# Table of Contents

Lab Overview - HOL-1951-06-VWS - VMware Horizon 7 Enterprise – Advanced – JMP, App Volumes and User Environment Manager ................................................................. 2  
Lab Guidance ........................................................................................................................................ 3  
Module 1 - Just-in-Time Management Platform - Deep Dive (60 Minutes) ........................................... 9  
  Introduction .................................................................................................................................. 10  
  Overview ..................................................................................................................................... 11  
  JMP Workflows .......................................................................................................................... 14  
  JMP Application Entitlement ........................................................................................................ 48  
  JMP Manual Application ............................................................................................................. 54  
  JMP - How to Install - VIDEO (1:15) ....................................................................................... 66  
  JMP - How to Export Certificate - VIDEO (1:09) ..................................................................... 69  
  JMP Expert Series - Video (19:19) .......................................................................................... 72  
  READ ME GUIDE - Install consideration ............................................................................... 73  
  Conclusion ................................................................................................................................... 88  
Module 2 - App Volumes - Deep Dive (60 Minutes) ........................................................................ 89  
  Introduction .................................................................................................................................. 90  
  Creating AppStacks .................................................................................................................. 91  
  Updating AppStacks .................................................................................................................. 121  
  Attaching AppStacks to RDS Hosts .......................................................................................... 139  
  Working with Writable Volumes ............................................................................................... 140  
  Backing up Writable Volumes .................................................................................................... 148  
  OST Files and Writable Volumes ............................................................................................... 150  
  Advanced Concepts .................................................................................................................. 151  
  Conclusion ................................................................................................................................... 161  
Module 3 - User Environment Manager (UEM) - Deep Dive (60 Minutes) ...................................... 163  
  Introduction - User Environment Manager ............................................................................. 164  
  Application Customization ......................................................................................................... 168  
  Application Profiling .................................................................................................................. 187  
  Smart Policy ................................................................................................................................ 201  
  Application Blocking .................................................................................................................. 226  
  Privilege Elevation ..................................................................................................................... 245  
  Integration with Logon Monitor ............................................................................................... 270  
  Conclusion ................................................................................................................................... 275
Lab Overview - HOL-1951-06-VWS - VMware Horizon 7 Enterprise - Advanced - JMP, App Volumes and User Environment Manager
Lab Guidance

Note: It may 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.

Configure VMware Horizon 7 Enterprise as a Just in Time Management platform (JMP) with App Volumes, User Environment Manager

Lab Module List:

- Module 1 - Just-in-Time Management Platform (JMP) (60 Minutes)(Advanced)
- Module 2 - App Volumes (60 Minutes)(Advanced)
- Module 3 - User Environment Manager (60 Minutes)(Advanced)

Lab Captains:

- Captain - Vernon Lihou - Senior EUC Specialist SE, UK
- Captain - Logan Smith - Senior Solution Engineer, US
- Captain - Laurel Spadaro - Senior Solution 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:

Ask for a headset or use your own - video reference material ahead!

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 cannot 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 two 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.

Insert @ Symbol

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.
3. Click on the @ sign
4. 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 has finished all the startup routines and is ready for you to start. If you see anything other message than "Ready", please wait a few minutes. If after 5 minutes if your lab has not changed to "Ready", please ask for assistance.
Module 1 - Just-in-Time Management Platform - Deep Dive (60 Minutes)
Introduction

This module will focus on Just-in-Time Management Platform (JMP) technology

Module 1 contains the following lessons:

- **Lesson 1** - Overview
- **Lesson 2** - Design and Install consideration
- **Lesson 3** - JMP Workflows
- **Lesson 4** - JMP Expert Series VIDEO (2 minutes)
- **Conclusion**
The new JMP (Just-in-Time Management Platform) Integrated Workflow features in Horizon Console allow you to easily define and manage desktop workspaces that consist of a desktop operating system, applications, and settings. These features integrate the JMP technologies (Instant Clones for rapid image creation, VMware App Volumes for real-time application delivery, and VMware User Environment Manager for policies and personalization) into a single workflow.

With VMware Horizon JMP (Just-in-Time Management Platform) Integrated Workflow features, you can use a single console to define and manage desktop workspaces for users or group of users.

A desktop workspace is created by defining a JMP assignment that includes information about the VMware Horizon desktop pools, VMware App VolumesAppStacks, and VMware User Environment Manager settings. After a JMP assignment is submitted, the JMP automation engine communicates with the Horizon 7, App Volumes, and User Environment Managersystems to entitle the user to a desktop.
User-Centric Management

With JMP, you can manage outcomes instead of technologies. This means that instead of managing how users get their workspaces, you can define what kind of workspace a user should receive and JMP will automate the creation of the workspace.

Example, you can define what a Finance desktop should be what kind of OS, images, and user personalization and access privileges it should have and then simply assign Finance desktops to Finance users or Finance groups.

Workspace definition and assignment are done through a single console that ties all of the underlying technologies together. This decreases assignment time by over 50 percent. Additionally, exceptions and issues are caught early during the definition phase, which prevents extended test and deployment cycles.

Just-in-Time Delivery

The new deployment model with JMP enables you to go from static to dynamic management. Since the OS, applications, and user personalization are all maintained separately from each other, changes can be made very quickly and independently of the other components.
This is especially important with Windows 10 deployments where OS updates are released much more frequently than updates for previous Windows versions. With JMP, you can simply change the OS version for the desktop definition to update all users with a new OS update without having to change anything else.

You can also test application and OS combinations very quickly before rollout to ensure compatibility for your most critical applications. When a new version of Windows 10 is released, the assignments can be easily updated to consume the new version, and if there are issues, rollback is a matter of just a few clicks.

**Stay Secure**

Dynamic management and policies dramatically improve your security profile. With JMP, because OS and application images leverage the same golden, trusted images, there are far fewer images to maintain. If a security patch needs deployment, it can be done very quickly to the golden image, and rolled out to thousands of users. What's more, every time the user logs out, the desktop is destroyed and reassembled when the user logs back in.

This means that malware that is inadvertently or intentionally activated during a user session is obliterated every time the user logs out, and the desktops and apps start from a pristine, trusted image every time the user logs in.

**Lower Cost**

Lower Costs with JMP, you can drive down both operational and capital costs. JMP reduces downtime for your employees because you can very quickly spin up workspaces for employees to reduce maintenance windows. Imagine delivering new updated workspaces to 1,000 employees in just 20 minutes.

Because JMP automatically builds the workspaces your users need, you reduce time and costs for manual administration of images and infrastructure.

Capital expenses are also greatly reduced because instead of separate desktop and application images for each user, every desktop image and application image leverages the same parent footprint consider the savings of having 1 image instead of 1,000.
JMP Workflows

Creating JMP workflows from start to finish. The following exercise will walk through the JMP assignment process including the components that make up a successful assignment.

Chrome

On the HOL-1951 Main Console Desktop

1. Select Google Chrome

New TAB

1. Click - new TAB in Chrome
2. Select the Horizon folder
3. Click - Horizon-01-Admin
Horizon Login

1. User Name = administrator
2. Password = VMware1!
3. Domain = CORP
4. Click - Log In

Horizon Dashboard

1. Click the Catalog to expand
2. Click Desktop Pools

We have one Desktop pool that we will use for this exercise - [IC-Pool1]

Horizon Console

At the top of the Horizon 7 Administrator Console

1. Click Horizon Console
1. Click Settings

Once the JMP server is validated you can click through the TABS to see what the requirements are for each connection. When you are happy to continue, return to the Assignments section below.

Take note: If the JMP server is not "VALIDATED" or in a ready state, all the other options (Horizon 7 / Active Directory / App Volumes / UEM) will be greyed out and cannot be selected, nor can you proceed with workflows!
Assignments

1. Click - Assignments

New JMP Assignments

1. Click - New
User Selection

1. Next to CORP Domain use the search box and Type - **User4Mod1**
2. **Select** the User [User4Mod1]

This is the first step to assign a JMP workflow to a user. We can use a single user or a group at this point.

Continue

1. Click - **Next**
IC-Pool1 is a pre-created pool and we will assign the user to this Instant Clone desktop pool as the first part before assigning UEM policies or App Stacks.

1. **Select** the **pool** (ensure **IC-Pool1** is highlighted)
2. Click **Next**
This section will reach-out to the App Volumes server and show any App Stacks that is currently available. This will only look for App Stacks and not Writable Volumes. Please follow the standard procedure to attach a Writable Volume before or after you created the JMP assignment.

1. Click and select **Utilities**
2. Now **HOVER** your mouse pointer over the word **Utilities**. This will report back from the App Volumes server to display the App Stack information to ensure your select the correct stack for your assignment.
3. Click **Next**
1. Click and Select **Notepad (Shortcuts)**
2. ***Feel free to use the filter option to look for the application***
3. Click - **Next**

The UEM server will be interrogated at this point and any pre-defined user personalization will be displayed for selection. Personalization policies cannot be created at this point, only selected and applied.

There is no consistency check, so ensure you know what personalization will be applied by checking UEM first (ie Select Word personalization only if the user has Word installed). Should you have no need for UEM policies at this point then Select (A) and switch to YES to disable all UEM settings for THIS workflow only.
1. Feel free to give your Assignment a useful name to ensure consistency in your environment - **Windows 10 Desktop Pool**

2. This will save a lot of time when you need to duplicate this assignment ensuring the description captures what you assigned. **Write a description!**

3. The selection can be left at default (**On Next Login**), alternatively the user could already have a desktop in the pool selected in the first stage and this would allow (**Immediately**) for the App Stack to be presented in real time without the need for the user to log out and back in.

4. Click - **Next**
Summary

The final overview screen presented as a summary to the entitlement and assignment of the first 5 steps. When you are satisfied with the selection then click submit or click back to make further changes.

1. Click **Submit**

Status Review

The Status for the assignment will go from Orange to Green when completed.

Leave this TAB open and the screen as is, we will come back to this screen!
App Volumes

1. Click **New tab** in chrome

**App-Vol-01**

Click AppVol-01

**App Volumes Login**

Let's have a look at the assignment that is made in App Volumes

1. Username = **administrator**
2. Password = **VMware1!**
3. Domain = **CORP**
4. Click **Login**

**Volumes**

1. Click **VOLUMES**

**AppStack**

1. Expand **Utilities**
Utilities Assignment

1. Click on Assignments

We can now see that User4Mod1 is assigned to the App Stack Utilities, but not attached as the user is not logged into a desktop at this point.

VMware Horizon 7

1. Click and switch back to the Horizon 7 Console
1. Click **Refresh** if you have not done so already

**Windows 10 Desktop Pool**

Status should be green before you continue

1. Click on **Windows 10 Desktop Pool**
Windows 10 Desktop Pool Overview

This is the JMP Assignment overview screen of the Windows 10 Pool and we will come back to this, please leave this open.

You have successfully created a desktop pool, assigned an App Stack and personalized Notepad via UEM. Please continue to test your desktop pool.

Horizon Assignment Test

1. Click New tab in chrome
Chrome Favorites - VMware Horizon

1. Click VMware Horizon

VMware Horizon HTML Access

1. Click - Horizon HTML Access
1. Username = **User4Mod1**
2. Password = **VMware1!**
3. Click - **Login**
Instant Clone Pool

1. Click **Win10 Instant Clone 1**

**Desktop Preparation**

Wait while the new desktop is being prepared and the changes applied as per the JMP assignment.
WIN10 Desktop - Test Notepad++

1. Once the desktop is ready feel free to look at the newly attached App Stack (Notepad ++). Click Notepad++
2. Notepad shortcut created via UEM

Within 6 steps, you selected a user, assigned an App Stack, applied UEM user personalization, ensuring you have a repeatable workflow for Users/Groups, Horizon, UEM and App Volumes.

DO NOT CLOSE this desktop session! - Please continue to the next step.
Horizon 7 Console

1. Click on the **Horizon 7** tab in chrome

Select Windows 10 Desktop Pool

1. Click **Assignments**
2. Click **Windows 10 Desktop Pool**
EDIT - JMP assignments

1. Click **Edit**
1. Click **Next**
1. Click **Next** (ensure Pool is highlighted)
### Edit Assignment - Applications

1. Click **ALL** next to name to select both App Stacks
2. Click **Next**

#### Table:

<table>
<thead>
<tr>
<th>Name</th>
<th>Apps</th>
<th>Operating System</th>
<th>Creation Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multimedia</td>
<td>2</td>
<td>Windows 10 (x64)</td>
<td>6/5/2018</td>
</tr>
<tr>
<td>Utilities</td>
<td>3</td>
<td>Windows 10 (x64)</td>
<td>6/5/2018</td>
</tr>
</tbody>
</table>
Edit Assignment - UEM

1. Verify that **Disable UEM settings** is set to **NO**
2. Click **Next**

**NOTE:** The skip button will only be available when no option is selected
Edit Assignment - Definitions

1. Click **drop down**
2. Click and select **Immediately**
3. Click **Next**
We have successfully edited the original JMP assignment while the user is working and as demonstrated this can be done to update any part of the assignment including upgrading your base image, patching, changing a pool from a non compliant UEM pool to a compliant state etc.

1. Click **Submit**
Horizon Desktop View

1. **Click** the **VMware Horizon** tab and switch back to your desktop for User4Mod1

Give the screen a minute or two to refresh and feel free to look at the new App Stack (VLC and GIMP). Note that we have not created a shortcut for GIMP and you can access GIMP via the Start Menu

Leave this desktop open, **DO NOT Sign Out**
AppStack - Information Only

Having a sneak peak at the App Volumes Dashboard we would notice that the user now has an App Stack assigned and showing as attached in IC-Pool1. Feel free to switch to the App Volumes Manager and have a look, but stay connected to the desktop to view the attached AppStack.

JMP Console Explore

1. Click and switch back to the **VMware Horizon 7** Console
1. Click **Machines**
1. Next to machine, click and drag the column open to see the full machine name!
2. Click **WIN10IC-1**
# Machine Summary

The summary screen can be used for:

- **A - Restart Desktop** = Windows assisted restart
- **B - Reset Virtual Machine** = Hard reset of the VM with an automatic power on
- **C - Recover** = This will delete the virtual machine and spawn a new virtual machine
- **D - Remove** = Delete the virtual machine completely

1. Click **vCenter Settings**
Machine - vCenter Settings

Part of the summary is the virtual machine information that is used to identify the resources used and location for this assignment.
Sign out of any Open Desktops

When you are done looking around, please sign out

1. Click on the **Horizon TAB** in Chrome
2. Right Click the **Windows Icon**
3. Click **Shut down or sign out**
4. Click **Sign out**

Hope you enjoyed this module, this concludes JMP Workflows!
JMP Application Entitlement

Using the JMP console to grant a user entitlement to an application.

**Chrome**

On the HOL-1951 Main Console Desktop

1. Select *Google Chrome*

**New TAB**

1. Click - *new TAB* in Chrome
2. Click - *VMware JMP*
1. Type username = **Administrator**
2. Type password = **VMware1!**
3. Ensure the domain is **CORP**
4. Click **Sign in**
***We can also entitle a user to a desktop or an application using the Applications or Desktop tab under the Inventory section.

In this exercise we are going to entitle the user via the Users and Groups.

1. Click **Users and Groups**
2. Click **Entitlements**
3. Click **Add Application Entitlement**
### Add Application Entitlement

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In the Name/User name: type <strong>User4Mod4</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Find</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Select the user [User4Mod4]</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>Next</strong></td>
</tr>
</tbody>
</table>
Select Application

1. Click **Paint**
2. Click **Submit**

User overview

Users and Groups
We can see the user has desktop entitlements, application entitlements and any current sessions by looking at the Users and Groups dashboard.

1. Click on **user4mod4**

**Application Entitlement**

1. Click on **Application Entitlements**

You can now see the application entitlements for User4Mod4. If you clicked on the application name this would take you to the Applications within the Inventory and further amendments at application level could be done here.

The down arrow would allow you to download an Excel copy of the entitlements if you wish, but remember, we do not have excel installed on this server in order to view the downloaded file. Whenever you see the down arrow presented, the ability to export information is possible.
JMP Manual Application

Scenario - Company ABC wants to give an admin access to an RDP session without allowing access to the host that initiated the session. The user cannot complete the RDP session details or specify the remote server name (this needs to be pre-populated). We could publish an application to the user, but the program in questions is not in our list of applications as it is not under the Program Files directory. Let’s have a look at how to publish this application manually with advanced parameters.

Chrome

On the HOL-1951 Main Console Desktop

1. Select Google Chrome

New TAB

1. Click - new TAB in Chrome
2. Click - VMware JMP
VMware Horizon 7 - If you are logged out

1. Type username = Administrator
2. Type password = VMware1!
3. Ensure the domain is CORP
4. Click Sign in
Applications

We can entitle a user to a desktop or an application using the Applications or Desktop tab under the Inventory section.

In this case we are going to entitle the user via the Users and Groups.

1. Click **Applications**
2. Click **Add**
3. Click **Add Manually**

Add Application Pool

[Diagram of Add Application Pool]
1. In the RDS Farm field this should already be **RDSH-01** as we only have one at this point.
2. In the ID field type **RDS-JMP-01**
3. In the Display Name field type **RDP_Jump_Box**

**Add Application Pool - Scroll down**

1. **Scroll Down**
2. In the Path field, type the full path of the application (drag this & paste into the screen) `C:\Windows\System32\mstsc.exe`
3. Specify the Parameters for the session to automatically connect to our App Volumes server (drag this & paste into the screen) `/v:Appvol-01.corp.local`

**Submit**

1. Click **Submit**
Confirm - If requested

The application has not been installed on one or more RDS hosts. Do you still want to save the application pool?

1. Click **Confirm** (only if you see this pop-up otherwise continue with the next step)

Add User

1. Click **Add**
Find User

1. In the Name/User name: field, type **User4Mod4**
2. Click **Find**
3. **Select** User4Mod4
4. Click **OK**
Accept - Add Entitlement

Find User or Group

1. Click **OK** to confirm and accept the entitlement

Login as User4

1. Click to open a **New tab** in chrome
2. Click **VMware Horizon**

**VMware Horizon HTML Access**

You can connect to your desktop and applications by using the VMware Horizon Client or through the browser.

The VMware Horizon Client offers better performance and features.

1. Click **VMware Horizon HTML Access**
Log Out

If you are still logged in as User4Mod1, please Log Out first

1. Select **Log Out**
2. Click **OK**
Login

1. Type username = **User4Mod4**
2. Type password = **VMware1!**
3. Ensure domain is **CORP**
4. Click **Login**
1. Click the **RDP_Jump_Box** tile

### Enter password

1. Enter password = **VMware1!**
Success!! You have managed to publish a manual application with parameters.

1. Click **Windows**
2. Click **Shutdown or sign out**
3. Click **Sign out**
JMP - How to Install - VIDEO (1:15)

Follow this install video to get familiar with how to install your first JMP server. We have already installed all the required infrastructure components, so make sure you have a working Horizon environment before following this guide.

NOTE: NO SOUND IN THIS VIDEO
This video will guide you through the certificate import and export required when configuring a JMP server.
JMP Expert Series - Video (19:19)

Explaining JMP in detail through Q&A interview - please visit https://techzone.vmwarre.com for more content
READ ME GUIDE - Install consideration

JMP Technical Overview

Over a decade ago, when VMware first offered a virtual desktop infrastructure (VDI) solution, the strategy was to take a Windows desktop system, virtualize it, and place it in the data center. In those days, each employee’s virtual machine (VM) was a dedicated, persistent entity that required almost the same maintenance effort as a physical desktop.

Today, with JMP (Just-in-Time Management Platform) technologies from VMware, the components of the desktop are decoupled from each other and are assembled on demand to provide a modern digital workspace.

JMP is composed of the following VMware technologies:

- **VMware Instant Clone Technology** for fast desktop and RDSH provisioning
- **VMware App Volumes** for real-time application delivery
- **VMware User Environment Manager** for contextual policy management
JMP and Horizon 7 Components
This diagram and corresponding descriptions show the relationships between the major Horizon 7 version 7.1 (or later) components of a JMP deployment.

1. Horizon Client
2. Connection Server
3. VMware Instant Clone Technology
4. RDSH VMs and Desktop VMs
5. Agents
6. RDSH farms
7. Application pools
8. Desktop pools
9. App Volumes Manager
10. User Environment Manager
11. VMware Unified Access Gateway
12. Workspace ONE
13. Display Protocol
14. NEW JMP Server
Architecture of a JMP and Horizon 7 Deployment

Horizon 7 Pod

- SMB Shares
  - User Data
  - User Environment Manager Profiles
  - User Environment Manager Configuration

- ~2,000 Users
- Resource Block
  - Resource Cluster
    - Desktop Pools
    - Desktop Pools
    - RDSH Pools
    - ESXi Hosts
  - Shared Storage
  - Switched Ethernet Network
  - Resource Block vCenter Server

- ~2,000 Users
- Resource Block
  - Resource Cluster
    - Desktop Pools
    - Desktop Pools
    - RDSH Pools
    - ESXi Hosts
  - Shared Storage
  - Switched Ethernet Network
  - Resource Block vCenter Server

- ~2,000 Users
- Resource Block
  - Resource Cluster
    - Desktop Pools
    - Desktop Pools
    - RDSH Pools
    - ESXi Hosts
  - Shared Storage
  - Switched Ethernet Network
  - Resource Block vCenter Server

Management Block

- Management Block vCenter Server
- Connection Servers
- Unified Access Gateways (DMZ)
- User Environment Manager (GPO)
- SQL Database
- App Volumes Managers
- Datastores
This diagram depicts a one-site deployment, which includes one Horizon 7 pod containing three resource blocks and a single management block.

1. **Pod** - A pod is made up of a group of interconnected Connection Servers that broker desktops or published applications. A pod can broker up to 10,000 sessions (**please reference at the latest Horizon 7.x release notes for current limitations), including desktop and RDSH sessions. A pod is divided into multiple resource blocks.

2. **Resource blocks** - Each resource block consists of a VM cluster of desktop pools, RDSH pools, or both types of pools, as well as VMware ESXi hosts, shared storage for VMs, a switched Ethernet network, and a vCenter Server. Shared storage has separate datastores for desktop and RDSH server master images and for App Volumes AppStacks.

3. **Management block** - The management block includes vCenter Server, Unified Access Gateway appliances, Connection Servers, GPOs for User Environment Manager, and App Volumes Managers. A highly available SQL database cluster can support databases for all the App Volumes Managers, Horizon 7 Event databases, and vCenter Servers in the environment.

4. **SMB file shares** - Server Message Block file shares store user data through folder redirection, and file shares store User Environment Manager profiles and configuration files. User Environment Manager combined with folder redirection is the recommended solution for managing user personas.

**Setup and Configuration Process - JMP**

Please note that this is a high level walk-through of the setup process and key considerations. Please refer to the latest [Install JMP Server Guide](#) for a detailed setup.

Please do not change these settings in your current lab.
To use the JMP Integrated Workflow features, you must first install and configure JMP Server and the required VMware JMP technology products. Please refer to this Link Install JMP Server Guide for a detailed guide on setup.

Synchronize Time

Synchronize Time Between Horizon Connection Server and JMP Server Hosts.
• If time is unsynchronized between the two hosts, the Horizon Connection Server rejects the token provided by JMP Server resulting in the following error message: Horizon SSO token could not be verified.
• Synchronize time on the Horizon Connection Server and JMP Server hosts to a common Network Time Protocol (NTP) Server.
• Apply the following:
  1. Use the following VMware Tool commands on the Windows host.
     - C:\Program Files\VMware\VMware Tools>VMwareToolboxCmd.exe timesync status
     - C:\Program Files\VMware\VMware Tools>VMwareToolboxCmd.exe timesync enable
  2. On the ESXi host, synchronize ESXi Clocks with a Network Time Server.
     - Start the VMware Host Client, and connect to the ESXi host.
     - Click Configure.
     - Under System, click Time Configuration, and click Edit.
     - Select Use Network Time Protocol (Enable NTP client).
     - In the Add NTP Server text box, enter the IP address or fully qualified domain name of one or more NTP servers to synchronize with.

Main Steps to Configure the Certificates for JMP Server

![Diagram of certificate configuration process]

- Step 1
  - If TLS/SSL is enabled in your SQL Server, import the TLS/SSL certificate into the JMP Server host’s local certificate store.

- Step 2
  - Save the certificate to the C:\Program Files (x86)\VMware\JMPcom\XMS\config\ca.pem file.
  - Save the private key to the C:\Program Files (x86)\VMware\JMPcom\XMS\config\ca\jmp_self_vmware.com.key file.

- Step 3
  - Save the ca-chain.cert.pem file to C:\Program Files (x86)\VMware\JMPcom\ folder.

- Step 4
  - Copy the certificate file to the C:\Program Files (x86)\VMware\JMPcom\XMS\config\ca\app volumes manager 2.14 or later

- Step 5
  - Copy the certificate file to the C:\Program Files (x86)\VMware\JMPcom\XMS\config\ca\app volumes manager 2.14 or later

- Step 6
  - Copy the certificate file to the C:\Program Files (x86)\VMware\JMPcom\XMS\config\ca\app volumes manager 2.14 or later

- Step 7
  - Copy the certificate file to the C:\Program Files (x86)\VMware\JMPcom\XMS\config\ca\app volumes manager 2.14 or later
How to Replace the Default TLS Certificate

Procedure:

- In the JMP Server host, stop the three JMP Server services using the Windows Services Manager tool.
  1. VMware JMP API Service
  2. VMware JMP File Share Service
  3. VMware JMP Platform Services

- Save your CA-signed TLS cert and key files as jmp_self_vmware.com.crt and jmp_self_vmware.com.key in the NGINX configuration folder on the JMP Server host.

  (Optional) If you want to use different filenames that are different from the expected certificate filenames, you must modify the NGINX configuration file with the new filenames.

  C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf
Configure JMP Settings for the First Time

Before you can create any JMP assignments, you must configure the JMP settings using Horizon Console

### JMP Server Settings

Please do not change any of these settings in your lab, but feel free to browse and follow along. These steps have been designed to assist with a successful configuration of the JMP server after the initial install.

![Diagram showing steps to configure JMP settings](image)

**Procedure**

1. In the Horizon Console, click **Settings (JMP)**.
2. Enter the JMP Server information.
3. In the **JMP Server** tab, click **Add JMP Server**.
5. Click **Save**.

To complete the JMP setup, please have the URL, user name, and password for the following components:

- VMware Horizon® 7 Pod (required)
- Active Directory (required)
- VMware App Volumes (optional)
- VMware User Environment Manager (UEM) File Share (optional)
6. The JMP Server URL is validated. If you receive the JMP Server is unreachable message, verify that you had entered the correct URL, that the JMP Server is configured correctly, and that the JMP Server is reachable.

**Horizon Server Settings**

<table>
<thead>
<tr>
<th>JMP Server</th>
<th>Horizon 7</th>
<th>Active Directory</th>
<th>App Volumes</th>
<th>UEM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Edit Credentials**

**Horizon Server URL:**
https://horizon75-1.beta/mweuc.com/

**Service Account Username:**
administrator

**Service Account Domain:**
BETA/MWEUC

**Procedure** - Enter the account information for the Horizon 7 Connection Server version 7.5 or later that you plan to use with JMP Server.

1. Click the **Horizon 7** tab.
2. If not auto-filled, enter the **Connection Server URL** value. This URL is the same URL as the Horizon 7 Connection Server URL to which the Horizon Console is connected.
3. Enter your Horizon 7 service account user name and password.
4. In the **Service Account Domain** text box, enter a valid name to be used with the JMP assignments that you are creating and press **Enter**.
5. Click **Save**.
**Active Directory Settings**

**Procedure** - Enter the information for the Active Directory that you are going to use with the JMP assignments.

1. Click the **Active Directory** tab.
2. Click **New**.
3. In the **NETBIOS Name** text box, select from the list of available NetBIOS domain names. The DNS Domain Name and Context text boxes are updated with default values.
4. Verify that the default value that was added in the **DNS Domain Name** text box is the correct value to use. Optionally, enter another fully qualified Active Directory domain name. For example, mycompany.com.
5. In the **Protocol** section, select the protocol used by your Active Directory.
6. In the **Bind Username** and **Bind Password** text boxes, enter the credentials for the Bind Distinguished Name (DN) user account. For example, administrator.
7. Modify the value in the **Context** text box, if you want to use a value different from the default. The value is used as the root for the Active Directory data search.
8. (Optional) Click **Advanced Properties** and modify the default Port number value. The default Port value is based on the protocol you selected earlier. You can modify the Port value or leave the text box blank.
9. In the **Domain Controller** text box, optionally enter one or more host names or IP addresses to use for handling the Active Directory traffic. For example, adserver.mycompany.com, 10.111.XXX.XXX. If the text box is left blank, the value in the **DNS Domain Name** text box is used.
10. Click **Save**.
App Volumes Settings

<table>
<thead>
<tr>
<th>JMP Server</th>
<th>Horizon 7</th>
<th>Active Directory</th>
<th>App Volumes</th>
<th>UEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Edit</td>
<td>Delete</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>App Volumes URL</th>
<th>Service Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Volumes 2.14</td>
<td><a href="https://avm-fa-1.betavmweuc.com">https://avm-fa-1.betavmweuc.com</a></td>
<td>administrator</td>
</tr>
</tbody>
</table>

**Procedure** - If you plan to use App Volumes AppStacks when creating JMP assignments, configure the App Volumes Manager that you plan to use.

1. Click the **App Volumes** tab.
2. Click **New**.
3. In the **Name** text box, enter a name to assign to the App Volumes instance. If you leave the text box blank, the value you enter in the **App Volumes Server URL** text box is used.
4. Enter a valid URL for the App Volumes Manager that you want the JMP Server pod to be associated. **Important:** If a load balancer manages the App Volumes Manager that you plan to use, enter the URL for that load balancer.
5. Enter the App Volumes Manager or load balancer administrator account credentials that your JMP Server can use to access your App Volumes Manager.
6. Enter the domain name for the App Volumes Manager service account that is to be used for the JMP assignments.
7. (Optional) If you are registering more than one App Volumes Manager, use the toggle button to indicate if the App Volumes Manager you are adding is the default server to use when creating JMP assignments. You can change the instance you want to use at the time a JMP assignment is being created.
8. Click **Save**.
**Procedure** - If you are going to use a User Environment Manager configuration share when you create JMP assignments, add the information for it to the JMP settings.

1. Click the UEM tab.
2. Click **New**.
3. Enter a value in the **File Share UNC Path** text box in the format of `\server-name\UEM-configuration-share-pathname`. For example, `\server\UEMConfig`.
4. Enter the User Environment Manager administrator account credentials to be used to connect to the User Environment Manager configuration share.
5. Select from the **Active Directory** list the domain name to be used with the User Environment Manager configuration share. **Note:** An Active Directory can be associated with only one User Environment Manager configuration share.
6. Click **Save**
Conclusion

Module 1 provided an overview, Design and Install considerations including JMP workflows.

You've finished Module 1

Congratulations on completing Module 1.

If you are looking for additional information on Horizon 7 JMP, try one of these:

• Click on this link
• Or go to https://techzone.vmware.com
• Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

• Module 2 - App Volumes (90 minutes)
• Module 3 - User Environment Manager (90 Minutes)

How to End Lab

To end your lab click on the END button.
Introduction

In this module we will dive deeper into configuring and administering App Volumes.

- Introduction
- Creating AppStacks
- Updating AppStacks
- Attaching AppStacks to RDS Hosts
- Working with Writable Volumes
- Backing up Writable Volumes
- OST Files and Writable Volumes
- Advanced Concepts
- Conclusion

What is VMware App Volumes?

VMware App Volumes is a real-time application delivery system that IT can use to dynamically deliver and manage applications.

This module will be covering advanced App Volumes topics, and allow you to gain hands-on experience with the solution. If you would like a general overview of App Volumes, please take lab HOL-1951-02-VWS - Horizon Getting Started.
Creating AppStacks

This lesson will look at creating, provisioning and assigning an AppStack.

The lesson contains three sections:

Create an AppStack
Provision an AppStack
Assign an AppStack

Creating an AppStack

In this section we will walk through the process of creating an AppStack.

Launch Google Chrome

1. On the Main Console desktop, launch the Google Chrome browser
Login to vCenter

1. Click on **vCenter**
2. Select and click **RegionA vSphere Client (HTML)**
Login to vCenter

1. Click - **Use Windows session authentication**

**Note:** Should this step fail then use:

User name: `corp\administrator`

Password: `VMware1!`

2. Click **Login**

Power on Base Image

We will now power on the base image we will be using to capture the application.

If BASE-W10-1709-X64-01 is already powered-on (green arrow on VM icon), then skip the following and continue to the **next step**.

1. Right click on **base-w10-1709-x64-01 (under RegionA01-IC01)**
2. Select **Power**
3. Click **Power On**
As a best practice, you should create a virtual machine snapshot of the base machine before capturing the AppStack, and revert to that snapshot when complete. This will keep the capture machine clean for future captures and updates.

Login - Console BASE-W10-X64-01

1. Click on base-w10-1709-x64-01
2. Click in the middle of the Windows Console Window

*New tab should open at the top.

Open VM Console

1. Select the new **tab name base-w10-1709-x64-01** at the top
2. Click **Send Ctrl+Alt+Delete**
Log into the Virtual Machine

1. Ensure you log in as **administrator@corp.local** (select other user, if needed)
2. In the Password box type **VMware1!**
3. Click to continue

Once the desktop loads successfully continue to the next step.

App Volumes Management Console

1. Select a **new tab** in Chrome
1. Click on the **AppVolumes** folder, then **AppVol-01** shortcut
2. Log in as **Administrator**
3. Password **VMware1!**
4. Verify the Domain equals **CORP**
5. Click **Login**

Once authenticated, you will be taken to the App Volumes Dashboard.
**Volumes**

1. Click and select **VOLUMES**
2. Click **Create**

**Complete AppStack Info**

1. Select the Name: field and type "**Notepad++**"
2. Change Storage to "**vcsa-01a.corp.local: [RegionA01] ESX04a-Local**". **If this option is not selected, you will be unable to capture the AppStack.**
3. Select Description: field and type "**Notepad++**"
4. Click **Create**

**Confirm Create App Stack**

1. Using the default setting, click **Create**

**Confirm the Creation of the App Stack**

1. If the Notepad++ App Stack does not show immediately, then click **refresh**
2. Click the + Symbol next to Notepad++
Review AppStack Status

Note that the AppStack is now created, but not yet provisioned.

App Volumes automatically reminds the user of the next steps to create a successful AppStack. We will now start the capture process of the Notepad++ application.

Provisioning an AppStack

1. Click on **Provision** to start the process

This process should be followed carefully. Please note the different alerts during this process, telling you exactly when to click OK!
Search for the Base Machine

We will now locate the virtual machine that will be used to capture the application. Please note, the capture machine already has the App Volumes agent installed. This is a requirement for the machine to appear as "Available" in the App Volumes console.

1. Type **base** in the search box and click **search**
2. Select and click the **radio button** next to CORP\BASE-W10-X64-01$
3. Click **Provision**

This will trigger the provisioning agent on the Windows Desktop to start "capture mode" and link the Notepad++ App Stack to the VM, ready to install the application.

Start Provisioning

1. Click **Start Provisioning**
Start Provisioning

Once again the next step is defined by App Volumes for you.

Login to Capture Machine

1. Switch to the **base-w10-1709-x64-01** tab
2. If you have been logged out then re-log in using **Send Ctrl+Alt+Delete**
3. Type the password **VMware1!**
4. **Click** to login
Provisioning Window

You are now in provisioning mode and this window MUST stay open until the entire install has completed. Make sure you see the VMware App Volumes Provisioning notification banner before you continue.

Do not click OK or Cancel until the application is completely installed!

Open Windows Explorer

1. Click on the folder icon
Browse to SourceApps Folder

1. Navigate to `\controlcenter\SourceApps`
2. Double-click to open **Notepad++**

Security Warning

1. Click **Run**
Install Notepad++

1. Click **OK**

Click Next

1. Click **Next**
Click Next

1. Click I Agree

Click Next

1. Click Next
Click Next

1. Click Next

Create Shortcut

1. Check the box that says Create Shortcut on Desktop
2. Click **Install**

**Finish Install**

1. When the installer completes, uncheck the box that says **Run Notepad++ v7.5.5**
2. Click **Finish**
Close Windows Explorer

1. Click the X to close Windows Explorer

Complete Provisioning

1. Click OK to complete provisioning
Confirm

1. Click **Yes** to confirm

Confirm

1. Click **OK**

Your Computer will reboot at this point and will ensure the capture is completed. **You must wait for the desktop reboot, then log back into the VM to complete the process.** Do not return to App Volumes Manager before you have completed this step.
Login to Capture VM

1. Switch to the **base-w10-1709-x64-01** tab (if you are not still on the same tab)
2. Once the reboot is complete, then log in using **Send Ctrl+Alt+Delete**
3. **VMware1!** as the password
4. **Click** to log in

Provisioning Complete
1. Click OK

**Open Horizon**

We will now sign into our test virtual machine and verify Notepad++ does not appear on the desktop.

1. Open a **new tab** at the top while in Chrome
2. Select the **Horizon** shortcut on the bookmarks bar
Open Horizon HTML Access

1. If you receive the VMware Horizon prompt then click and select the HTML Access.
2. If not then continue to login.
Sign in

1. Username - user4mod2
2. Password - VMware1!
3. Click Login

Open Pool

1. Click and select Instant Clone Pool
Sign in to Virtual Machine

We’re getting everything ready for you

This will take a minute, as it's the first time the user User4Mod2 has logged onto this pool.
Check for Notepad++

Notice Notepad++ doesn't yet appear on the desktop.
Switch to App Volumes Manager

We will now assign the AppStack to the user4mod2 user.

1. Switch to the **App Volumes Manager** tab
2. Notice that the application has been successfully captured and the icon shows that we have Notepad++ installed in the AppStack.
Note - If the provisioning doesn't appear to be complete, you might need to press the refresh button.

**Assign an AppStack**

We will now assign the captured AppStack to a virtual machine. When assigned to a VM, the AppStack will be mounted when the computer boots, prior to anyone logging onto the machine. If the AppStack was assigned to a user, the AppStack would be mounted when the user logs on.

**Assigning an App Volumes AppStack**

1. Click **Assign**
Assign User4Mod2

We will assign the AppStack to user "user4mod2". This will ensure that the AppStack is connected when the user logs onto any virtual machines with the App Volumes agent installed (and the same OS as the capture machine). You would normally want to assign the AppStack to an Active Directory group, not an individual user. You can also assign the AppStack to a machine, where it would be mounted upon computer start-up instead of when the user logs on.

1. In the search Active Directory, type user4mod2
2. Click Search
3. Select the checkbox next to CORP\user4mod2
4. Click Assign
Attach Immediately

1. Click **Attach AppStacks immediately**
2. Click **Assign**

Attaching the AppStack immediately will mount the AppStack if a user is logged into the virtual machine. Selecting **Attach AppStack on next login** will only mount the AppStack after the existing users logs off (or reboots) and the assigned user logs on.

Test the AppStack

Now we'll test to verify the AppStack is appearing in the VM.

1. Click the **VMware Horizon** browser tab
Confirm Notepad++ Appears on Desktop

The Notepad++ application should now be on the desktop ready for use. It might take up to 30 seconds to appear.

Congratulations, you have successfully assigned your first AppStack!

Sign off Virtual Machine

1. Right-click on the Windows symbol
2. Hoverover Shut down or sign out
3. Click Sign Out

More Information

This lesson helped you to create and provision your first AppStack. For more information on other AppStack considerations, please visit the following website:

App Volume Deployment Considerations
Updating AppStacks

In this lesson, we will be adding WinSCP to the existing Utilities AppStack in App Volumes. We're going to be adding an application that is not currently included in the AppStack, but you could also use this process to update an existing application to a newer version.

Introduction to Updating an AppStack

The VMware App Volumes update feature makes a copy of an existing AppStack, and allows you to add more applications, update current applications, or make any other changes to the newly copied AppStack. The original AppStack still exists and is unaffected by the changes to the copy.

Power on Base Image

In the following steps, we will be powering on the base virtual machines used to capture and update App Stacks. If the virtual machine is already powered on, you can skip to the next step by clicking this link. The machine will already be powered on if you completed the chapter Creating and AppStack.

Launch Google Chrome

1. On the Main Console desktop, launch the Google Chrome browser
Login to vCenter

1. Click on **vCenter**
2. Select and click **RegionA vSphere Client (HTML)**
Login to vCenter

1. Click - **Use Windows session authentication**

**Note:** Should this step fail then use:

User name: `corp\administrator`
Password: `VMware1!`

2. Click **Login**

Power on Base Image

We will now power on the base image we will be using to capture the application.

If `BASE-W10-1709-X64-01` is already powered-on (green arrow on VM icon), then skip the following and continue to the next step.

1. Right click on `base-w10-1709-x64-01 (under RegionA01-IC01)`
2. Select **Power**
3. Click **Power On**
Login - Console BASE-W10-X64-01

1. Click on **base-w10-1709-x64-01**
2. Click in the middle of the **Windows Console** Window

*New tab should open at the top.

Open VM Console

1. Select the new **tab name base-w10-1709-x64-01** at the top
2. Click **Send Ctrl+Alt+Delete**
Log into the Virtual Machine

1. Ensure you log in as **administrator@corp.local (select other user, if needed)**
2. In the Password box type **VMware1!**
3. **Click** to continue

Once the desktop loads successfully continue to the next step.

App Volumes Management Console

1. Select a **new tab** in Chrome
App Volumes Management Console

1. AppVol-01
2. Username: Administrator
3. Password: ********
4. Domain: CORP
5. Login button

[Image of App Volumes Management Console login screen]
Update the AppStack

1. On the App Volumes Manager page, click on the Volumes tab. Existing AppStacks are displayed.
2. Locate the Utilities AppStack, click on the Add(+) icon.
3. Click Update.
Update the Utilities AppStack

1. Change the Storage to `vcsa-01a.corp.local: [RegionA01] ESX04a-Local`. **If you do not make this change, you will be unable to update the AppStack.**
2. Click Create

Confirm Update AppStack

1. Click **Wait for completion**. This will wait to refresh the screen until after the update Appstack is created.
2. Click **Update**
New AppStack vs. Original AppStack

Notice the update AppStack now appears in the list with the original AppStack. Updating AppStacks creates a copy, and the original AppStack still exists and is unaffected by the changes to the copy.

Start the Provisioning Process

The status of the AppStack should be Unprovisioned, indicating that the provisioning process is not yet complete.

1. Click **Provision**
Search for Provisioning Virtual Machine

1. We will now locate the virtual machine that will be used to update the Utilities AppStack.
2. Type **base** in the search box and click **search**
3. Select and click the **radio button** next to CORP\BASE-W10-X64-01$
4. Click **Provision**, and **Start Provisioning** (not shown)

Note - This will trigger the provisioning agent on the Windows Desktop to start "capture mode" and link the Utility AppStack to the VM, ready to update the application.
Open WinSCP Installer

1. Switch to the **base-w10-1709-x64-01** tab
2. If you have been logged out then log in using **Send Ctrl+Alt+Delete**
3. **VMware1!** as the password
4. **Click** to login

Confirm Provisioning Mode
You are now in provisioning mode and this window MUST stay open until the entire install has completed. Make sure you see the VMware App Volumes provisioning notification banner before you continue.

Open Windows Explorer

1. Click on the folder icon

Open WinSCP Installer

1. Type `\controlcenter\SourceApps` in the address bar, and press Enter
2. Double-Click `WinSCP-5.13.2-Setup` to open the installer
Install WinSCP

1. Click **Run** in the security warning dialog box

Select the Defaults

1. Select **Accept** in the setup wizard, and defaults for the remainder of the install, until the **Completing the WinSCP Setup Wizard** page appears
Complete the Install

1. Uncheck the boxes next to Launch WinSCP and Open Getting started page
2. Click Finish

Close Windows Explorer

1. Click the X to close Windows Explorer
Complete Provisioning

1. Click **OK**

Complete Provisioning

1. Click **Yes**

Confirm Reboot

1. Click **OK**

Your computer will reboot at this point and will ensure the capture is completed. **You must wait for the desktop reboot, then log back into the VM to complete the process.** Do not return to App Volumes Manager before you have completed this step.
Sign into Provisioning Virtual Machine

1. Switch to the **base-w10-1709-x64-01** tab (if you are not still on the same tab)
2. Once the reboot is complete, then log in using **Send Ctrl+Alt+Delete**
3. **VMware1!** as the password
4. **Click** to log in
Provisioning Complete

1. Click **OK**

Return to App Volumes Manager

1. Click the **App Volumes Manager** browser tab

Refresh the List

1. Click the **refresh** button to refresh the list.
Confirm the AppStack is Provisioned

You should now see WinSCP appears as a fourth application in the AppStack, and the AppStack is completely provisioned and ready for assignment. When deploying an updated AppStack, be sure to unassign the original AppStack before assigning the updated version.
Attaching AppStacks to RDS Hosts

This lesson will discuss creating and attaching AppStacks to RDS Hosts.

Assigning AppStacks to RDS Hosts

AppStacks can also be captured and assigned to RDS Hosts. Using App Volumes in a RDSH environment allows for easy application deployments and updates, and when used with VMware Just-in-Time technology, you can decouple and manage servers and applications independently in a centralized manner, yet reconstitute them on-demand to deliver a personalized user workspace when needed.

App Volumes attaches applications to the RDSH server at boot time, and User Environment Manager retains user preferences and applies contextual policy management. RDSH farms are created using Instant Clone Technology, and the RDSH server VMs can be refreshed according to a recurring maintenance schedule.

Note - When using App Volumes with RDSH instant-clone server farms, you must assign App Volumes AppStacks to Active Directory OUs rather than groups.

For more information, please refer to the whitepaper for VMware Horizon 7 Instant-Clone Desktops and RDSH Servers:

https://tinyurl.com/yah4byfp
Working with Writable Volumes

This lesson will walk you through working with writable volumes.

It contains the following sections:

- Creating Writable Volumes
- Expanding Writable Volumes
- Allowing End Users to See the Size of Their Writable Volumes

Working with Writable Volumes
The App Volumes writable volumes feature enables the creation of a per-user volume where the following user-centric data can be installed and configured in different ways and move with the user:

- Application settings
- Licensing information
- Configuration files
- User-installed applications

Writable volumes do not provide a complete user environment management solution, but complement a user environment management solution. VMware User Environment Manager is a companion to App Volumes and provides management of user application settings that are applied when the user logs in or when an application launches. VMware User Environment Manager can manage data within writable volumes at a more granular level and provide contextual rules to enforce policies based on different conditions or events.

Note the key differences between AppStacks and writable volumes:

- **AppStack VMDKs** are mounted as read-only and can be shared among all desktop virtual machines (VMs) within the data center.
- **Writable volumes** are dedicated to individual users and are mounted as the user authenticates to the desktop. Writable volumes are user-centric and roam with the user for non-persistent desktops.

After writable volumes are created and assigned to a user, that user can install and configure applications. For this functionality to work properly, users require account permissions that allow application installation. App Volumes defers to Microsoft Windows security policies to determine user rights assignments.

### Creating and Assigning a Writable Volume

In this module we will walk through the creation of a Writable Volume.

**Launch Google Chrome**

1. On the Main Console desktop, launch the Google Chrome browser
App Volumes Manager

1. Open the AppVolumes Manager folder
2. Click on AppVol-01
3. Username Administrator
4. Password VMware1!
5. Confirm the Domain is CORP
6. Click Login

Once authenticated, you will be taken to the App Volumes Dashboard.
Create Writable Volume

1. Click and select **VOLUMES**
2. Click **Writables**
3. Click **Create**

Search for User

1. In the Search Active Directory box, type user4mod2
2. Click **Search**
Configure the Writable Volume

1. Select CORP\user4mod3 check box
2. Change the storage to vcsa-01a.corp.local: [RegionA01] ESX04a-Local
3. **Accept the default**
4. Drop down the source template section and **select** the /template_uia_only.vmdk (10GB)
5. Select **Prevent user login** check box
6. Select **Limit the attachment check** box
7. Only attach when the name of the host computer begins with - type **base**. This will prevent the writable volume from attaching to any virtual machines who's machine name doesn't begin with "base"
8. Click **Create**
Confirm Create Writable Volumes

1. Click **Create volumes immediately**
2. Click **Create**

Confirm the Writable Volume was Created

1. **Click** + to expand User information

User4Mod2 now has a writable volume that will follow the user on any VM that has the prefix "base" in it's machine name.

We can now edit, disable, expand or delete the writable volume.

Expanding Writable Volumes

If a users writable volume has reached or is about to reach full capacity, it can be expanded.
Edit the Writable Volume

1. Click the **Volumes** tab
2. Click **Writables**
3. Expand the writable volume created in the previous step by clicking the + sign next to its name.
4. Click **Expand**

Enter the New Value

1. Enter **20480** as the new value
2. Click the **Expand** button

Congratulations! You have expanded the user's writable volume to twice it's original size.
Allowing End Users to See the Size of Their Writable Volumes

You can view space remaining in writable volumes from the App Volumes Manager. You can also allow the end user to see available space on their writable volume, from their system volume.

To do this, you will need to create a new registry key during the App Volumes Agent configuration. For information on how to perform the necessary steps, please refer to the App Volumes Deployment Considerations whitepaper.

Free Space Report

After you make the registry modifications, and you reboot the system:

1. C:\ object now reports free space on the user’s writable volume (which is 8.13 GB total in this case).
2. The total space still reflects the combined C:\ value.
Backing up Writable Volumes

This lesson will walk you through backing up writable volumes.

**Backing up Writable Volumes**

Writable Volumes have the ability to be backed up and restored within App Volumes Manager. You have several options for backing up writable volumes - you can back up single or multiple volumes manually, or you can schedule a reoccurring backup of all writable volumes.

Storage groups are not supported targets for moving or backing up writable volumes.

**Location of Backup and Restore**

You are able to backup and restore writable volumes on the Writables tab within App Volumes Manager. The volume cannot be backed up when it is attached. If a backup operation is kicked off when a volume is attached, the action is queued and will be performed when the volume is detached.
Regular Backups can be scheduled within the Settings tab in App Volumes Manager.
OST Files and Writable Volumes

This lesson will discuss using Microsoft OST files in conjunction with Writable Volumes.

OST files in App Volumes

When using Microsoft Outlook in non-persistant VDI environment, there are two different ways to handle Outlook connectivity:

1. Outlook can be configured to be in "Online" mode, constantly connected to Office 365. This configuration reads the messages directly from Office 365, and does not require your mailbox to be copied to the local machine. The user experience for this method will be affected by network latency or bandwidth constraints.
2. Outlook can be configured in "Cached Mode", where a local copy of the mailbox is created. This mode historically hasn't worked well in a non-persistance VDI environment:
   - OST file is discarded when desktops are refreshed/recovered.
   - Outlook re-creates the OST file each time a user logs into a new desktop.
   - Depending on the size of the OST file, Outlook load times might be significantly affected.
   - Redirecting OST to network shares has limited support, and may affect performance.

In App Volumes version 2.14 and newer, the OST file is redirected automatically. There is no additional configuration needed above and beyond having writable volumes configured.
Advanced Concepts

In this module we will look at some advanced topics for VMware App Volumes.

This module contains the following lessons:

- TLS Connections in App Volumes
- Troubleshooting
- Conclusion

TLS Connections in App Volumes Manager

You can modify the Nginx configuration file to ensure that App Volumes Manager accepts connections only from specified TLS versions. This will add an additional level of security. For example, if you configure App Volumes to use only TLSv1.1 and TLSv1.2, App Volumes Manager will accept connections only from these TLS versions.

App Volumes Manager uses SSL and TLS to communicate securely with servers and App Volumes agents.

Launch Google Chrome

1. Validate you're on the main console desktop
2. If not already open, launch the Google Chrome browser
Login to vCenter

1. Open the **vCenter** folder.
2. Select and click **RegionA vSphere Client (HTML)**.
3. Check the box to enable **Windows session authentication**.
4. Click **Login**
Login - Console AppVol-01

1. Click on AppVol-01
2. Click in the middle of the Black Console window

*New tab should open at the top.

Send Ctrl-Alt-Delete

1. Select the new tab name AppVol-01 at the top
2. Click Send Ctrl+Alt+Delete
Enter Password

1. In the password box type **VMware1!**
2. **Click** to continue

Once the desktop loads successfully then continue to the next step.

Open Windows Explorer

1. **Click** **File Explorer (Folder Icon)** on Task Bar

Navigate to NGINX folder

1. Type - **C:\Program Files (x86)\CloudVolumes\Manager\nginx\conf**
2. **Click** **continue**
Edit the File

1. Right-click nginx.conf
2. Select Edit with Notepad++

Open Search Box

1. Click Search
2. Click Find
Search for TLS

1. Search for **TLS**

This file can now be edited to accept only TLS connections approved by your organization’s security team. For example, if you include TLSv1.1 and TLSv1.2 in the ssl_protocols line, App Volumes Manager will accept connections only from these TLS versions.

**TLS Version**

```plaintext
server {
  server_name 192.168.110.10;
  listen 3443;
  listen 443;
  listen [::]:443;

  ssl on;
  ssl_certificate appvol_cal_vmware.com.crt;
  ssl_certificate_key appvol_cal_vmware.com.key;
  ssl_protocols TLSv1.2
  ssl_session_cache builtin:1000;
}
```
In this example, App Volumes Manager will accept connections only from agents that use TLS v1.2 protocols, as specified in the ssl_protocols entry in the Nginx configuration file.

**Sign out of Desktop**

1. **Close** Notepad - Do not make or commit any changes
2. **Sign out**

**Troubleshooting**

This chapter will discuss a couple of the more commonly seen issues by VMware support when troubleshooting App Volumes. These are concept walk-throughs, and do not need to be performed in the lab.

**Slow User Login**

When experiencing slow logins, there are two different areas to investigate.

**Review Logon Segment Timing**

You can use the Horizon Help Desk Tool to troubleshoot slow logins. This tool will show how long each segment of the login takes. To see this information in the Help Desk Tool, you will need to enable the timing profiler on each connection server.
Use the following `vdmadmin` command to enable the timing profiler on each Connection Server instance:

```
vdmadmin -I -timingProfiler -enable
```

Use the following `vdmadmin` command to enable the timing profiler on a Connection Server instance that uses a management port:

```
vdmadmin -I -timingProfiler -enable -server {ip/server}
```

**Optimize clock.yml**

If you are experiencing performance degradation as your deployment scales in size, consider making changes to the `clock.yml` file. Note - As a best practice, please contact VMware Support to ensure you are inputing the optimal settings for your environment.

More information can be found here:


**AppStack Not Attaching at Logon**

If your AppStack is not attaching when logging onto the virtual machine, there are several things you can check.
If one host in vSphere cluster does not have access to the shared datastore where the AppStack resides, the AppStack will not consistently attach. This can be a common oversight, especially with Storage Groups. You would see a "vmdk was not found" in the logs, as shown above.

**Conflicting Minifilter Driver**

If you have a conflicting Minifilter driver, your AppStack may not attach. For more information, please refer to the following Microsoft article:


**Additional Troubleshooting Resources**

For additional information for troubleshooting your Horizon and App Volumes environment, please take the HOL-1951-05-VWS Lab, or refer to the following presentation:
Conclusion

This module took a deeper-dive into App Volumes, demonstrated how to capture and update AppStacks, create and assign writable volumes, and configure advanced options.

Congratulations, you've finished Module 2

Congratulations on completing Module 2.

If you are looking for additional information on VMware App Volumes, try one of these:

- Click on this [link](#)
- Or go to [https://tinyurl.com/gp9uy37](https://tinyurl.com/gp9uy37)
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

- [Module 1 - Just in Time Management Platform (60 minutes)](#)
- [Module 2 - App Volumes (60 minutes)](#)
- [Module 3 - User Environment Manager (60 minutes)](#)
How to End Lab

1. To end your lab click on the **END** button.
Module 3 - User Environment Manager (UEM) - Deep Dive (60 Minutes)
Introduction - User Environment Manager

VMware User Environment Manager offers personalization and dynamic policy configuration across any virtual, physical and cloud-based Windows desktop environment. User Environment Manager simplifies end-user profile management by providing organizations with a single, light-weight and scalable solution that leverages existing infrastructure. It accelerates time-to-desktop and time-to-application by replacing bloated roaming profiles and unmaintainable, complex logon scripts. It maps environmental settings (such as networks and printers), and dynamically applies enduser security policies and personalizations. This focused, powerful and scalable solution is engineered to deliver workplace productivity while driving down the cost of day-to-day desktop support and operations, and is a key component of JMP the next generation of desktop and application delivery.

Features

• Centralized and Simplified Management of Windows Environments
• Dynamic, Contextual Policy Management
• Consistent User Experience Across Devices and Locations
• Easy Start for Adding Applications and Environment Settings to Manage
• Application Templates and Application Profiler
• Self-Support Tool
• Helpdesk Support Tool

Use Cases

Some of the most popular reasons why enterprises use User Environment Manager:

• **Saving Users’ Settings Across Devices** for a consistent user experience
• **Improving Logon Times** by carrying out tasks dynamically if and when needed instead of all at logon time
• **Managing Least Privileges** to improve IT ops with privilege elevation to elevate permissions instead of granting local admin privilege to end users
• **Providing Desktops Just in Time** giving user flexibility to customize while maintaining non-persistent desktops for streamline management

Components of User Environment Manager

User Environment Manager can be summarized in three parts:

1. **Management Console** - Primary application interface for IT to configure and manage User Environment Manager.
2. **FlexEngine** - Agent component, which is installed on the virtual or physical machines that you want to manage.

3. **File shares** - User Environment Manager relies on a folder hierarchy. User Environment Manager stores configuration files in the configuration share. User data is stored in the profile archives share.

## Architecture of User Environment Manager

Overview of the architecture shows how the components relate to each other. All components of User Environment Manager that you deploy communicate between each other by using the SMB protocol.

- **User Environment Manager GPO** - You create a GPO for each Active Directory organizational unit (OU) you want to manage.

- **User Environment Manager Management Console** - You use this User Environment Manager administrative UI to configure application settings, Windows environment manager settings, conditions under which the settings go into effect, and various other configuration settings and Horizon Smart Policies for things like printer mapping, attaching devices to the virtual desktop or application, and the ability to copy and paste text.

- **User Environment Manager Application Profiler** - For the few applications for which you cannot find an already-created application template, you can use this standalone application that analyzes where the application stores its file and registry configuration, and also set the initial configuration state of the application.

- **Central configuration share** - You create this file share to store the Management Console configuration and User Environment Manager configuration files. The User Environment Manager agent (FlexEngine) on virtual desktops and
RDSH servers reads the configuration file on this share and applies the settings specified in the configuration file.

- **Network folder per user** - In this file share that you create, each folder, or profile archive, contains ZIP files where the User Environment Manager agent (FlexEngine) stores the personalized settings of a user. For each User Environment Manager (Flex) configuration file that you create, FlexEngine creates a profile archive for each user.

- **User Environment Manager Helpdesk Support Tool** - This tool provides capabilities to support and maintain the User Environment Manager profile archives and profile archive backups.

- **Clients with User Environment Manager FlexEngine** - The agent software, FlexEngine, runs on each virtual desktop or RDSH server whose applications are to be managed. This agent reads the centralized configuration file, applies User Environment Manager settings, and saves those user settings that end users are allowed to control. In this client-server architecture, the FlexEngine agent software plays the **client** role, and the User Environment Manager Flex configuration file plays the **server** role.

- **SyncTool** - Laptop users who are not always connected to the corporate network need access to their User Environment Manager configuration files while offline. SyncTool makes all VMware User Environment Manager configuration files available locally and synchronizes changes when users connect to the corporate network. Additionally, users with a slow WAN connection can use local User Environment Manager configuration files, thus limiting network traffic and avoiding continuously roaming personal settings.

## Easy Start

By default, User Environment Manager does not manage any applications or environment settings after you install it. You must specify which applications and settings to manage. Although this approach takes a little more work up front, this solution prevents excessive profile growth and profile corruption, enables user settings to roam across Windows versions, and gives you granular control to manage as much or as little of the user experience as needed.

To help with getting started, the Easy Start button instantly adds many common Windows applications, including several versions of Microsoft Office, to the whitelist of applications managed by User Environment Manager. Many Windows environment settings are also added by Easy Start. You can then easily select an application or Windows setting to review and change the default settings.
Clicking this button allows User Environment Manager to manage many common Windows applications.

*Note: This has already been done for you in this lab.*
Application Customization

With the application personalization feature, end users can roam between disparate devices while preserving custom application settings and Windows personalization settings. When a user logs in to a virtual desktop or application, User Environment Manager reads the profile archive file for that user's profile and can, for example, display the desktop background or application settings that the user saved during the last session.

Application Configuration Management

With User Environment Manager, you can configure the initial settings of an application without having to rely on the defaults of the application. You can define the application settings that the user can personalize and the settings that always remain unchanged each time the user opens the application. In this way, you can combine policy-enforced settings and user personalization.

You can also use User Environment Manager to manage certain user environment settings when an application starts. For example, you can configure drive and printer mappings, apply custom settings for files and folders, and registry, and run custom tasks. You can also define settings and configurations for all users to guarantee compliance and provide a consistent environment.

Open UEM Management Console

From the Main Console, double-click the UEM Management Console shortcut on the desktop. This will open up the User Environment Manager Management Console.

You may need to minimize the Chrome Browser so you can see the desktop.
Personalization of Applications in UEM

Under personalization we will look at Wordpad.

1. Under the **Personalization** tab
2. **Expand the Applications** by clicking the + sign by the applications under General
3. Click on **Wordpad**
4. Note the DirectFlex is configured and enabled for this application

In this lab we are going to open wordpad and make some changes to the layout as well as map a drive to the application. We will logout and back in to see these changes stick and show drive mapping.
In this module, we will be logging into a desktop, making policy changes through UEM and verifying those changes on the Desktop. UEM settings are applied every time the user logs in. We are using an Instant Clone Desktop in a limited lab environment so do not want to wait on the Instant Clone Desktop to refresh. We will instead set that the UEM settings are refreshed upon unlock of the Desktop. To do this we will set a Triggered Task User Environment setting in UEM.

The Triggered Task Settings option allows triggered task settings to be refreshed when users disconnect, reconnect, or lock or unlock their workstation. Previously, these settings were refreshed only after users logged out of the virtual desktop or application.

1. Click on the management console User Environment Tab
2. Click on Triggered Tasks
3. Click Create
**Complete Settings for Triggered Task**

1. General Settings Name and Label: **Refresh UEM at unlock**
2. Under Triggered Task Settings pull down select **Workstation Unlock**.
3. Under Action pull down select **User Environment refresh** and this will bring up the variables to choose to refresh
4. Under Refresh click the box next to:
   - Application Blocking Settings
   - Drive Mappings
   - Horizon Smart Policies
   - Privilege Elevation Settings.
5. Click on **Show Message**
6. Enter Caption: **HOL UEM Refresh**
7. Enter Message: **The UEM Settings were refreshed.**
8. Click on **Close Automatically after** and enter 8 for the seconds. Click **Also allow user to dismiss message.**
9. Click **Save**

**Minimize the UEM Management Console**

1. Click on Refresh of the UEM Management Console.
2. Minimize the UEM Management Console so we can launch a desktop.
Horizon HTML Access

1. Open Chrome Browser
2. Select the **VMware Horizon** bookmark
3. Select **VMware Horizon HTML Access**
Login to VMware Horizon

Login to Horizon HTML Access:

1. Login as: **user4mod3** *(please make sure to login as user4mod3 user if another one is listed)*
2. Password: **VMware1!**
3. Click **Login**
Launch the Instant Clone Desktop

Click the **Instant Clone Pool** to launch the desktop. It will automatically log user4mod3 user into the desktop.

**Launch Wordpad from the desktop**

Notice Wordpad icon says it was "created by VMware UEM".

**Double-click on Wordpad** to open up the application. We will make some changes to the application and show how they are retained at the next login and launch of that application.

Note that Update Virus Protection alert may pop-up on the Instant Clone desktop. You can ignore this warning for our lab environment.
Make some changes to the application

1. Click on View
2. Uncheck Ruler and Uncheck Status Bar
3. Click on Measurement units and change to Centimeters

Save File As
1. Click on **File**
2. Click on **Save As** to see what drives are being mapped currently.

**Notice No Drive Mapping for M: Drive**

1. Under **This PC**, Observe no M: drive mapping is mapped at this time.
2. Click **Cancel** as we will not be saving the file.
Close the Application

Click the X in the top right corner of the Wordpad application to close it.

Click OK if asked.

Lock the Desktop

1. Click on the Window in the bottom left corner
2. Click on the Person icon
3. Click lock

We will lock the user's desktop while we make some policy changes in UEM for Wordpad
Go back to the UEM Management Console

![Image of VMware Horizon Client with 'Production' Environment highlighted]

We need to open the UEM Management Console back up in order to Add a Drive Mapping for the application.

Click on the 'Production' Environment on the bottom toolbar to re-open the VMware User Environment Console.

**UEM - Add Drive Mapping**

1. Under **Personalization**
2. Expand **Applications**
3. Click on **Wordpad** on the left column
4. Click on **User Environment** on the tabs under Wordpad window.
5. Click On **Add**
6. Click **Drive Mapping** to map a drive
1. Enter a name for the drive mapping and Label: **UEMTest**
2. Select a Drive Letter under Drive Mapping Settings: M
3. Enter Remote Path: `\localhost\c$\tools`. In our lab environment we will just map a local folder. *You can highlight the path and use the hand to drop into the lab.*
4. Click on "**Undo at application exit**" to unmap the drive once Application is closed.
5. Click **Save**
UEM Save Config File

Click on **Save Config File** at the top to save the changes made to mapping the drive.
Unlock the Horizon HTML Access Desktop

1. Open the Desktop back up by clicking on the Chrome Browser tab for the Horizon HTML Access
2. Click in the Desktop to get the prompt for password to unlock: Enter password: **VMware1!** and hit return.

Click on the background desktop to close the window prompt.

The triggered task we configured earlier in this lesson will pop up when you unlock the desktop. You can dismiss this window or wait the 8 seconds we configured for it to clear. This is letting you know that the UEM environment was refreshed. Their is also another pop up about workstation unlocked that is used for another lab that you can dismiss.

Launch the Wordpad Application from the desktop
Double-click on Wordpad to open up the application. We will make some changes to the application and show how they are retained at the next login and launch of that application.

Observe the Application

Confirm that the changes are there.

1. Click on View in the Wordpad app.
2. Notice Ruler and Status Bar are not present and unchecked.
3. Click on the Measurement units to show the check mark next to Centimeters.
4. Click on File
5. Click on Save As where we can check the drive mapping in the next step.
Confirm Drive Mapping

1. Browse to the "This PC" and expand.
2. Notice the tools directory is mapped to the M drive. Click on it to see the path at the top or expand the window to see the entire path.
3. Click Cancel

This allows you to map drives only for when that application is launched.
Close the Application

Click the X in the top right corner to close the Wordpad application.

Click Don't Save if prompted.

You can also open the File Explorer and see the drive mapped when application is opened and is removed when application is closed.
Sign out of the Desktop and close Chrome Browser

1. Click on the **Window** in the bottom left corner
2. Click on the **Person** icon
3. Click **Sign Out**

Close the Chrome Browser by clicking **X** in the top left corner of the Chrome App.
Application Profiling

Application Profiler is a standalone tool that helps you determine where in the file system or registry an application is storing its user settings. The output from Application Profiler is a configuration file which can be used to preserve and roam application settings for your end users. Optionally, you can record a default set of application settings, and apply and/or enforce these defaults for your users based on a variety of conditions.

Application Profiler analyzes where an application stores its file and registry configuration. The analysis results in an optimized Flex configuration file, which you can edit in the Application Profiler or use directly in the User Environment Manager environment.

With Application Profiler, you can also create application-specific predefined settings, with which you can set the initial configuration state of applications. Save the Flex configuration file with predefined settings to export the current application configuration state.

Application Profiler is licensed as a VMware User Environment Manager component.

Application Profiling Overview

From a high-level perspective, the process is as follows:

1. Start Application Profiler.
2. From within Application Profiler, start the application to analyze.
3. In the background, Application Profiler monitors the registry and file system actions of the started application.
4. Change the necessary settings in the application to make sure that all application settings are saved, and exit the application.
5. Application Profiler stops monitoring and outputs the collected information as a Flex configuration file.

Launch User Environment Manager Management Console

Click on the UEM Management Console on the Main Console Desktop to launch the User Environment Manager Management Console.
Applications that have Profiles

In the left side expand the Applications folder and see which applications are recognized by UEM with profiles.

Make a note that there is not a Notepad++ or NPP listed under applications.

We are going to profile this application.

Minimize the UEM Management Console.

Let's look at UEM Application Profiler tool

From the Main Console Desktop click on the Application Profile app to open the UEM Application Profiler tool.
Application Profiler Overview

The application profiler produces 4 files upon completion of the profile:

1. INI - User Environment Manager configuration file containing the import and export locations. This file defines the parameters for User Environment Manager to manage the application.
2. ICO - Icon used by User Environment Manager Management Console and the Self-Support tool.
3. FLAG - Flag file for FlexEngine, when DIrectFlex is enable (default)
4. ZIP - Contains the predefined user settings. (Not to be opened directly. It is critical to use the Edit Profile Archive button in the Application Profiler. Using anything else will render the file unreadable by FlexEngine.)

Start Session

1. Click **Start Session** from the top left toolbar on Application Profiler.
2. Browse to and select the application in Programs-->Notepad++ then select Notepad++.
3. After you click OK, Application Profiler opens the application to be profiled and begins monitoring the changes you make and where those changes are saved in the Windows registry and file system.

Profiling Notepad++

We are going to make some changes in Notepad++.

1. From the menu bar, select Settings
2. Click on Preferences

Make some changes to Notepad++

![Screenshot of Notepad++ preferences settings]
1. From the Toolbar list, select **Big icons**.
2. **De-select the Show status bar** Show status bar check box.
3. **Close** the preferences box.

**Finish Application Profiling the App**

Close the Notepad++ application by clicking on the **X** in the top right corner of the Notepad++ application.

Application Profiler saves the changes you made, wait till it prompts you to confirm that profiling is finished.

Click **OK**
App Data

Application Profiler also displays the location in the file system where the Notepad++ configuration changes were made. In this case, settings were written to a Notepad++ subfolder of the AppData folder.

We can verify the location of Application Configuration Changes.

1. From Windows Explorer window type in
2. `%AppData%\Notepad++` to navigate to that path. (use grap and drag)
Verify Application Config Changes

The contents of the Notepad++ folder display including a updated config file.
Save the Config File

1. From the **UEM Application Profiler**, Click on **Save**
2. Click **Save Config File** from the choices.
3. Close the Application Profile by clicking on the **X** in the top right corner of the Application Profile window.

**Note:** Because we select Save Config File, rather than Save Config File with Predefined Settings, the preference settings we changed in this lab will NOT be present to end users or when we launch the Notepad++ application in the next steps. We changed preference settings in Notepad++ only so that Application Profiler could monitor and determine the path to the application configuration file.

*If you select Saving a Flex Configuration File with Predefined Settings, a profile archive is created to use for predefined settings when a user logs in.*
Save Config Files to Desktop

1. Save the files to the desktop by selecting Desktop in the left menu.
2. Give File name of NPP
3. Click Save

We created a config file to enable application personalization by the end user so that when an end user changes a Notepad++ preference, the user's preference will be saved across sessions and VMs.
Copy the Config Files

On the Main Console Desktop

Click on the desktop and drag up over these 3 files that were copied to the Main Console Desktop: **NPP.ini, NPP.ini.flag, NPP.ico**.

Once all three are selected, Right click on them and say **Copy**.

Remember the ini file is the application config file, the ini.flag file is the tells UEM to import and export the settings when the application starts/closes, and .ico is the icon file.
Paste the files to the Application Folder on Config Share

1. Navigate the Windows Explorer to C:\UEMProd\general\Applications
2. Paste the 3 files here by right clicking then select Paste.
1. Click back on the **UEM Management Console**. Be sure **NOT** to click on the Application Profiler window.
2. Click the **Refresh Tree Button** on the top left bar under Personalization.
Notepad++ is listed under Applications now

Now Notepad++ or NPP as we called it is located in the Application Personalization.

Viewing the Profile Archive

This is for informational purpose only, we will not be doing this step in the lab.
You can also view the Profile Archive of an application that you save. To view this zip file you need to use the Edit Profile Archive instead of opening the ZIP and editing.

This is for informational purpose only, we will not be doing this in the lab.

To see the file you would click on Edit Profile Archive and Select the application under C:\UEMProd\general\Applications\ 

Under the VMware UEM Profile Archive Settings is the Registry file. In the Registry folder there will be a Flex Profiles.reg file. This is the registry file that will get merged with the registry on the fly when THE APPLICATION is used on UEM enabled machines.

While you may be tempted to open and edit the ZIPfile directly from Windows Explorer, it is critical that the Edit Profile Archive button be used instead. User Environment Manager uses the standard ZIPfile format to prevent the creation of proprietary file formats, but the writes to and reads from the ZIPfiles are optimized for performance. Using tools outside of User Environment Manager to edit these ZIPfiles makes them unreadable by FlexEngine.

**Conclusion Application Profiler**

VMware provides application management templates for commonly-used software packages, and the VMware User Environment Manager Community Forum contains many more templates created with an included tool called Application Profiler.

Application Profiler is a standalone tool that helps you determine where in the file system or registry an application is storing its user settings. The output from Application Profiler is a configuration file which can be used to preserve and roam application settings for your end users. Optionally, you can record a default set of application settings, and apply and/or enforce these defaults for your users based on a variety of conditions.
Smart Policy

You can use Smart Policies to create policies that control the behavior of the USB redirection, virtual printing, clipboard redirection, client drive redirection, and PCoIP display protocol features on specific remote desktops.

With Smart Policies, you can create policies that take effect only if certain conditions are met. For example, you can configure a policy that disables the client drive redirection feature if a user connects to a remote desktop from outside your corporate network.

You use the User Environment Manager Management Console to create a Horizon smart policy in User Environment Manager. When you define a Horizon smart policy, you can add conditions that must be met for the smart policy to take effect.

What are Horizon Smart Policies?

With Smart Policies, administrators have granular control of a users desktop experience. A number of key Horizon 7 features can be dynamically enabled, disabled, or controlled based not only on who the user is, but on the many different variables available through Horizon 7: client device, IP address, pool name, and so on.

You can use Smart Policies to enable or disable features including clipboard redirection, USB access, printing, and client drive redirection. For example, you can create a policy so that a desktop login from outside the corporate network results in disabling of security-sensitive features such as cut-and-paste or USB drive access. Additionally, bandwidth profile settings allow you to customize the user experience based on user context and location.

Smart Policies can be enforced based on role, and evaluated at login and logout, disconnect and reconnect, and at predetermined refresh intervals. With all these capabilities and fine grain control, you can use one desktop pool to address many different use cases.

Note: In most cases, Smart Policy settings that you configure for remote desktop features in User Environment Manager override any equivalent registry key and group policy settings.

How Smart Policies are Applied

To create a Smart Policy, you select settings for the Horizon 7 features that you want to control and specify the conditions, if any, under which the policy will go into effect. If you do not specify any conditions, the policy is applied to all users in the user OU configured for User Environment Manager. Settings are always applied when the user logs in. You can optionally configure triggers to also re-evaluate the settings at other times, such as when users reconnect to the desktop or application.
Overview of lab

In this section of the lab, Horizon Smart Policies will be used to disabling USB Redirection, while conditionally enabling printing and clipboard use. This lab will feature Printer Mapping and Condition Sets in conjunction with Horizon Smart Policies.

Open UEM Management Console

Click on the Management Console on the Main Console desktop to launch the UEM Management Console.

Create Horizon Smart Policies

1. In the User Environment Manager Management Console, select the User Environment tab and click Horizon Smart Policies in the tree view.
2. Existing Horizon smart policy definitions, if any, appear in the Horizon Smart Policies pane. Right-click Horizon Smart Policies.
3. Select **Create Horizon Smart Policy** definition to create a new smart policy.

You can also select Horizon Smart Policies and then click on create to open the create Horizon Smart Policy dialog box.

**Create Smart Policies for Internal User**

![Horizon Smart Policies dialog box](image)

The Horizon Smart Policy dialog box appears.

In the Settings tab you define the smart policy settings.

1. In the General Settings section,
- Type a name for the smart policy in the Name text box: **Inside Corporate Network**
- Type a Label: **USB and Clipboard Enabled**
- Tag: **Internal**

2. In the Horizon Smart Policy Settings section, select the remote desktop features and settings to include in the smart policy. You can select multiple remote desktop features.
  - Click on box to enable **USB Redirection** and confirm it says **enabled**.
  - Click on **Clipboard** and select **Allow All**.

**Don't hit save button yet as we will set Conditions in next step.** If you went ahead and hit save you can click on the Internal Corporate Network Smart Policy and hit Edit then proceed to next step.
Add a Condition

To add a condition to the smart policy, select the Conditions tab, click Add, and select a condition.

You can add multiple conditions to a smart policy definition.

1. Click on the **Conditions** tab
2. Click **Add**
3. Select **Horizon Client Property**
Set the Client Location to Internal

1. For Property, select **Client location**
2. Set the location to **Internal**
3. Click **OK**

When you connect directly to a Connection Server, the gateway location is Internal. If you connect to a VMware Unified Access Gateway appliance or Security Server, the gateway location is External.
Save the Horizon Smart Policies

Click on Save to save the Horizon Smart Policy we just created with the condition.

The Smart Policy setting and condition are now defined. These settings are always evaluated and applied whenever the user logs in. You can specify an event that triggers the reevaluation of the Smart Policy whenever the user reconnects, rather than logs in. This is called a triggered task.

Overview of Features controlled by Smart Policies

*The features controlled by Smart Policies.*
You can use Smart Policies to enable, restrict, or disable Horizon 7 features that include clipboard redirection, USB access, printing, and client drive redirection, and you can select a profile that manages bandwidth usage.

- **USB redirection** - Controls whether a user is allowed to use locally attached USB devices, such as thumb flash drives, cameras, and printers, from the remote desktop.
- **Printing** - Controls if a user is allowed to print documents from the remote desktop to a network printer or a USB printer that is attached to the client computer.
- **Clipboard** - Controls whether users are allowed to copy and paste text and graphics only from the client system to the remote desktop, only from the remote desktop or application to the client system, or both, or neither.
- **Client drive redirection** - Controls whether drives and folders on the client system are shared with the remote desktop and, if so, whether they are readable only or readable and writable.
- **HTML Access file transfer** - (available with User Environment Manager 9.1 and later) Controls whether you can upload files from the client system to the remote desktop, download files from the remote desktop to the client system, or both, or neither, when you are using the web client to access the remote desktop. Note that this feature requires Connection Server and Horizon Agent 7.0.1 or later.
- **Bandwidth profile** - Prevents the agent (remote desktop) from attempting to transmit data at a higher rate than the link capacity.

**Copy some data to the Clipboard**

![Clipboard](image-url)
We are going to grab some data to put in the clipboard to show how we can paste to the Desktop.

1. Open the **README.txt** file on the Main Console Desktop by double clicking it. It will open in Notepad app.
2. Click on some text in this file to highlight by double clicking on a line or holding down left mouse to select some text.
3. Right click in the document and select **Copy**

**Open VMware Horizon Client**

We will now test connecting in as an internal user using the VMware Horizon Client.

Click on VMware Horizon Client to open up the Horizon Client.

**Connect Through the Horizon-01 Server**

Click the **horizon-01.corp.local** server.

We will show how we enabled the ability to paste from the clipboard.
Login the user4mod3 user

![Login screen]

Login as user4mod3 user with password of VMware1! and click Login.

Connect to the Instant Clone Pool

![Instant Clone Pool]

Double-click the Instant Clone Pool to bring up the Instant Clone Desktop.

It may take a minute to bring up the Desktop since we are in a nested lab environment.

Open Wordpad

![Wordpad]

Double-click on Wordpad (created by VMware UEM) to open the Wordpad application
Paste the Data from the Clipboard

1. In the Wordpad application click on the Paste icon in the left top of the window. You can also right click in the area and select Paste.
2. You were able to Paste the text from the Clipboard.
3. Click the X in the top of the window to exit the application and if prompted confirm exit without saving the document.
Close Wordpad and Disconnect from desktop

1. Close the Wordpad app by clicking X in top right corner of Wordpad window.
2. To Disconnect and Log Off from the Desktop, Click on Options in the top left corner of the Desktop window
3. Click on Disconnect and Log Off. Click OK when asked are you sure.
Disconnecting from the Horizon-01 Server.

1. Click the Disconnect symbol in the top left of the VMware Horizon Client window.
2. Confirm by clicking OK when prompted.
Horizon Smart Policies External

Now we will set a Horizon Smart Policy and Condition based on an external user to the system. This user will not have access to copy/paste or printing.

1. In the User Environment Manager Management Console, select the User Environment tab and click Horizon Smart Policies in the tree view.
2. Select Create to create a new Horizon Smart Policy for external users.
Create External Access Smart Policies

The Horizon Smart Policy dialog box appears.

In the Settings tab you define the smart policy settings.

1. In the General Settings section,
   - Type a name for the smart policy in the Name text box: **External Horizon Session**
   - Type a Label: **No Clipboard or Printing**
   - Tag: **External**
2. In the Horizon Smart Policy Settings section, select the remote desktop features and settings to include in the smart policy. You can select multiple remote desktop features.
   ◦ Click on box to enable **Printing** and confirm it says **Disabled**.
   ◦ Click on **Clipboard** and select **Disabled**.

**Don't hit save button yet as we will set Conditions in next step.** If you went ahead and hit save you can click on the External Horizon Session and hit Edit then proceed to next step.

**Add a Condition for External User Smart Policy**

![Add Condition for External User Smart Policy](image-url)
1. Click on the **Conditions** tab
2. Click **Add**
3. Select **Horizon Client Property**

### Set the Client Location to External

![Image of Horizon Client Property dialog box]

1. For Property, select **Client location** from the drop down
2. Set the location to **External**
3. Click **OK**
Set a second condition set for External

We will set a second condition for External access.

1. Click on **Add**
2. Click **Remote Display Protocol**
1. From the pull down for Remote display protocol select **Blast** and click **OK**.

Click on **Save** to save the Horizon Smart Policy we just created with the condition.

The Smart Policy setting and condition are now defined. These settings are always evaluated and applied whenever the user logs in. You can specify an event that triggers the reevaluation of the Smart Policy whenever the user reconnects, rather than logs in. This is called a triggered task.
Remember by default: When you connect directly to a Connection Server, the gateway location is Internal. If you connect to a VMware Unified Access Gateway appliance or Security Server, the gateway location is External.

Copy Text into the Clipboard

1. Open the Readme file on the Main Console Desktop
2. Highlight some text and right click
3. Select Copy

Connect Through the VMware Unified Access Gateway

This time we will connect in through the VMware Unified Access Gateway to show how an external user would access the environment.
1. Click back on the **VMware Horizon Client** to open the window back up if you minimized it.
2. Click the **uag-01.corp.local** server to connect to the Unified Access Gateway. *It might be in a different order than pictured above.*

We will show how we disabled the ability to copy/paste to the clipboard.

**Login the user4mod3 user**

![Login Screen]

Login as user4mod3 user with password of VMware1! and click Login.

**Connect to the Instant Clone Pool**

![Desktop Screen]

Double-click the Instant Clone Pool to bring up the Instant Clone Desktop.

It may take a minute to bring up the Desktop since we are in a nested lab environment.

**Open the Wordpad Application**
Double-click on the Wordpad (created by VMware UEM) on the desktop to launch Wordpad.

**External User No Paste**

![Image of Wordpad with Paste option greyed out]

Notice Paste in the top left of the window is greyed out.

Also if you right click in the document, Paste is greyed out here as well.

You are not able to paste into this environment due to the Horizon Smart Policy.
Close Wordpad and Disconnect from desktop

1. Close the Wordpad app by clicking X in top right corner of Wordpad window.
2. To Disconnect and Log Off from the Desktop, Click on Options in the top left corner of the Desktop window
3. Click on Disconnect and Log Off. Click OK when asked are you sure.
Disconnecting from the UAG-01 Server.

1. Click the Disconnect symbol in the top left of the VMware Horizon Client window.
2. Confirm by clicking OK when prompted.

Close VMware Horizon Client

Click the X in the top right corner to close the VMware Horizon Client.
Close the README.txt File

Click the X in the top right corner to close the README.txt file.

Processing Smart Policies

User Environment Manager processes the Horizon smart policy each time a user connects or reconnects to the remote desktop.

User Environment Manager processes multiple smart policies in alphabetical order based on the smart policy name. Horizon smart policies appear in alphabetical order in the Horizon Smart Policies pane. If smart policies conflict, the last smart policy processed takes precedence. For example, if you have a smart policy named Sue that enables USB redirection for the user named Sue, and another smart policy named Pool that disables USB redirection for the desktop pool named Win7, the USB redirection feature is enabled when Sue connects to a remote desktop in the Win7 desktop pool.
Application Blocking

Application blocking allows you to enable or block applications from launching. Also called application authorization, this feature enables administrators to build blacklists and whitelists of applications to control application and license sprawl. You can also create condition settings to control the circumstances under which an application can be used. For example, you can create a condition that allows a user access to company-specific applications only when the user is on the internal corporate network.

By default, once you enable application blocking, only applications from the Windows folder, C:\Program Files, and C:\Program Files (x86) are allowed to run. To fine-tune application blocking, you can further specify applications to allow or block based on path, hash, or publisher.

You can configure the following types of application blocking:

- **Path-based.** You can specify a path to a folder. Or, you can specify a fully qualified file name (the configured path includes the full path and file name of the executable).
- **Hash-based.** You can specify to allow or block based on a hash that matches a particular executable.
- **Publisher-based.** You can specify a publisher to allow, and executables associated with that publisher can launch. You cannot block applications by publisher.

Note: If you configure multiple types of application blocking, it is important to understand the order in which they are evaluated.

Enable and Configure Application Blocking

Application blocking is disabled by default. You must enable it manually, configure conditions to control the users eligible for application blocking, and define a custom message.

Launch User Environment Manager

Open the UEM Management Console from the Main Console desktop by Double-clicking on the Icon **UEM Management Console** on the desktop.
If UEM is still open from previous lesson then you can continue to the next step.

**Bring up Application Blocking**

1. Click on **User Environment**
2. Click on **Application Blocking**
3. Click on **Global Configuration**
Global Configuration of Application Blocking

You will notice that Application Blocking is turned off by default.

1. Click the Check box to **Enable** Application Blocking
2. Click OK
Click OK
Horizon HTML Access

1. Open Chrome Browser
2. Select the VMware Horizon bookmark
3. Select VMware Horizon HTML Access
Login to VMware Horizon

Login to Horizon HTML Access:

1. Change username to: `user4mod3` *(please make sure to change default user)*
2. Password: `VMware1!`
3. Click **Login**
Launch the Instant Clone Desktop

Double Click the Instant Clone Pool to launch the desktop. It will automatically log user4mod3 user into the desktop.
Launch Run from Desktop

1. Right Click the Windows in the bottom left corner
2. open up Run.

Run the command prompt
Type `C:\windows\system32\cmd.exe` in the Open: prompt for Run (use click & drag)

**Command Prompt Launces Successfully**

![Command Prompt Screenshot]

Note the command application opens successfully.

You might see a pop up that applications are blocked but we are able to launch this app. We will specifically block this app in the next steps.
Lock the Desktop

1. Click on the Window in the bottom left corner
2. Click on the Person icon
3. Click lock

We will be using this desktop more in a minute. We set a Triggered Task so that the UEM Application Blocking will be refreshed upon Unlock of the Desktop. We did this so we didn’t have to wait on the Instant Clone Desktop to be provisioned after disconnect.

Open up the UEM Management Console

If not already open, click on the Production environment at the bottom of the desktop to reopen the UEM Management Console.
Allow and Block Applications

1. Under the User Environment Tab
2. Click on **Application Blocking**
3. Click on **Create**
Application Blocking Settings

We are going to block the Command application from launching.

1. Under Settings Type for the Name: **Command Blocking** and Label: **CMD**
2. Under Block, Click on **Add**
Select path to block

1. You can either type path above `C:\Windows\System32\cmd.exe` or click on Select File.... and navigate to the file. (Use Click & Drag)
2. Click OK
Save Application Blocking

Click on Save.
Confirm Application Blocking

You should now see the Application Blocking is enabled and you have the Command Blocking Application blocked.

Now we will see that this is blocked when we try to run it as a user.

Minimize the UEM Management Console.
Unlock the Horizon HTML Access Desktop

1. Open the Desktop back up by clicking on the Chrome Browser tab for the Horizon HTML Access
2. Click in the Desktop to get the prompt for password to unlock: Enter password: VMware1! and hit return.

Click on the background desktop to close the window prompt.
Launch Run from Desktop

Right Click the Windows in the bottom left corner and open up Run.

Run the command prompt

Type CMD in the Open box of Run.
Does the cmd prompt launch?

A message is displayed saying command was blocked.
Click OK to continue as this is expected since you just blocked that application.

Sign out of the Desktop

1. Click on the Window in the bottom left corner
2. Click on the Person icon
3. Click Sign Out
Disable Application Blocking

In the UEM Management Console be sure to disable Application Blocking as some of the next steps in this lab may be impacted.

1. From UEM Management Console
2. Click on **User Environment** tab at the top
3. Click on **Application Blocking**
4. Click on **Global Configuration**
5. **Uncheck** the box for **Enable Application Blocking** in order to disable it
6. Click **OK**

In this Lesson, we demonstrated how to turn on Application Blocking and block an application from running.
Privilege Elevation

With privilege elevation, administrators can now allow end users to run certain applications as administrators, as well as install their own applications if they meet the specified criteria. IT administrators can create rules that elevate privileges based on a file hash, a software publisher, or a path to a file or folder.

Overview

- User Environment Manager administrators pre-define applications to run or install using elevated privileges.
- Standard user accounts can run these applications as if they were a member of the local administrators group
- This improves security by removing local administrator privilege from domains users, while enabling elevation for specific applications.

Use cases for Privilege Elevation

1. Elevated Application
   - Use to elevate applications that are already installed
   - Used for legacy apps requiring local admin rights to run

2. User Installed Applications
   - Use this to elevate application installers
   - Used for application installers requiring local admin rights to install
   - Create a repository from where users can install approved software

Privilege Elevation Overview

Privilege Elevation is disabled by default. You must enable it manually, configure conditions to control the elevated applications, and define an elevation message.

Note: If you use application blocking, by default only applications in Program Files and Windows are allowed to run. You might need to create an allow setting to enable the application to run.

Argument-Based Privilege Elevation

Configure executables to be elevated only if they are invoked with specific arguments. Elevation options now available:

- Argument-based
- Hash-based
• Path-based
• Publisher-based

Benefit is improved security when elevating certain EXEs and enable user to execute only specific scripts in the context of a local administrator.

With Argument-based Privilege Elevation, if the EXE is run with a matching argument, the EXE is elevated. If the EXE is run with any other arguments (or none), the EXE runs in context of the user.

**Preparing for the Demo**

We will be using some scripts to show the Argument Based Privilege Elevation.

- **PEdemo.vbs**: This will be the Argument and refers to a vb script located in UEMS-scripts folder. This script invokes a second executable (legacyapp.exe)
- **legacyapp.exe**: This executable is designed to show when it is run as a user or as an administrator
- **legacyapp.exe.config**: config file for the executable

We need to move the scripts in order to use for Privilege Elevation.
Copy the PEdemo.vbs Script

First we will copy the PEdemo.vbs script to the Scripts directory of the UEMProd.

1. Open the Windows File Explorer,
2. Navigate to C:\Tools\UEM-Lab
3. Right click on the file PEdemo.vbs script
4. Select Copy.

We are copying this file to be pasted in the script folder in the next step.
Put file in the Scripts Folder
We will create Scripts folder in C:\UEMProd\general\FlexRepository and copy our script into this folder for use later.

1. Go to the C:\UEMProd\general\FlexRepository folder and **right click**.
2. Select **New** and **Folder**
3. Type **Scripts** and return
4. And copy PEdemo.vbs file into this folder by **Right Click** on the newly created Scripts folder and select **Paste**.

We are putting the script we will be using into the UEM Scripts folder so that we can use it later.

**Copy the Legacy App Files**

![Image of UEM Lab interface showing the path to the Legacy App files]

We also need to copy the legacyapp.exe and the legacyapp.exe.config file into UEM custom file and folders to share with Desktop.

**We will copy the two files here and will be pasting them in the next few steps from within the UEM Manager.**

1. Go into the C:\Tools\UEM-Lab folder on the Main Console
2. Select both files: **LegacyApp.exe** and **LegacyApp.exe.config**.
3. **Right Click** to **Copy**
Open up the UEM Management Console

From the Main Console, double-click the Management Console shortcut on the desktop. This will open up the User Environment Manager Management Console.

If you have UEM still open from the previous lesson, then you can proceed to the next step.

You may need to minimize the Windows Explorer Windows or Chrome Browser so you can see the desktop.

Set up Files and Folders to Share Script to Desktop

We are going to add customer files to the user environment. We will set up the files to share on the User's Desktop upon login.

1. Click on the **User Environment**
2. Click on **Files and Folders**
3. Click **Create**
4. Enter **PE Demo** for the Name and Label
5. Click on **Create** under Files and Folders Settings

We will paste those files to the User's Desktop by UEM when the user logs into the Windows 10 Instant Clone desktop.
Add Files for Windows 10 Share

The window will pop up for the VMware UEM Profile Archive Settings.

**Right click** over the Desktop in the middle pain and select **Paste** to copy those files into the Desktop folder.
Complete Adding Custom File to Desktop
1. Click X to close the Desktop window inside VMware UEM Profile Archive Settings
2. Back on the Files and Folders Box, Click **Done**.
3. Click **Save**.

We have copied those two files into the Users Desktop through UEM for when you log in as user.

**Privilege Elevation**

We are going to enable Privilege Elevation. It is disabled by default.

1. On the **User Environment** tab
2. Select **Privilege Elevation**.
3. Click **Global Configuration**.
Enable Privilege Elevation Overview

1. Select Enable Privilege Elevation. It is disabled by default.
2. Select Also elevate all child processes to elevate child processes on a global level. If you select this option, all processes of a user-installed application run elevated.
3. Click OK.

In this section you also have the ability to configure conditions to control the elevated applications. We are not going to configure any conditions in this lab. You also can add a Message to display with User-installed apps. You would select Ask user to elevate in the Message section to display a message when a user launches an application that is configured for elevation. The user is presented with the option to run the application elevated or with the normal privileges of the user. We will not be doing that in this lab.
Warning for Privilege Elevation

The Privilege Elevation feature grants temporary administrator privileges to a user. The feature must be used only for specific use cases by administrators. It is not intended as a security feature. Use additional security measures to prevent malicious use.

Click **OK**.
Configure Argument-based Privilege Elevation

We are going to configure Argument-based Privilege Elevation.

1. On the User Environment tab, select **Privilege Elevation**.
2. Click **Create**.
3. Enter a name for the setting definition: **PE Demo**
4. Enter Label: **PE Demo**
5. Click on **Also elevate child processes**
6. Select the privilege elevation type from the Type drop-down under Privilege Elevation Settings: **Argument-based elevated application**
   - You can only use folders for user-installed applications.
   - If you are configuring path-based settings that reference network paths, specify UNC paths instead of drive letters. When users launch these applications, they should access them from the UNC path.
7. Click **Add** in the Elevate section

Select Executable and Arguments to elevate

![Privilege Elevation dialog box]

You can use the selection tool to highlight any text below and drag the hand to the lab to paste text instead of typing it in the demo environment.

1. Select the folders or applications to add to the list: *(Use Click & Drag)*
   - Executable: `C:\Windows\System32\wscript.exe`
   - We have to put in the entire path for the executable.
   - Argument: `%UEMScripts%\PEdemo.vbs`
This Argument refers to a vb script located in UEMScripts folder. The script invokes a second executable that is designed to show when it is run as a user or as an administrator.

2. Verify that **Case-sensitive arguments** is enabled. We will demonstrate using correct case to run as elevated privilege or not.
3. Click **OK** in the Select executable and arguments to elevate box
4. Click **Save** for the Privilege Elevation box

**Minimize the UEM Management Console**

Minimize the UEM Management Console so we can launch a desktop.
Horizon HTML Access

If you have the Instant Clone Desktop still open from the previous lesson, then you can open the Instant Clone Desktop from the Chrome Browser for User4Mod3 and enter the password: VMware1!

1. Open Chrome Browser
2. Select the **VMware Horizon** bookmark
3. Select **VMware Horizon HTML Access**
Login to VMware Horizon

Login to Horizon HTML Access:

1. Change username to: **user4mod3** *(please make sure to change default user)*
2. Password: **VMware1!**
3. Click **Login**
Launch the Instant Clone Desktop

Double Click the Instant Clone Pool to launch the desktop. It will automatically log user4mod3 user into the desktop.

Confirm the Files are on the Users Desktop

The files we added to the UEM share are present on the users desktop upon login. Notice LegacyApp.exe and LegacyApp.exe.config are on the desktop.
Open run

1. **Right-click on the window** in the bottom left corner
2. Select **Run** from the menu
Run the wscript.exe with correct argument

For this first test we will run wscript.exe executable with the argument that is formatted properly.

Make sure to use case sensitive with the script paying particular attention to PEdemo.vbs case.

You can click on the text in step one below and drag with the handtool to the desktop instead of typing out the text.

In the Run window type in the Open box: *(Use Click & Drag)*

1. C:\windows\system32\wscript.exe %UEMScripts%\PEdemo.vbs
2. Click on OK

Invoke Remote Executable message

Windows Script Host box pops up saying the VBScript will invoke a remote executable.

Click OK

If you get a pop up about needing a script from the internet to run just click cancel.
Notice running as Admin

Observe that Privilege Elevation executed wscript.exe and the secondary application with administrative privileges.

Click X in the top right corner of the Demo Tool window to close the box.

Run the wscript.exe with incorrect argument

For this test we will run the wscript.exe executable with the argument improperly formatted.

Right click on the window and click Run.

In the Run box type with the argument pedemo.vbs in lower case letters. (Use Click & Drag)

1. `c:\windows\system32\wscript.exe %UEMScripts%\pedemo.vbs`
2. Click OK
Windows Script Host Box

Click **OK** to continue to the secondary script.

If you get a popup about Search for app in the Store? Click **NO**.

**Notice runs as user**

The second app now runs in the context of the user not as Administrator. *wscript.exe* was not elevated since argument case did not match that of the privilege elevation rule.

Click the X in the top right corner of the Demo Tool to close the window.
You could also update the rule so that child processes are not run with elevated privileges. When you rerun wscript.exe with the correct syntax for the argument, wscript.exe was run with admin privilege but the child process will not.

You can test this if you want or go ahead and logout to clean up the environment.
Lock the Desktop

1. Click on the Window in the bottom left corner
2. Click on the Person icon
3. Click lock

We will be using this desktop more in the next lesson.

Close UEM Management Console

Click the X in the top right corner of the UEM Management Console window.

In this lesson, we set up Argument-based Privilege Elevation where we configured executables to be elevated only if they are invoked with specific arguments. We also customized the user desktop by adding custom files to the user environment to be on the desktop at login.
Integration with Logon Monitor

With VDI it is important to understand how changes impact users and make sure they have a good impression and experience. The first thing they will see is logon time and it is critical that the solution is not negatively impacted to yield longer logon times. It is important to get a good understanding on what is affecting the logon speed.

That is where VMware Logon Monitor comes in. It measures the logon process and reports on what's happening during a user logon.

What is VMware Logon Monitor

VMware Logon Monitor monitors Windows user logons and reports a wide variety of performance metrics intended to help administrators, support staff, and developers troubleshoot slow logon performance. Metrics include, but are not limited to, logon time, CPU/memory usage, and network connection speed. VMware Logon Monitor also receives metrics from other VMware products which provide even more clues about what is happening during the logon flow.

While other VMware products are not required to benefit from VMware Logon Monitor, some VMware products may be active during user logon. The Horizon Agent, Horizon Persona Management, and App Volumes are examples and report additional metrics which further enhance the value of VMware Logon Monitor’s logs.

Integration with Horizon VMware Logon Monitor Service

User Environment Manager continues to improve Horizon 7 integration with the VMware Logon Monitor service (VMLM) feature. VMLM collects and logs information during the login process to the following file:

C:\ProgramData\VMware\VMware Logon Monitor\Logs\vmlm.txt

Both App Volumes and User Environment Manager add events to this log file, providing a comprehensive log file for events that occur during login to Horizon 7 desktops.

Logon Monitor Included in Horizon 7.1 or Higher

Logon Monitor is included by default with Horizon 7.1 and higher releases. If you are using an older version of Horizon, there is a Fling you can download to get this functionality.
Unlock the Instant Clone Desktop

We will use the Instant Clone Desktop that we used in the previous lesson. If you signed out and closed the desktop then you will need to open Chrome and click on the VMware Horizon favorite to sign in as User4Mod3 and launch Instant Clone desktop again.

These steps are to unlock the Instant clone Desktop you previously had open:

1. Click on the **VMware Horizon Desktop** that is running in the Chrome Browser
2. Click on the background to bring up the User4Mod3 user logged in
3. Unlock by entering password for User4Mod3: **VMware1!**
Let's Open the VMLM log file

1. Open Windows File Explorer
2. Navigate to the folder C:\ProgramData\VMware\VMware Logon Monitor\Logs. This is a hidden folder so you will need to type it or click and drag the folder path.
3. We will look at the vmlm text file so double click on the file vmlm to open it in Notepad for viewing.

Note: If you changed the font and clicked on wordwrap in the previous labs for Notepad, you can click on the pulldown under format for notepad and uncheck wordwrap. You can also edit the font and change size for better viewing of the file.
Search for data in the VMLM Log File

1. Click on **Edit** button for Notepad and click on **Find**.
2. You can search for **UEM** or **Logon** to see the data is populated in the file.
3. Click **Find Next** to see what UEM log data is captured.
4. Click the **X** in top right corner of the Notepad window to close the file when done.
Sign out of Desktop

1. Click on the Window in bottom left corner
2. Select the person
3. Click **Sign out**

Click **Close** to the You have been disconnected message.
Conclusion

In this module we went over User Environment Manager. We looked at Application Customization, Application Profiling, Horizon Smart Policies, Application Blocking, Privilege Elevation and UEM Integration with Logon Monitor.

You've finished Module 3

Congratulations on completing Module 3.

If you are looking for additional information on User Environment Manager, try one of these:

- Click on this [https://www.vmware.com/products/user-environment-manager.html](https://www.vmware.com/products/user-environment-manager.html)
- Or go to [https://tinyurl.com/ybtxqx89](https://tinyurl.com/ybtxqx89)
- Or go to [https://techzone.vmware.com](https://techzone.vmware.com)
- Or use your smart device to scan the QRC Code.

This concludes HOL-1951-06-VWS lab. You can go Proceed to any module below which interests you most.

- **Module 1 - Just-in-Time Management Platform - Deep Dive** (60 minutes)
- **Module 2 - App Volumes - Deep Dive** (60 minutes)
- **Module 3 - User Environment Manager (UEM) - Deep Dive** (60 Minutes)
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-1951-06-VWS

Version: 20181112-174543