineer, US; Tom Baella, Systems Engineer, US

This lab manual can be downloaded from the Hands-on Labs Document site found here:

http://docs.hol.vmware.com

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:


Location of the Main Console

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the EXTEND to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.
Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are some very helpful methods of entering data which make it easier to enter complex data.

Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.
Click once in active console window

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the **Shift** key.

Click on the @ key

1. Click on the "@ key".

Notice the @ sign entered in the active console window.
Activation Prompt or Watermark

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Look at the lower right portion of the screen
Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.
Module 1 - Optimize Windows Images (30 minutes)
Introduction

Optimization of the Windows 10 master image is key to delivering a high performance desktop to the users in the Horizon environment. We will show the top settings in the Optimization Tool to use when analyzing and optimizing the environment. We’ll cover the basics of how to install the tool and what to look out for when these optimizations are offered by the analysis portion of the tool. We’ll also cover some basic best practices when creating an initial master image as well.

This module contains the following lessons:

• Introduction to the VMware OS Optimization Tool - In this lesson we will go over the high level benefits of the OS Optimization Tool.

• Running the VMware OS Optimization Tool - We will run the OS Optimization Tool on a Windows 10 desktop and show you how to optimize the desktop.
VMware OS Optimization Tool Overview

The VMware OS Optimization Tool (OSOT) helps optimize Windows 7/8/2008/2012/10 systems for use with VMware Horizon View. The optimization tool includes customizable templates to enable or disable Windows system services and features, per VMware recommendations and best practices, across multiple systems. Since most Windows system services are enabled by default, the optimization tool can be used to easily disable unnecessary services and features to improve performance.

You can perform the following actions using the VMware OS Optimization Tool:

- Local Analyze/Optimize
- Remote Analyze
- Optimization History and Rollback
- Managing Templates

Windows was designed for physical hardware, specifically desktops, and for that hardware to be accessed by just one user at a time. Windows uses many resources to present a responsive desktop, but many of its settings are unnecessary or even detrimental when applied to a virtual environment. These actions include, for example, animating windows as the user opens them. Performing this animation takes significant CPU resources, which decreases the number of desktops that you can host per VMware vSphere server. Consequently, this non-essential function in a virtual machine (VM) environment increases the amount of system hardware that you need. Even if hardware is plentiful, Windows animations do not perform well when accessed remotely, especially when connecting over a slow WAN or Internet connection. As a result, keeping animations enabled (in addition to other features unnecessary for VMs) impairs the end-user experience. Another example of desktop optimization in a virtual machine environment is to disable Windows Update so that control of the service is isolated to administrators. Administrators can run Windows Update in batch mode for the VMs as opposed to users performing this task.

What Are You Optimizing?

Using the recommendations provided in the OSOT, you are maximizing the efficiency and performance of your virtual desktops and RDSH servers.

Optimizing virtual desktops

- Increases their performance
- Increases their density, boosting the number of virtual desktops that can be hosted per vSphere server, thereby reducing infrastructure costs
- Improves end-user experience
- Reduces end-user support incidents

Optimizing RDSH servers
• Increases hosted desktop and application performance
• Reduces the amount of system resources that each RDSH server requires
• Increases the number of RDSH servers that can be hosted virtually on Windows Server 2008 R2 or Windows Server 2012
• Increases the number of users that can be supported per RDSH server
• Improves the end-user hosted desktop and application experience
• Reduces system support incidents

When Do You Optimize?

The traditional approach to optimizing virtual desktops or RDSH servers is to use a master image. You apply optimizations to the master image, which is used to create a desktop pool. You can also use a master image to deploy multiple RDSH servers.

Another optimization type frequently performed is one that is made spontaneously to remote systems. This kind of optimization is often performed to tune something that was not optimized when the system was first deployed. However, it is also performed because something has changed, and new optimizations are needed on remote systems that cannot be redeployed.

You can perform both types of optimization using the OSOT.

VMware OS Optimization Tool Provides

The OSOT provides the easiest and most efficient way to optimize your Windows desktop and server master images. It offers many advantages over traditional scripts, including the ability to roll back changes, selectively edit optimization values, and view detailed audit information before applying optimizations.

The OSOT includes customizable built-in templates to enable or disable Windows features and system services across multiple platforms. You use the OSOT to improve Windows performance, as per VMware recommendations and best practices.

The OSOT is a free VMware Fling that you can download.

https://labs.vmware.com/flings/vmware-os-optimization-tool
Running the VMware OS Optimization Tool

We are going to log in to a desktop and run the VMware OS Optimization Tool which is located on the ControlCenter Server.

Launch Chrome Browser

From the Main Console launch the Chrome browser from the tool bar.

1. Click the Chrome icon along the bottom toolbar of the Main Console.

Log in to the vSphere Web Client

1. From the HOL-1851 Admin drop down on the Chrome Browser, click on the **vCenter Web Client** to launch the webclient.
2. Log in as **Administrator@corp.local** and standard HOL password **VMware1!**
3. Click Login

1. Scroll down the left pane or expand the **RegionA01-IC01** cluster.
2. Scroll down to the bottom of the list.
Open Console to W10-IC-01

We are going to open up a console into the W10-IC-01 server which is running Windows 10.

1. Right-click on W10-IC-01 desktop.
2. Click on Open Console.
Login as Administrator to the Desktop

1. Once the desktop loads, click on **Send Ctrl+Alt+Del**
2. Log in as administrator. Make sure CORP\Administrator is selected, otherwise click **Other user** in the bottom left corner and enter **Administrator@corp.local**
3. Enter password **VMware1!** and Click Enter or --> to login
Close the Identity Manager Desktop - Login Window

If the Identity Manager Desktop - Login window appears, close it as we will not be using it in this module but it is used for other labs.

1. Click the X in the top right corner of the Identity Manager Desktop - Login window
Bring up the OSOT file from the ControlCenter server.
1. Click on the Windows Explorer icon in the W10-IC-01 window toolbar.
2. Go to the tools directory on the ControlCenter system by typing in: `\controlcenter\c$\tools` and hit return.
3. Double-click the `VMwareOSOptimizationTool_b1090b` directory.

**Launch the OSOT Executable**

![Image of file explorer showing VMwareOSOptimizationTool_b1090b]

Double-click the `VMwareOSOptimizationTool_b1090` to run the tool.

**Run the VMware OS Optimization Tool**

![Image of security warning dialog]

Click Run to continue to the tool.
Resize OSOT Window Size if needed

This tool may be hard to view on a small screen. You can resize the Main Console window by either Toggle Full-screen or Maximize the window buttons located at the top right of the window. You can also resize the Windows 10 desktop (W10-IC-01) window by clicking on View Fullscreen.

VMware OS Optimization Tool Features

This section describes some of the tool's graphical features.

- Tab Functions: A row of tabs provides the main functions of the OSOT:
  - **Analyze** - Analyze the registry entries, services, and scheduled tasks of the virtual machines that you want to optimize.
  - **History** - View optimization history, and roll back virtual machines to a pre-optimized state.
Remote Analysis - Browse a list of virtual machines in a remote desktop environment to analyze them.

Templates - Edit the built-in OSOT templates and save the changes to create your own OSOT templates.

References - Use the links provided to
  ▪ Download the latest version of the OSOT
  ▪ Provide feedback or submit your questions to the OSOT development team and the community
  ▪ Access third-party reference guides

OS Template Choices

The following built-in OSOT templates come with a list of modifications for a standard master image. Each OSOT template is an XML file that contains the coding for the optimizations. The default settings are the recommended values for optimizing your Windows operating system.

- Windows7 (built-in) - Optimizes Windows 7 desktops.
- Windows8 (built-in) - Optimizes all versions of Windows 8 desktops.
- Windows8_1 (built-in) - Optimizes all versions of Windows 8.1 desktops.
- Windows10_beta (built-in) - Optimizes all versions of Windows 10 desktops.
- Others listed above

Note: The OSOT does not support optimizing Windows Server 2008 or 2012 when those operating systems are used as single-session desktops.

Select Analyze

Click Analyze or Compatibility to produce a list of optimizations for the selected template. Click Analyze if you are not using Persona Management. Click Compatibility if you are using Persona Management (you will see the feature is selected by default). This excludes the Volume Shadow Copy Service from optimization, and ensures that Persona Management continues to function.

1. Click **Analyze** to start the analysis of the Windows 10 desktop.
Optimizations for the Windows 10 Desktop

The results from the Analysis should appear in a short time. Look under the Optimizations/Descriptions section highlighted above. Review the list of selected and deselected items to be optimized.

Optimization Importance

- **Mandatory** - You must apply the optimization to the item in the target system because of problems or issues that the OSOT has identified.
- **Recommended** - Even if the OSOT recommends an optimization, there can be valid reasons to not apply it. Determine if the recommended setting is applicable to your organization’s use cases.
- **Optional** - The OSOT has no recommendation regarding applying the optimization to the item in the target system. Determine if the setting is applicable to your organization’s use cases.
- **OK** - The item already has the proper value or setting and does not require any optimization.

The OSOT recommendations have icons to show Mandatory, Recommended, Optional and OK.
Those items without an icon are not settings that will be configured, but actions that will be performed when optimization is run. The action that will be performed is shown in the Description column.

**Analysis Summary**

![Analysis Summary Chart]

The Analysis Summary pane in the upper-right of the main OSOT window provides a graphical representation of the current optimization of the targeted system.

The graphical chart makes it easy to review how close the analyzed system is to being optimally configured for best performance in terms of the optimization importance.

**Export Results**

![Export Results Dialog Box]
Before you optimize the master image, you can export the analysis results to an HTML file for record keeping and to share with other personnel. You can also compare the analysis results with the post-optimization results.

The **Export Analysis Result** is in the bottom right corner of the screen.

**Optimize the Desktop**

![Image of VMware OS Optimization Tool interface]

We are not going to do every recommendation so let's choose one to see the results show Success.

1. Click the top check box to select all *then check again to deselect all*. You will only select one to optimize at this time to keep simple and save time in this lab environment.
2. Click on the first one "Advertising ID" to select only that optimization.
3. Click on Optimize
Optimize Success

Note that the Optimization was a SUCCESS for that one optimization.

Also a new tab is present that says Optimize.

History Tab

You can view the details of the optimization operations that you have performed.

Click the History tab

You can also roll back to the Pre-Optimized State. You can roll back any master image that you have optimized and reverse all optimizations that you made with the OSOT.
Note: It is not necessary in this step to rollback and arrow is merely pointing out where the button is located.

Close the VMware OS Optimization Tool

Click the X in the top right corner to close the optimization tool.

Sign out of the Desktop as Administrator
We need to sign out as the administrator to free up the desktop.

1. **Right-click** on the Window. Right-click will bring up the Shut down or sign out menu.
2. Select Shut down or sign out.
3. Click on Sign Out to disconnect as Administrator.

**Close the Console to the W10-IC-01 Desktop**

Close the browser tab to the W10-IC-01 desktop by clicking on the X on the tab with the W10-IC-01.
Conclusion

You have finished Module 1 on Optimizing Windows Images using the VMware Optimization Tool.

This module went over the OS Optimization Tool pointing out what to optimize, when to optimize and what the tool provides. It went over the OS Optimization Tool including an installation of the OS Optimization Tool and a run through of a Windows 10 desktop optimization.

You've finished Module 1

Congratulations on completing Module 1.

If you are looking for additional information on the VMware Optimization Tool, try one of these:

- Click on this link
- Or go to https://tinyurl.com/y7s3jwas
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

- **Module 2 - Management with Group Policies** (30 minutes) (Advanced) Using the Horizon Extras GPO Bundle to optimize and streamline your virtual environment's resources.
- **Module 3 - Management using PowerCLI for Horizon** (30 minutes) (Advanced) Making daily task and automation of Horizon functions easier with Horizon PowerCLI 6.5
- **Module 4 - Reporting with Log Insight iSIM** (15 minutes) (Advanced) Making log and events analysis easier and more intuitive with Log Insight. (iSIM)
- **Module 5 - vRealize Operations for Horizon (iSIM)** (30 minutes) (Intermediate) In-depth analysis and proactive investigation of your Horizon environment with vRealize Operations for Horizon. (iSIM)
How to End Lab and not continue on with the modules

You can continue on with the other modules above or you can end your lab completely by clicking on the **END** button.
Module 2 - Management with Group Policies (30 minutes)
Introduction

Use of the Horizon GPO Bundles pack is essential for any Horizon implementation. Most companies miss implementing these essential GPO's or do not have them properly set with the most important variables. We will cover the settings that can make a difference on a Horizon implementation along with how to get those ADMX files installed into the Horizon environment properly.

This module contains the following lessons:

- Horizon Group Policy Objects
- RDS Host Group Policies
- Group Policy Settings for User Environment Manager
- Group Policies Best Practices
Horizon Group Policy Objects

In this lesson we will use the Horizon GPO Bundle to show some of the Windows GPO templates for the Horizon environment.

Horizon 7.1 GPO Bundle

You can download the Horizon 7.1 GPO Bundle from your myvmware.com site.

https://my.vmware.com/web/vmware/downloads

Under Desktop & End-User Computing, select the VMware Horizon7 download, which includes the GPO Bundle.

The file is named VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip, wherex.x.xis the version and yyyyyyy is the build number. All ADM and ADMX files that provide group policy settings for View are available in this file.
1. From the **Main Console**, open an **Explorer** window and traverse to **C:\tools**.
2. In that folder you will see the **Vmware Horizon Extras Bundle** file named **VMware-Horizon-Extras-Bundle-4.4.0-5171611.zip**.

Note the Horizon Extras Bundle has already been extracted for use in this lab.

**Horizon Extras Bundle**

1. Note the **Horizon Extras Bundle** has already been extracted so no need to do so here.
2. **Double-click** on the folder **VMware-Horizon-Extras-Bundle-4.4.0-5171611**. This folder contains all the ADM, ADMX, and ADML files for the Horizon group policies.
Horizon Extras Bundle - ADM, ADMX, and ADML Files
As a best practice, use the ADMX versions versus the ADM group policies. As we move into the newer versions of Horizon, the ADM files may eventually be deprecated.

1. The en-US folder houses the group policy library files for the Horizon Extras Bundle, noted here as the english US versions and seen highlighted in step (5). Some important ADMX files are listed below:

2. **pcoip.admx** - The PCoIP ADMX template file contains policy settings related to the PCoIP display protocol. The individual settings for this template will be discussed in a later module.

3. **vdm_agent.admx** - The Horizon Agent Configuration ADMX template file contains policy settings related to the authentication and environmental components of Horizon Agent.

4. **vdm_blast.admx** - The VMware Blast group policy ADMX template file contains policy settings for the VMware Blast display protocol. The individual settings for this template will be discussed in a later module.

5. These are the individual english library files for the Horizon Extras Bundle.
Copy the ADMX Files

1. Hold the CTRL key down and using your mouse, click on the `pcoip.admx` ADMX file.
2. Hold the CTRL key down and using your mouse, click on the `vdm_agent.admx` ADMX file.
3. Hold the CTRL key down and using your mouse, click on the `vdm_blast.admx` ADMX file. Now right-mouse click on this file and select **Copy**. This will copy all three ADMX files.
Note: Depending on what device you are using, you may need to hold down the SHIFT key to select the multiple files.

Paste ADMX Files to Default Active Directory Policy Folder

1. In the location field in the Explorer window, type in `\corp.local\SYSVOL\corp.local\Policies\PolicyDefinitions` and press Enter.
2. You should see the default group policies for the domain here. Right-mouse click in this window and choose Paste from the sub-menu to copy the Horizon ADMX files into the location.

Copy Example ADMX Library Files to Default Active Directory Policy Library Folder

1. In the Explorer window location field, type in `C:\tools` and press Enter.
Go to the Horizon Extras Bundle Folder

Click on the Horizon Extras Bundle Folder

1. Click into the `VMware-Horizon-Extras-Bundle-4.4.0-5171611` folder again.

Copy the ADML Files

1. Click into the `en-US` folder.
2. Hold the CTRL key down and using your mouse, click on the `pcoip.adml` ADML file.

1. Click on the Horizon Extras Bundle Folder
2. Click into the `VMware-Horizon-Extras-Bundle-4.4.0-5171611` folder again.
3. Hold the CTRL key down and using your mouse, click on the `vdm_agent.adml` ADML file.
4. Hold the CTRL key down and using your mouse, click on the `vdm_blast.adml` ADML file. Now right-mouse click on this file and select **Copy**. This will copy all three ADML files.

*Note: Depending on what device you are using, you may need to hold down the SHIFT key to select the multiple files.*

**Paste the Horizon ADML Files**

1. In the location field in the **Explorer** window, type in `\corp.local\SYSVOL\corp.local\Policies\PolicyDefinitions\en-US` and press **Enter**.
2. You should see the default group policy libraries for the domain here. Right-mouse click in this window and choose **Paste** from the sub-menu to copy the Horizon ADML files into the location.

**Windows Group Policy Management Console Launch**
On the desktop of the Main Console, find and launch Group Policy Management. You may need to minimize the Explorer window.

**Windows Group Policy Management Console - New GPO**

1. Click on the arrow next to the Horizon Organizational Unit (OU) and verify that we have only the UEM group policy at this time.
2. Right-mouse click on the Horizon OU and click on Create a GPO in this domain, and link it here...
3. Name the New GPO Horizon or whatever name you wish.
4. Click OK to continue.
Open Group Policy Management Editor for Horizon

1. Right-click on the new Horizon GPO you just created.
2. Click Edit to open up the Group Policy Management Editor for that new Horizon GPO.
Horizon GPO - PCoIP Session Variables

1. Computer Configuration
2. Policies
3. Administrative Templates: Policy definitions
4. PCoIP Client Session Variables
5. PCoIP Session Variables

Configure PCoIP session encryption algorithms: Not configured
Configure PCoIP USB allowed and unallowed device rules: Not configured
Configure PCoIP virtual channels: Not configured
Configure PCoIP image quality levels: Not configured
Configure PCoIP event log verbosity: Not configured
Configure PCoIP event log cleanup by time in days: Not configured
Configure PCoIP event log cleanup by size in MB: Not configured
Configure SSL connections to satisfy Security Tools: Not configured
Configure SSL protocols: Not configured
Configure clipboard redirection: Not configured
Configure clipboard memory size on server (in kilobytes): Not configured
Configure frame rate vs image quality preference: Not configured
Configure the PCoIP session MTU: Not configured
Configure the PCoIP session bandwidth floor: Not configured
Configure the PCoIP session audio bandwidth limit: Not configured
Configure the PCoIP transport header: Not configured
Configure the TCP port to which the PCoIP Server binds and listens: Not configured
Configure the UDP port to which the PCoIP Server binds and listens: Not configured
Configure the maximum PCoIP session bandwidth: Not configured
Disable sending CAD when users press Ctrl+Alt+Del: Not configured
Enable access to a PCoIP session from a vSphere console: Not configured
Enable/disable audio in the PCoIP session: Not configured
Enable/disable microphone noise and DC offset filter in PCoIP session: Not configured
Filter Microsoft Office text data out of the incoming clipboard data: Not configured
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data: Not configured
Filter Microsoft Text Effects data out of the incoming clipboard data: Not configured
Filter Microsoft Office text data out of the outgoing clipboard data: Not configured
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data: Not configured
Filter Microsoft Text Effects data out of the outgoing clipboard data: Not configured
Filter Rich Text Format data out of the incoming clipboard data: Not configured
Filter Rich Text Format data out of the outgoing clipboard data: Not configured
Filter images out of the incoming clipboard data: Not configured
Filter images out of the outgoing clipboard data: Not configured
Filter text out of the incoming clipboard data: Not configured
Filter text out of the outgoing clipboard data: Not configured
Turn off Build-to-Lossless feature: Not configured
Turn on PCoIP user default input language synchronization: Not configured
Use alternate key for sending Secure Attention Sequence: Not configured
1. Within the Group Policy Management Editor for the Horizon Policy you just created, under Computer Configuration, click on the expansion box or arrow next to Policies to open the folder.
2. Click the expansion box or arrow next to Administrative Templates to open the folder.
3. Click the expansion box or arrow next to PCoIP Session Variables to open the folder.
4. Click on the folder icon for Overridable Administrator Defaults.
5. Note all the possible PCoIP Session Variables.

Horizon GPO - View Agent Variables

1. Within the Group Policy Management Editor for the Horizon Policy you just created, under Computer Configuration, click on the expansion box or arrow next to Policies to open the folder.
2. Click the expansion box or arrow next to Administrative Templates to open the folder.
3. Click on the folder icon for Agent Configuration.
4. Note all the possible View Agent Variables.
## Horizon GPO - BLAST Extreme Session Variables

### Diagram:

1. Computer Configuration
   - Policies
     - Software Settings
     - Windows Settings
     - Administrative Templates: Policy definitions

2. Agent Configuration
   - Agent Security
   - Control Panel
   - Network
   - PCoIP Client Session Variables
   - PCoIP Session Variables
   - Printers
   - Smartcard Redirection
   - System
   - True SSO Configuration
   - Unity Touch and Hosted Apps
   - View USB Configuration

3. VMware Blast

### Table:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio playback</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Cookie Cleanup Interval</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Image Quality</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>H.264</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>H.264 Quality</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>HTTP Service</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Max Session Bandwidth (kb/s)</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Max Frame Rate</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Max Session Bandwidth</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Min Session Bandwidth</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>PNG</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Screen Blanking</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>UDP Protocol</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter images out of the incoming clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter images out of the outgoing clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter Microsoft Chart and Smart Art data out of the incoming clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter Microsoft Text Effects data out of the incoming clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter Microsoft Text Effects data out of the outgoing clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter Microsoft Office text data out of the incoming clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter Microsoft Office text data out of the outgoing clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter Rich Text Format data out of the incoming clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter Rich Text Format data out of the outgoing clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter text out of the incoming clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Filter text out of the outgoing clipboard data</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Keyboard locale synchronization</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Clipboard memory size on server (in kibibytes)</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Configure clipboard redirection</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Configure file transfer</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>HTML Access printing</td>
<td>Not configured</td>
<td>No</td>
</tr>
</tbody>
</table>
1. Within the Group Policy Management Editor for the Horizon Policy you just created, under **Computer Configuration**, click on the expansion box or arrow next to **Policies** to open the folder.
2. Click the expansion box or arrow next to **Administrative Templates** to open the folder.
3. Click on the folder icon for **VMware Blast**.
4. Note all the possible **VMware Blast Variables**.

**Horizon GPO - Close Group Policy Management Editor**

1. In the **Group Policy Management Editor**, click on **File**.
2. Click on **Exit** to close the editor.
RDS Host Group Policies

When we are using RDS hosts, there are group policy settings that must be applied as per Using Remote Desktop Services Group Policies in Setting Up Desktop and Application Pools in View. To define these, we first need to copy the `vmware_rdsh.admx` and `vmware_rdsh_server.admx` files and the en-US folder (from the Horizon Extras Bundle zip file) to the `C:\Windows\PolicyDefinitions` folder on the Active Directory Domain Controller you are creating GPOs on.

**RDS Host Settings**

<table>
<thead>
<tr>
<th>SETTING</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the specified Remote Desktop license servers</td>
<td>Enabled (List license servers)</td>
</tr>
<tr>
<td>Hide notifications about RD Licensing problems that affect the RD Session Host server</td>
<td>Enabled</td>
</tr>
<tr>
<td>Set the Remote Desktop licensing mode</td>
<td>Enabled (Match mode of licenses)</td>
</tr>
<tr>
<td>Use mandatory profiles on the RD Session Host server</td>
<td>Enabled</td>
</tr>
<tr>
<td>Set path for Remote Desktop Services Roaming User Profile</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Windows Group Policy Management Console Launch**

On the desktop of the Main Console, find and launch Group Policy Management.
Windows Group Policy Management Console - New GPO

If you already created this Horizon Group Policy Object in the previous modules, please skip this section. The lab already has the \vmware_rdsh.admx and \vmware_rdsh_server.admx files installed so no need to install them into the domain.

1. Click on the arrow next to the Horizon Organizational Unit (OU) and verify that we have only the UEM group policy at this time.
2. Right-mouse click on the Horizon OU and click on Create a GPO in this domain, and link it here...
3. Name the New GPO Horizon or whatever name you wish.
4. Click OK to continue.
Horizon GPO - Remote Desktop Services Group Policies

In the next sections, **Remote Desktop Services Group Policies** are discussed, but these are just a sample of the group policies available. For an extended list of the **Remote Desktop Services Group Policies**, please refer to our Horizon 7 online documentation: [Documentation Center for VMware Horizon 7 version 7.1](#)

1. Right-click on the **Horizon** GPO you created.
2. Click **Edit** to open up the Group Policy Management Editor for that **Horizon** GPO.

**Horizon GPO - RDS Application Compatibility Settings**

![Diagram of Group Policy Management Editor]

1. **Computer Configuration**
2. **Policies**
3. **Administrative Templates**
4. **Windows Components**
1. Within the Group Policy Management Editor for the Horizon Policy, under Computer Configuration, click on the expansion box or arrow next to Policies to open the folder.
2. Click the expansion box or arrow next to Administrative Templates to open the folder.
3. Click the expansion box or arrow next to Windows Components to open the folder.

RDS Application Compatibility Settings

1. Scroll down and click the expansion box or arrow next to Remote Desktop Services to open the folder.
2. Click the expansion box or arrow next to Remote Desktop Session Host to open the folder.
3. Click on the folder icon for Application Compatibility.
4. Note all the possible RDS Application Compatibility Settings.
Horizon GPO - RDS Connection Settings

1. Within the Group Policy Management Editor for the Horizon Policy, under Computer Configuration, click on the expansion box or arrow next to Policies to open the folder.
2. Click the expansion box or arrow next to Administrative Templates to open the folder.
3. Click the expansion box or arrow next to Windows Components to open the folder.
RDS Connection Settings

1. Scroll down and click the expansion box or arrow next to **Remote Desktop Services** to open the folder.
2. Click the expansion box or arrow next to **Remote Desktop Session Host** to open the folder.
3. Click on the folder icon for **Connections**.
4. Note all the possible **RDS Connections Settings**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Allowance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic reconnection</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Allow users to connect remotely by using Remote Desktop Services</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Deny logoff of an administrator logged in to the console session</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Configure keep-alive connection interval</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Limit number of connections</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Suspend user sign-in to complete app registration</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Set rules for remote control of Remote Desktop Services</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Select network detection on the server</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Select RDP transport protocols</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Restrict Remote Desktop Services users to a single Remote Desktop</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Allow remote start of unlisted programs</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Turn off Fair Share CPU Scheduling</td>
<td>Not configured</td>
<td>No</td>
</tr>
</tbody>
</table>
Horizon GPO - RDS Device and Resource Redirection Settings

1. Within the Group Policy Management Editor for the Horizon Policy, under Computer Configuration, click on the expansion box or arrow next to Policies to open the folder.
2. Click the expansion box or arrow next to Administrative Templates to open the folder.
3. Click the expansion box or arrow next to Windows Components to open the folder.
1. Scroll down and click the expansion box or arrow next to Remote Desktop Services to open the folder.
2. Click the expansion box or arrow next to Remote Desktop Session Host to open the folder.
3. Click on the folder icon for Device and Resource Redirection.
4. Note all the possible RDS Device and Resource Redirection Settings.
Horizon GPO - RDS Printer Redirection Settings

1. Within the Group Policy Management Editor for the Horizon Policy, under Computer Configuration, click on the expansion box or arrow next to Policies to open the folder.
2. Click the expansion box or arrow next to Administrative Templates to open the folder.
3. Click the expansion box or arrow next to Windows Components to open the folder.

RDS Printer Redirection Settings

- Do not set default client printer to be default printer in a sess... Not configured No
- Do not allow client printer redirection Not configured No
- Use Remote Desktop Easy Print printer driver first Not configured No
- Specify RD Session Host server fallback printer driver behavior Not configured No
- Redirect only the default client printer Not configured No
1. Scroll down and click the expansion box or arrow next to **Remote Desktop Services** to open the folder.
2. Click the expansion box or arrow next to **Remote Desktop Session Host** to open the folder.
3. Click on the folder icon for **Printer Redirection**.
4. Note all the possible **RDS Printer Redirection Settings**.

**Horizon GPO - RDS Remote Session Environment Settings**

1. Within the Group Policy Management Editor for the Horizon Policy, under **Computer Configuration**, click on the expansion box or arrow next to **Policies** to open the folder.
2. Click the expansion box or arrow next to **Administrative Templates** to open the folder.
3. Click the expansion box or arrow next to **Windows Components** to open the folder.
1. Scroll down and click the expansion box or arrow next to **Remote Desktop Services** to open the folder.

2. Click the expansion box or arrow next to **Remote Desktop Session Host** to open the folder.

3. Click on the folder icon for **Remote Session Environment**.

4. Note all the possible **RDS Remote Session Environment Settings**.

**RDS Remote Session Environment Settings**

- **RemoteFX for Windows Server 2008 R2**
  - Limit maximum color depth: Not configured
  - Enforce Removal of Remote Desktop Wallpaper: Not configured
  - Limit maximum display resolution: Not configured
  - Limit number of monitors: Not configured
  - Remove "Disconnect" option from Shut Down dialog: Not configured
  - Remove Windows Security item from Start menu: Not configured
  - Use advanced RemoteFX graphics for RemoteApp: Not configured
  - Configure compression for RemoteFX data: Not configured
  - Configure image quality for RemoteFX Adaptive Graphics: Not configured
  - Enable RemoteFX encoding for RemoteFX clients designed f... Not configured
  - Configure RemoteFX Adaptive Graphics: Not configured
  - Start a program on connection: Not configured
  - Always show desktop on connection: Not configured
  - Allow desktop composition for remote desktop sessions: Not configured
  - Do not allow font smoothing: Not configured
  - Use the hardware default graphics adapter for all Remote De... Not configured
1. Within the Group Policy Management Editor for the Horizon Policy, under Computer Configuration, click on the expansion box or arrow next to Policies to open the folder.
2. Click the expansion box or arrow next to Administrative Templates to open the folder.
3. Click the expansion box or arrow next to Windows Components to open the folder.

RDS Session Time Limits

- Set time limit for disconnected sessions
- Set time limit for active but idle Remote Desktop Services sessions
- Set time limit for active Remote Desktop Services sessions
- End session when time limits are reached
- Set time limit for logoff of RemoteApp sessions

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not configured</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Not configured</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Not configured</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Not configured</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Not configured</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
1. Scroll down and click the expansion box or arrow next to **Remote Desktop Services** to open the folder.
2. Click the expansion box or arrow next to **Remote Desktop Session Host** to open the folder.
3. Click on the folder icon for **Session Time Limits**.
4. Note all the possible **RDS Session Time Limits**.

### Horizon GPO - Close Group Policy Management Editor

1. In the **Group Policy Management Editor**, click on **File**.
2. Click on **Exit** to close the editor.
Group Policy Settings for User Environment Manager

The following instructions are taken from the User Environment Manager Administrators Guide. Refer to this guide for more details on Group Policy settings.

UEM - Group Policy Settings

You configure FlexEngine by creating an Active Directory Group Policy Object (GPO). You use the User Environment Manager administrative templates that are provided in the download package.

If you want to provide different FlexEngine configurations, you can use multiple GPOs. For example, you can manage multiple User Environment Manager environments such as test and production.

GPO Mandatory Settings

After you deploy FlexEngine to the client devices, you must configure FlexEngine to run during the Windows logon and logoff processes.

FlexEngine runs during Windows logon to get all the settings for the client device and apply them as soon as the user logs in.

You can configure FlexEngine in the following ways to run during Windows logon process:

- By setting Group Policy Run FlexEngine as Group Policy Extension.
- By configuring a logon script in Group Policy. Use this method if you prefer to write a logon script.
FlexEngine runs again during Windows logoff to save all the settings for the client device to the profile archives share. To run FlexEngine during Windows logoff, configure a logoff script in Group Policy.

You must also configure the path to the configuration share and the profile archives share in the GPO.

**GPO Optional Settings**

The two most common optional GPO settings for User Environment Manager are as follows:

- Use the Profile Archives Backups setting to configure the location and number of backups. Users can restore their settings from a backup using the Self-Support Tool or help desk personnel can do this by using the Helpdesk Support tool.
- Use the FlexEngine Logging setting to configure the location and filename of the log file, the level of log detail, and the maximum file size. The log file helps with troubleshooting.

**Windows Group Policy Management Console Launch**

On the desktop of the Main Console, find and launch Group Policy Management.
Windows Group Policy Management Console - Open UEM Group Policy Object

The lab already has a UEM Group Policy Object and the VMware UEM.admx and VMware UEM FlexEngine.admx ADMX templates files installed so no need to install them into the domain.

1. Click on the arrow next to the Horizon Organizational Unit (OU).
2. Right-mouse click on the UEM Policy and click on Edit...
1. Within the Group Policy Management Editor for the Horizon Policy, under User Configuration, click on the expansion box or arrow next to Policies to open the folder.

2. Click the expansion box or arrow next to Administrative Templates to open the folder.

3. Click the expansion box or arrow next to VMware UEM to open the folder.

4. Click on the folder icon for FlexEngine.

**FlexEngine Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application blocking logging to the Windows event log</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Certificate support for mandatory profiles</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>DirectFlex - advanced settings</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>FlexEngine logging to the Windows event log</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Flex config files</td>
<td>Enabled</td>
<td>No</td>
</tr>
<tr>
<td>Run FlexEngine as Group Policy Extension</td>
<td>Enabled</td>
<td>No</td>
</tr>
<tr>
<td>FlexEngine logging</td>
<td>Enabled</td>
<td>No</td>
</tr>
<tr>
<td>Paths unavailable at logon</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Profile archive backups</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>FlexEngine archives</td>
<td>Enabled</td>
<td>No</td>
</tr>
<tr>
<td>FlexEngine refresh settings</td>
<td>Enabled</td>
<td>No</td>
</tr>
<tr>
<td>Prevent access to VMware UEM Self-Support</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Show VMware UEM logon and logoff progress information</td>
<td>Not configured</td>
<td>No</td>
</tr>
<tr>
<td>Sito-specific Flex config files</td>
<td>Not configured</td>
<td>No</td>
</tr>
</tbody>
</table>

1. Note all the possible User Environment Manager FlexEngine.
Configuring the appropriate User Environment Manager Group Policy settings is important. At a minimum, the following must be set:

2. **Flex config Files**- Location of the User Environment Manager configuration share

3. **Run FlexEngine as a Group Policy Extension**- This is what enables the FlexEngine agent. Alternatively, it can be called from a logon script.

4. **Profile archives**- Location of the User Environment Manager user profile share.

### UEM Log off Script

1. **A logoff script** must be defined for User Environment Manager to save settings on logoff. The syntax of the logoff script should be:

   ```cmd
   "C:\Program Files\Immidio\FlexProfiles\FlexEngine.exe" -s
   ```
Group Policies Best Practices

Group Policy (GPO) can be used in a variety of ways to control and configure both Horizon components and also standard Windows settings. These policies are normally applied to the user or the computer Active Directory account depending on where they are located in Active Directory. In a Horizon environment it is typical to set specific user policy settings for the specific Horizon session only when a user connects to it. We also want to have user accounts processed separately from computer accounts with GPOs. This is where the loopback policy is widely used in any GPO that also needs to configure user settings. This is particularly important with User Environment Manager. User Environment Manager only applies user settings, so if the User Environment Manager GPOs are applied to computer objects, loopback processing must be enabled.

OU GPO Best Practices

Here are some best practices Group Policies

- Re-use GPOs.
- Separate OUs for users and computers.
- Ensure that each GPO is enabled or disabled for Computer and User settings.
- Group similar settings into one GPO.
- Monolithic and functional GPO.
  - Monolithic GPOs contain settings for many different areas and are quite large.
  - All settings in one place; should be used for generic settings that apply to all users or computers.
  - Functional GPOs contain a limited set of settings for a specific area.
  - Smaller GPOs that facilitate settings being defined for particular users or VMs.
  - Link the GPOs to the OU structure (or site), and then use Security Groups to selectively apply these GPOs to particular users or computers.
  - Use loopback replace to ensure that only settings for the VMs OU are applied to the session. Below is a list of group policy settings that would typically be applied (this is not an exhaustive list). Most other settings will be applied through User Environment policies. As part of the download of Horizon there is a View GPO Bundle ZIP file that contains a set of group policy templates to assist in defining these and other GPO settings.
Common GPO Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Configuration/Policies/Administrative Templates/System/Group Policy/</td>
<td></td>
</tr>
<tr>
<td>Configure user Group Policy/loopback processing mode</td>
<td>Enabled Mode = Replace</td>
</tr>
<tr>
<td>Configure Logon Script Delay</td>
<td>Disabled</td>
</tr>
<tr>
<td>Computer Configuration/Policies/Administrative Templates/System/Logon/</td>
<td></td>
</tr>
<tr>
<td>Show first sign-in animation</td>
<td>Disabled</td>
</tr>
<tr>
<td>Always wait for the network at computer startup and logon</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

This table lists some of the common GPO settings you should be aware of.

Desktop Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Configuration/Policies/Administrative Templates/System/User Profiles/</td>
<td></td>
</tr>
<tr>
<td>Set roaming profile path for all users logging onto this computer</td>
<td>Enabled (Specify the mandatory network share path).</td>
</tr>
</tbody>
</table>

This table shows a desktop setting to be aware of.

User Configuration Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Configuration/ Policies/Administrative Templates/Start Menu and Taskbar/</td>
<td></td>
</tr>
<tr>
<td>Remove and prevent access to the Shut Down, Restart, Sleep and Hibernate commands</td>
<td>Enabled</td>
</tr>
<tr>
<td>Add Logoff to the Start Menu</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Configuration/ Policies/Administrative Templates/Windows Components/Internet Explorer/</td>
<td></td>
</tr>
<tr>
<td>Automatically activate newly installed add-ons</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Configuration/ Policies/Administrative Templates/Windows Components/Internet Explorer/Internet Control Panel/ Security Page/</td>
<td></td>
</tr>
<tr>
<td>Site to Zone Assignment List • Zone assignments</td>
<td>Enabled</td>
</tr>
<tr>
<td>Example: <a href="https://workspace.vmweuc.com">https://workspace.vmweuc.com</a></td>
<td></td>
</tr>
<tr>
<td>Example: \vmweuc.com\files\</td>
<td></td>
</tr>
</tbody>
</table>
There are various settings that can be used to optimize the user experience while protecting the system. These are a few basic, initial settings that would normally be applied. Note that as these are user settings, this will require the use of the loopback processing setting.

**PCoIP GPO Best Practice Settings & Tuning**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the maximum PCoIP session bandwidth</td>
<td>Specifies the maximum bandwidth, in kilobits per second, in a PCoIP session. The bandwidth includes all imaging, audio, virtual channel, USB, and control PCoIP traffic.</td>
<td></td>
</tr>
<tr>
<td>Turn off Build-to-Lossless feature</td>
<td>Builds the image to a completely lossless state, pixel perfect image. Only required in special uses cases. Disabling this can reduce bandwidth demands greatly.</td>
<td></td>
</tr>
<tr>
<td>PCoIP Maximum Image Quality</td>
<td>A lower initial maximum image quality will reduce the bandwidth required back at the expense of image quality.</td>
<td></td>
</tr>
<tr>
<td>PCoIP Minimum Image Quality</td>
<td>Trades off display image quality with display frame update</td>
<td></td>
</tr>
<tr>
<td>Maximum Frame Rate</td>
<td>Set a limit on the display update rate. Can reduce bandwidth but as the cost of smooth motion</td>
<td></td>
</tr>
<tr>
<td>Configure the PCoIP session audio bandwidth limit</td>
<td>Configures audio compressing. The resulting audio bandwidth will be near or below the limit.</td>
<td></td>
</tr>
</tbody>
</table>

Again, these settings are sometimes overlooked, specifically for PCoIP. The list, as mentioned, is not exhaustive but does cover some use cases. Your mileage may vary.

**Configure the maximum PCoIP session bandwidth**

Set this value to the overall capacity of the link to which your endpoint is connected, taking into consideration the number of expected concurrent PCoIP sessions. For example, with a single-user VDI configuration (a single PCoIP session) that connects through a 4Mbit/s Internet connection, set this value to 4Mbit, or 10% less than this value to leave some allowance for other network traffic. When you expect multiple concurrent PCoIP sessions to share a link, comprising either multiple VDI users or an RDS configuration, you might want to adjust the setting accordingly. However, lowering this value will restrict the maximum bandwidth for each active session.

Setting this value prevents the agent from attempting to transmit at a higher rate than the link capacity, which would cause excessive packet loss and a poorer user experience. This value is symmetric. It forces the client and agent to use the lower of the two values that are set on the client and agent side. For example, setting a 4Mbit/s maximum bandwidth forces the agent to transmit at a lower rate, even though the setting is configured on the client.
When this setting is disabled or not configured on an endpoint, the endpoint imposes no bandwidth constraints. When this setting is configured, the setting is used as the endpoint's maximum bandwidth constraint in kilobits per second.

**Turn off Build-to-Lossless feature**

If this setting is enabled or not configured, the build-to-lossless feature is turned off, and images and other desktop and application content are never built to a lossless state. In network environments with constrained bandwidth, turning off the build-to-lossless feature can provide bandwidth savings.

If this setting is disabled, the build-to-lossless feature is turned on. Turning on the build-to-lossless feature is recommended in environments that require images and other desktop and application content to be built to a lossless state.

**PCoIP Maximum Image Quality**

Use the Maximum Initial Image Quality value to reduce the network bandwidth peaks required by PCoIP by limiting the initial quality of the changed regions of the display image. You can specify a value between 30 and 100. The default value is 80. A lower value reduces the image quality of content changes and decreases peak bandwidth requirements. A higher value increases the image quality of content changes and increases peak bandwidth requirements. Unchanged regions of the image progressively build to a lossless (perfect) quality regardless of this value. A value of 80 or lower best utilizes the available bandwidth.

**PCoIP Minimum Image Quality**

Use the Minimum Image Quality value to balance image quality and frame rate for limited-bandwidth scenarios. You can specify a value between 30 and 100. The default value is 40. A lower value allows higher frame-rates, but with a potentially lower quality display. A higher value provides higher image quality, but with potentially lower frame rates when network bandwidth is constrained. When network bandwidth is not constrained, PCoIP maintains maximum quality regardless of this value.

**Maximum Frame Rate**

Use the Maximum Frame Rate value to manage the average bandwidth consumed per user by limiting the number of screen updates per second. You can specify a value between 1 and 120 frames per second. The default value is 30. A higher value can use more bandwidth but provides less jitter, which allows smoother transitions in changing images such as video. A lower value uses less bandwidth but results in more jitter.

**Configure the PCoIP session audio bandwidth limit**

The audio processing monitors the bandwidth used for audio. The processing selects the audio compression algorithm that provides the best audio possible, given the current bandwidth utilization. If a bandwidth limit is set, the processing reduces quality by changing the compression algorithm selection until the bandwidth limit is reached. If
minimum quality audio cannot be provided within the bandwidth limit specified, audio is disabled.

To allow for uncompressed high quality stereo audio, set this value to higher than 1600 kbit/s. A value of 450 kbit/s and higher allows for stereo, high-quality, compressed audio. A value between 50 kbit/s and 450 kbit/s results in audio that ranges between FM radio and phone call quality. A value below 50 kbit/s might result in no audio playback.

This setting applies to Horizon Agent only. You must enable audio on both endpoints before this setting has any effect.

In addition, this setting has no effect on USB audio.

**BLAST Extreme GPO Best Practice Settings & Tuning**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Session Bandwidth</td>
<td>With this policy setting, you can set the maximum session bandwidth (in kilobits) that is reserved for the Blast protocol.</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>Min Session Bandwidth</td>
<td>With this policy setting, you can set the minimum session bandwidth (in kilobits) that is reserved for the Blast protocol.</td>
<td>256 kbps</td>
</tr>
<tr>
<td>Image Quality: Low JPEG Quality</td>
<td>When this setting is enabled, you can change the low-quality JPEG settings to different values. The actual JPEG quality levels used at low settings are individually configurable as numbers between 0 and 100.</td>
<td>25</td>
</tr>
<tr>
<td>Image Quality: Mid JPEG Quality</td>
<td>When this setting is enabled, you can change the mid-quality JPEG settings to different values. The actual JPEG quality levels used at mid settings are individually configurable as numbers between 0 and 100.</td>
<td>35</td>
</tr>
<tr>
<td>Image Quality: High JPEG Quality</td>
<td>When this setting is enabled, you can change the high-quality JPEG settings to different values. The actual JPEG quality levels used at high settings are individually configurable as numbers between 0 and 100.</td>
<td>90</td>
</tr>
<tr>
<td>Maximum Frame Rate</td>
<td>Set a limit on the display update rate. Can reduce bandwidth but as the cost of smooth motion</td>
<td>30</td>
</tr>
<tr>
<td>H.264 Quality</td>
<td>These settings control the image quality of the remoted display when using H.264 compression.</td>
<td>QP Maximum = 36, QP Minimum = 10</td>
</tr>
</tbody>
</table>

Again, these settings are sometimes overlooked, specifically for BLAST Extreme. You may find some new settings in this section that will greatly enhance your BLAST...
Extreme experience. The list, as mentioned, is not exhaustive but does cover some use cases. Your mileage may vary.

**Max Session Bandwidth**

Specifies the maximum bandwidth, in kilobits per second (kbps), for a VMware Blast session. The bandwidth includes all imaging, audio, virtual channel, USB, and VMware Blast control traffic.

**Min Session Bandwidth**

Specifies the minimum bandwidth, in kilobits per second (kbps), that is reserved for a VMware Blast session.

**Image Quality: Low JPEG Quality**

The low-quality settings are for areas of the screen that change often, for example, when scrolling occurs.

**Image Quality: Mid JPEG Quality**

The mid-quality setting is an attempt at a balanced quality for images.

**Image Quality: High JPEG Quality**

The high-quality settings are for areas of the screen that are more static, resulting in a better image quality.

**Maximum Frame Rate**

Specifies the maximum rate of screen updates. Use this setting to manage the average bandwidth that users consume.

**H.264 Quality**

Specifies the image quality for the remote display configured to use H.264 encoding. You can specify the minimum and maximum quantization values that determine how much an image is controlled for lossless compression. You can specify a minimum quantization value for the best image quality. You can specify a maximum quantization value for the lowest image quality. For the best image quality, set the quantization values to within +5 or -5 of the available range of values.
Conclusion

You have finished Module 2 on Management with Group Policies.

You've finished Module 2

Congratulations on completing Module 2.

If you are looking for additional information on the managing Horizon 7 environments using GPO's, try one of these:

- Click on this link
- Or go to User Environment Manager Online Documentation
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

- **Module 3 - Management using PowerCLI for Horizon** (30 minutes) (Advanced) Making daily tasks and automation of Horizon functions easier with Horizon PowerCLI 6.5
- **Module 4 - Reporting with Log Insight iSIM** (15 minutes) (Advanced) Making log and events analysis easier and more intuitive with Log Insight. (iSIM)
- **Module 5 - vRealize Operations for Horizon (iSIM)** (30 minutes) (Intermediate) In-depth analysis and proactive investigation of your Horizon environment with vRealize Operations for Horizon. (iSIM)

How to End Lab Completely and not continue on with other modules
You can continue on with the other modules or you can end your lab completely just click on the **END** button.
Module 3 - Management using PowerCLI for Horizon (30 Minutes)
Introduction

Automation and programmability are important when designing and maintaining a Horizon environment. We will show how Horizon PowerCLI 6.5 can help automate daily tasks and management.

This module contains the following lessons:

- What is PowerCLI 6.5 Horizon Module?
- Installing PowerCLI 6.5 Horizon Module
- Sample Scripts in PowerCLI 6.5 Horizon Module
Automating VMware Horizon 7 with VMware PowerCLI 6.5

With VMware PowerCLI 6.5 Release 1, the automation of VMware Horizon 7 matures and we get integrated PowerShell support for the View component of Horizon 7 built into VMware PowerCLI. We have a proper Horizon 7 module that is distributed and ships with the core VMware PowerCLI installation.

VMware PowerCLI 6.5 Overview

VMware PowerCLI contains modules of cmdlets based on Microsoft PowerShell for automating vSphere, VMware Site Recovery Manager, vSphere Automation SDK, vCloud Director, vCloud Air, vSphere Update Manager, vRealize Operations Manager, and VMware Horizon administration. VMware PowerCLI provides a PowerShell interface to the VMware product APIs.
Even though the Horizon 7 module contains only two cmdlets, they are extremely useful. These cmdlets allow you to connect and disconnect from the View API service. Importantly, this functionality provides a convenient way to access the full View API and the capabilities normally only available through the Horizon Administrator console.

Unlike previous VMware PowerCLI for Horizon 7 implementations, you can now connect and run VMware PowerCLI scripts for Horizon 7 from remote workstations or servers, such as an administrator’s desktop, using different credentials. You can also easily build federated scripts across VMware assets. For example, you can write a script to get a list of datastores from a vCenter Server inventory and use that information to select the best datastores on which to create a pool.

Three Benefits of PowerCLI Horizon 7 Module

- **PowerCLI**
  - Built-in cmdlets
    - Connect-HVServer
    - Disconnect-HVServer

- **View API**
  - Direct access to full View API
  - Documentation online

- **Advanced Functions**
  - Cmdlets written in PowerShell
  - Invoke View API functions easily
The benefits of PowerCLI for Horizon 7 are listed above.

**View API**

To accompany the new VMware PowerCLI module, VMware is happy to announce the release of public [View API Reference Documentation](#) for Horizon 7 and access to the full public View API. The View API is a web service and is available from any Horizon Connection Server within a Horizon Pod. The View API is used by the Horizon Administrator console for configuration, administration, and monitoring, so we are now exposing programmatic access to all the functionality available in the console.

To make exploring the data objects and methods of interacting with them easier, VMware has created a new [Developer Center online API Explorer](#), a unified interface for all API documentation across the VMware stack.

**Advanced Functions**

To get you started quickly, the Horizon 7 team has put together a set of functions that cover common operations. These functions allow you to easily interact with pools, farms, and desktops without having to write scripts from scratch. Be sure to visit the [VMware PowerCLI Community Repository](#) site on GitHub periodically to get new functions and consider contributing your own.

**Install VMware PowerCLI**

The above slide outlines the installation for PowerCLI.
Prerequisites

Before installing and running PowerCLI, verify that you have installed the required software on the same machine.

- vSphere 5.5 or higher
- Horizon 7.0.2 or higher
- PowerCLI 6.5 Release 1

Getting Started

1. Download the VMware PowerCLI 6.5 R1 installer and run the installation wizard.
2. As part of the installation, you are prompted to change the ExecutionPolicy of PowerShell.
3. Launch PowerShell (run as Administrator), and run the following command: Set-ExecutionPolicy RemoteSigned

Importing the Horizon API Module

Providing you have PowerCLI 6.5 R1 installed, you should also have the new Horizon API module (VMware.VimAutomation.HorizonView). You can check this using the following:

Get-Module –ListAvailable VMware*Horizon*

Next, import the module so we can start using it!

Get-Module –ListAvailable VMware*Horizon* | Import-Module

Notice how the same command was used? By piping the object from the previous command (VMware.VimAutomation.HorizonView) the Import-Module action was taken.

If you already know the name of the module you want to import, you could also run Import-Module VMware.VimAutomation.HorizonView.

Establish Connection to Horizon

Now we have the Horizon module imported, we can use the Connect-HVServer cmdlet to establish a connection to the Horizon API service of the Horizon Connection server.
Connect-HVServer -server cs1.domain.local -User user -Password password -Domain domain.local

If it has authenticated successfully, you should now have a connection to your Horizon Connection server.

**Note**: A preference that may be implemented is substitute the username, password, domain and Connection server with variables.

Please note this step is meant as a reference and not to be implemented in the lab.

### Listing the Horizon API services with ExtensionData

The Horizon API contains a long list of services we can use, contained in the ExtensionData property. We will add this to a variable `$hzServices` that we can use in our script.

```
$hzServices = $Global:DefaultHVServer.\ExtensionData
```

Now enter `$hzServices` and you’ll see all of the services available with the Horizon API module!

Please note this step is meant as a reference and not to be implemented in the lab.

### Using Get-Member to List Methods and Properties of an Object

Ok, so you can see a bunch of services using the `$hzServices` variable. Let’s pick one at random and see what we can actually do with it: `ConnectionServer`

```
$hzServices.ConnectionServer | Get-Member
```

Please note this step is meant as a reference and not to be implemented in the lab.

Please note this step is meant as a reference and not to be implemented in the lab.
Note: The Get-Member cmdlet lists the Methods and Properties of an object. In this example our object is ConnectionServer.

### Listing Horizon Connection Servers

We know what we can do with ConnectionServer, now let’s use our example to list the Connection servers in our environment using the ConnectionServer_List method.

```powershell
$hzServices.ConnectionServer.ConnectionServer_List()
```

Oh wait! All that did is list some more objects. Actually this is very cool, we can see what our MessageSecurity is set to, or take a look at the backup data. For now, let’s just list our Connection servers, so the General object is worth looking at.

```powershell
$hzServices.ConnectionServer.ConnectionServer_List().General
```

Now you should see a list of your Connection servers, along with the Name, ServerAddress, Version and a bunch of other useful data.
**Note:** In this example we are using our $hzServices variable with the ConnectionServer object and ConnectionServer_List method.

Please note this step is meant as a reference and not to be implemented in the lab.

**Using Variables**

```powershell
$hzUser = "Administrator"
$hzPass = "VMware1!"
$hzDomain = "domain.local"
$hzConn = "connect01.domain.local"
```

As we drill down into an objects Methods and Properties, your scripts can often benefit from using variables. As you can see in the previous examples, I used $hzServices to store the ExtensionData ($Global:DefaultHV Servers.ExtensionData). We can make further use of variables to make our scripts a little easier to work with.

Looking back at Step 5, we could add a variable that contains our Connection servers.

```powershell
$CServers = $hzServices.ConnectionServer.ConnectionServer_List().General
```

Now using $CServers on it's own will simply list our Connection servers without having to type out the entire command. You can then drill down further. Try $CServers.Name and see what happens!

When working with scripts, I also prefer to assign variables to information such as the username, password, domain, and so on.

Please note this step is meant as a reference and not to be implemented in the lab.
Example Script

```powershell
# User Configuration
$hzUser = "Administrator"
$hzPass = "VMware1!"
$hzDomain = "domain.local"
$hzConn = "connect01.domain.local"

# Import the Horizon module
Import-Module VMware.VimAutomation.HorizonView

# Establish connection to Connection Server
$hzServer = Connect-HVServer -server $hzConn -User $hzUser -Password $hzPass -

# Assign a variable to obtain the API Extension Data
$hzServices = $Global:DefaultHVServer.ExtensionData

# Retrieve Connection Server Health metrics

# Display ConnectionData (Usage stats)
$hzHealth.ConnectionData
```

This basic script takes everything that we have learned here. It retrieves the Horizon usage statistics, which is the same metrics listed under View Configuration > Product Licensing and Usage. Service providers can use this script or incorporate it with their existing scripts to automate the reporting of Horizon usage.

Please note this step is meant as a reference and not to be implemented in the lab.
Conclusion

You have finished Module 3 on Management using PowerCLI for Horizon.

You've finished Module 3

Congratulations on completing Module 3.

If you are looking for additional information on the managing Horizon 7 environments using PowerCLI, try one of these:

- Click on this link
- Or go to https://tinyurl.com/y9534qc4
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

- **Module 4 - Reporting with Log Insight **(iSIM)(15 minutes) (Advanced) Making log and events analysis easier and more intuitive with Log Insight. (iSIM)
- **Module 5 - vRealize Operations for Horizon **(iSIM)(30 minutes) (Intermediate) In-depth analysis and proactive investigation of your Horizon environment with vRealize Operations for Horizon. (iSIM)

How to End Lab and not continue on to the other modules

You can continue on to the other modules or you can end your lab completely just click on the **END** button.
Module 4 - Reporting with vRealize Log Insight (15 minutes)
Introduction

Log file and event logging research can be tedious work. With Log Insight, we will show how to gain visibility into the Horizon environment’s logs and events and do so from an intuitive interface.
vRealize Log Insight and Horizon

We will highlight the main features of the vRealize Log Insight tool and the Horizon View specific capabilities.

vRealize Log Insight Video

Please see this video created by our End User ComputingTestDrive Team for this vRealize Log Insight walkthrough:

https://youtu.be/AIf5jc32KVo

vRealize Log Insight Overview

VMware vRealize Log Insight delivers heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics and broad third-party extensibility, providing deep operational visibility and faster troubleshooting.

vRealize Log Insight Key Benefits

- Rapid troubleshooting and root cause analysis, within seconds. In recent internal testing, Log Insight was found to be three times faster than leading solution in query test across terabytes of data.
- Intuitive and easy-to-use, graphical interface for simple interactive searches as well as deep analytical queries.
- Extensible across physical, virtual and cloud environments, enables administrators to connect to everything in their environment, e.g., OS, apps, storage, network devices, providing a single location to collect, store, and analyze logs at scale.
- Built-in knowledge and native support for VMware vSphere, making Log Insight the best solution for VMware environments.

vRealize Log Insight Key Capabilities

- Integrates with VMware vRealize Operations to bring unstructured and structured data together, for enhanced end-to-end operations management.
- Easily troubleshoot Horizon View configuration and user experience issues.
- Monitor and alert on critical conditions impacting your Horizon View environment.
- Quickly identify trends and emerging utilization problem.
- VMware and third-party extensions available on VMware Solution Exchange.
- Built-in knowledge of vSphere, VMware Horizon with View, vRealize Operations and vRealize Automation.
• Collects and analyzes all types of machine generated log data, e.g., application logs, network traces, configuration files, messages, performance data, system state dumps, and more.
• Automatically chooses the best visualization for your data, saving you time.
• Automated alerts to pinpoint and track potential issues before they arise.
• Adds structure to unstructured log data, enabling administrators to troubleshoot quickly, without needing to know the data beforehand.
• Delivers real-time monitoring, search, and log analytics, coupled with a dashboard for stored queries, reports, and alerts, enabling correlation of events across the IT environment.
• Provides machine learning-based Intelligent Grouping, which groups related data together to enable high performance searching for faster troubleshooting across physical, virtual, and cloud environments.

vRealize Log Insight Deeper Dive

You can visit other labs that talk about vRealize Log Insight in more detail. These labs are part of our Software Defined Data Center track and Cloud Management Platform. The focus of these labs is on the entire data center with vRealize Log Insight and not just Horizon and Desktops.

• HOL-1806-01-CMP - vvRealize Suite - Getting Started
• HOL-1801-03-CMP - vRealize Suite Standard - Manage the SDDC
Conclusion

You have finished Module 4 on Reporting with vRealize Log Insight

You've finished Module 4

Congratulations on completing Module 4.

If you are looking for additional information on Reporting with vRealize Log Insight, try one of these:

- Click on this link
- Or go to https://tinyurl.com/yddcvyxp
- Or use your smart device to scan the QRC Code.

Proceed to the vRealize Operations for Horizon (iSIM) module below or return to previous modules in this lab.

- **Module 5 - vRealize Operations for Horizon (iSIM)** (30 minutes)
  (Intermediate) In-depth analysis and proactive investigation of your Horizon environment with vRealize Operations for Horizon. (iSIM)

**How to End Lab and not continue on to last module**

You can continue on to the last module or you can end your lab completely just click on the **END** button.
Module 5 - vRealize Operations for Horizon (30 minutes)
Module Overview

In this article, you will walk through some of the features of vRealize Operations for Horizon and explore some of the Horizon-specific out of the box dashboards. This iSIM demo will show the new helpdesk dashboard, explore root cause analysis, Horizon-based reports and smart alert details.
Hands-on Labs Interactive Simulation: vRealize Operations for Horizon

This part of the lab is presented as a Hands-on Labs Interactive Simulation. This will allow you to experience steps which are too time-consuming or resource intensive to do live in the lab environment. In this simulation, you can use the software interface as if you are interacting with a live environment.

1. Click here to open the interactive simulation. It will open in a new browser window or tab.
2. When finished, click the “Return to the lab” link to continue with this lab.
Conclusion

You have finished Module 5 on vRealize Operations for Horizon iSIM.

You've finished Module 5

Congratulations on completing Module 5.

If you are looking for additional information on the vRealize Operations for Horizon, try one of these:

- Click on this link
- Or go to https://tinyurl.com/y9g7fm3n
- Or use your smart device to scan the QRC Code.

Return to any module in this lab which interests you by clicking on the Table of Contents or End this lab and explore other Horizon Hands on Labs.

How to End Lab

To end your lab click on the END button.
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1851-07-ADV

Version: 20170920-142345