TECHNICAL WHITE PAPER – **JULY 2017**

BEST PRACTICES FOR PUBLISHED APPLICATIONS AND DESKTOPS IN VMWARE HORIZON APPS AND VMWARE HORIZON 7

VMware Horizon 7 version 7.2
VMware Horizon Apps version 7.2

Table of Contents

Introduction

VMware Horizon® 7 provides virtual desktop solution as well as an enterprise-class, application-publishing solution. For users who do not require personalized virtual desktops and who handle a standard set of tasks, VMware Horizon Apps is the ideal solution. Horizon Apps offers published applications and session-based desktops, without VDI.

Horizon Apps leverages Microsoft RDSH servers to deliver published applications or desktops. Data, applications, and desktops are centrally managed and secured. Users access their published applications and desktops from a single digital workspace, through single sign-on from any authenticated device or OS.

Critical Horizon 7 features and components, such as the Blast Extreme display protocol, instant-clone provisioning, VMware App Volumes™ application delivery, and VMware User Environment Manager™, are integrated with published applications and desktops to provide a seamless user experience and an easy-to-manage, scalable solution.

Published applications and desktops provide the opportunity to reduce hardware, software, and operating costs, and simplify installation, upgrades, and troubleshooting.

When deploying an RDSH-based Horizon Apps solution, administrators must take a number of considerations and best practices into account. Areas to consider include VMware ESXi host sizing, RDSH image configuration and optimization, Horizon 7 configuration and policies, antivirus solutions, provisioning, and recurring maintenance.

Administrators will also want to consider integrating VMware JMP technologies, which include VMware Instant Clone Technology, App Volumes, and User Environment Manager.

JMP – Next-Generation Application and Delivery Platform

JMP (pronounced *jump*), which stands for Just-in-Time Management Platform, represents capabilities in VMware Horizon 7 Enterprise Edition and Horizon Apps Advanced Edition that deliver Just-in-Time Desktops and Apps in a flexible, fast, and personalized manner. JMP is composed of the following VMware technologies:

- Instant Clone Technology for fast desktop and RDSH provisioning
- App Volumes for real-time application delivery
- User Environment Manager for contextual policy management

JMP allows components of a desktop or RDSH server to be decoupled and managed independently in a centralized manner, yet reconstituted on demand to deliver a personalized user workspace when needed. JMP is supported with both on-premises and cloud-based Horizon 7 deployments, providing a unified and consistent management platform regardless of your deployment topology.

The JMP approach provides several key benefits, including simplified desktop and RDSH image management, faster delivery and maintenance of applications, and elimination of the need to manage "full persistent" desktops.

Purpose

This guide provides best practices for anyone deploying a published application or published desktop solution based on Horizon 7.

Audience

This guide is for anyone installing or administering Horizon 7 or Horizon Apps. Readers should be familiar with basic installation and administration procedures, such as those described in Publishing Applications with VMware Horizon 7.

Organization of This Document

As you set up and configure your Horizon Apps deployment, you need to consider

- General vSphere best practices
- vSphere storage and networking best practices
- Core services infrastructure best practices
- ESXi host sizing best practices
- Remote Desktop Session Host configuration best practices
- Horizon 7 best practices
- User Environment Manager policy configuration best practices
- App Volumes best practices
- Antivirus configuration best practices
- Maintenance operations best practices

General vSphere Best Practices

Like any VMware deployment, Horizon 7 relies on hardware that is compatible with the appropriate versions of VMware vSphere® and VMware vSAN™ and configured according to VMware best practices.

System and Hardware Requirements

Before deploying a system, perform the following tasks:

- Verify that all hardware is compatible with the version of the VMware products that you plan to use. See the VMware Compatibility Guide.
- If you are using vSAN, ensure that all hardware, including disk controllers, are compatible. See the VMware Compatibility Guide – vSAN Components.
- Make sure that your hardware meets the minimum system requirements for the VMware products that you plan to use. See the Horizon 7 Documentation and the vSphere 6 Documentation.
- Consider using the latest version of Horizon 7 and the latest versions of ESXi and VMware vCenter Server® that are supported.

  For example, Horizon 7.1 requires ESXi 6.0 Update 2 or later and vCenter Server 6.0 Update 2 or later when not enabling TLS v1.0.
- Test your system memory for 72 hours, checking for hardware errors. For instructions, see the hardware manufacturer's documentation.

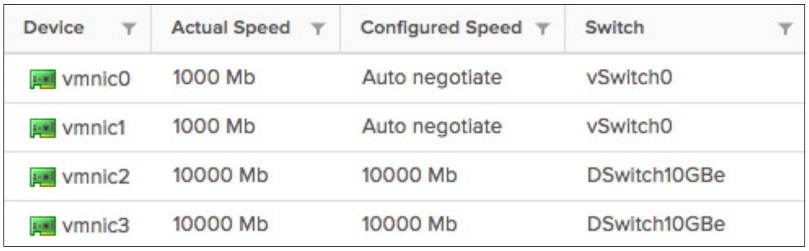
Network Adapter Recommendations

For the best networking performance, use network adapters that support the following hardware features:

- Checksum offload
- TCP segmentation offload (TSO)
- Large receive offload (LRO)
- Receive-side scaling (RSS)

When using load balancing across multiple physical network adapters connected to one vSwitch, make sure that all the NICs have the same line speed.

Figure 1 shows an example of the proper configuration. The two adapters vmnic0 and vmnic1 are connected to vSwitch0 and both have a line speed of 1000 Mb. The adapters vmnic2 and vmnic3 are connected to DSwitch10GBe. Both have a line speed of 10000 Mb.



Device	Actual Speed	Configured Speed	Switch
vmnic0	1000 Mb	Auto negotiate	vSwitch0
vmnic1	1000 Mb	Auto negotiate	vSwitch0
vmnic2	10000 Mb	10000 Mb	DSwitch10GBe
vmnic3	10000 Mb	10000 Mb	DSwitch10GBe

Figure 1: Multiple Network Adapters Connected to the Same vSwitch

ESXi Host General BIOS Settings

The following recommendations are for ESXi host BIOS settings:

- Run the latest BIOS version available for your system, as listed in the VMware Compatibility Guide.

  Note: After updates to the BIOS, review the BIOS settings in case new options have become available or the settings for existing options have changed.
- Enable all populated processor sockets and all cores in each socket.
- Enable Turbo Boost if your processors support it.
- Enable hyper-threading for processors that support it.
- Disable node interleaving (that is, leave NUMA enabled).
- Enable hardware-assisted virtualization features (VT-x, AMD-V, EPT, RVI, and so on).

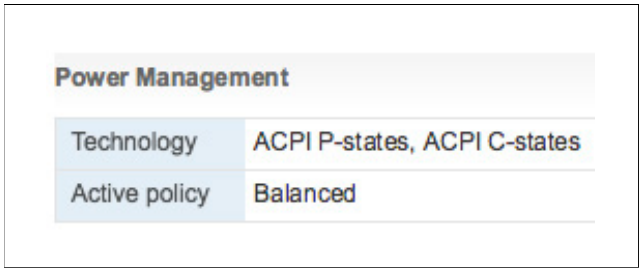
  Note: If you make changes, some systems might need to be powered off for the changes to take effect.
- Disable the devices you do not plan to use, such as unneeded serial, USB, or network ports.

ESXi Host Power-Management BIOS Settings

ESXi includes management capabilities that can save power when a host is not fully utilized.

Configure the BIOS settings to allow ESXi the most flexibility for the power-management features offered by your hardware and then make your power-management choices within ESXi. For example, disable all hardware-controlled power management features, but enable all power-management features that the operating system can control.

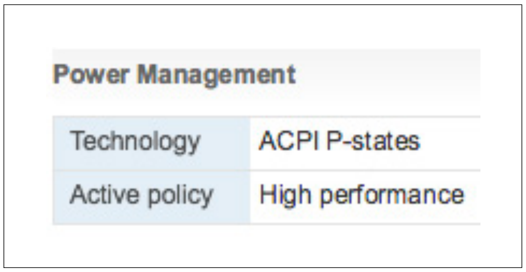
For the management cluster, the recommended power option is **Balanced**.



Power Management

Technology	ACPI P-states, ACPI C-states
Active policy	Balanced

For the resource cluster, the recommended power option is **High performance** because it allows the highest user density and provides consistent performance.



Power Management

Technology	ACPI P-states
Active policy	High performance

vSphere Storage and Networking Best Practices

To create a vSphere infrastructure that supports Horizon 7, you must follow particular storage and network guidelines.

General Storage Guidelines

Storage guidelines include recommendations for iSCSI performance and ESXi.

iSCSI Recommendations

Using jumbo frames with iSCSI can reduce packet-processing overhead, thus improving the CPU efficiency of storage I/O. For the best iSCSI performance, enable jumbo frames when possible. See the VMware knowledge base article iSCSI and Jumbo Frames configuration on VMware ESXi/ESX (1007654).

ESXi also supports jumbo frames for hardware iSCSI.

- To use jumbo frames with an independent hardware iSCSI adapter, enable jumbo frame support in the iSCSI storage array and any hardware network switches through which the traffic will pass.
- To use jumbo frames with a dependent hardware iSCSI adapter or with software iSCSI, enable jumbo frame support in the storage array, any hardware network switches through which the traffic will pass, and both the vmknic and the vSwitch in ESXi.

ESXi Storage Recommendations

The number of LUNs in a storage array and the way virtual machines (VMs) are distributed across those LUNs can affect performance.

Provisioning more LUNs with fewer VMs on each LUN can enable the ESXi servers to simultaneously present more I/O requests to the array. This setup has the potential to improve performance by ensuring full utilization of all array resources and giving the array more opportunities to optimize the I/O.

However, provisioning too many LUNs, especially when many ESXi servers are connected to a single array, can allow the ESXi hosts to simultaneously send so many I/O requests that they fill the array queue, and the array returns QFULL/BUSY errors. This situation can reduce performance due to the need to retry the rejected I/O requests.

Check with your storage vendor for the recommended settings.

Networking Recommendations

To ensure optimal network performance, we recommend using the vSphere Network I/O Control feature to control bandwidth. We also recommend using the VMXNET3 network adapter whenever possible.

Network I/O Control Feature

Network I/O Control (NetIOC) allows you to allocate different amounts of network bandwidth to specific network resource pools. You can create user-defined resource pools or select from among nine predefined resource pools:

- Management traffic
- Fault-tolerance traffic
- iSCSI traffic
- NFS traffic
- VMware vSAN traffic
- VMware vSphere vMotion® traffic
- VMware vSphere Replication™ traffic
- VMware vSphere Data Protection™ backup traffic
- VM traffic

Each resource pool is associated with a port group. When network resource pools are not split across physical network adapters, we recommend using NetIOC. For more information, see *vSphere Network I/O Control* in the vSphere Networking Guide.

VMXNET Network Adapters

The VMXNET family of paravirtualized network adapters provides better performance in most cases than emulated adapters, which include E1000e. VMXNET network adapters implement an idealized network interface that passes network traffic between the VM and the physical network interface card with minimal overhead.

The VMXNET network adapters—especially VMXNET3—also offer performance features not found in other virtual network adapters. For optimal performance, use VMXNET3. For more information, see *Network Adapter Types* in the vSphere Virtual Machine Administration Guide.

Core Services Infrastructure Best Practices

All core infrastructure components, such as Active Directory (AD), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP), Key Management Service (KMS), and Remote Desktop Licensing (RD Licensing), need to be highly available per site. When servers for these components are running as VMs, affinity rules need to be in place so that when a host or rack goes down, these services remain operational. For more information, see *vSphere HA and DRS Affinity Rules* in the vSphere Availability Guide.

Active Directory

To apply group policies to the RDS hosts that deliver remote desktop or application sessions, without affecting other Windows computers in the same AD domain, create an organizational unit (OU) specifically for your RDS hosts. This OU cannot have inheritance or linked GPOs applied to nonvirtual machines.

Domain Name Services

Make DNS servers highly available on every site. When running virtual affinity rules, set up the servers so that the instances are not running on the same host or rack.

Dynamic Host Configuration Protocol

Make sure that the subnet and DHCP pool are large enough—or prepare for multiple VLANs—to accommodate growth. When using instant clones, the lease time is not important because an instant clone releases the IP address before deleting the VM.

Network Time Protocol

For management and RDSH VMs and ESXi hosts, use AD as the NTP source.

Key Management Service

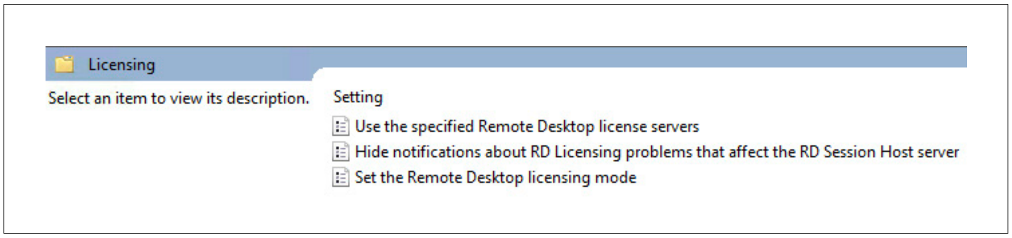
It is recommended to advertise KMS by DNS (`_vlmcs._tcp` SRV records) and to clear and disable the KMS cache when creating the client image. This action ensures that KMS requests are load-balanced by DNS, even when a KMS host is down during initial deployment.

Remote Desktop Licensing

Use GPO policy or Windows registry to specify all RDSH license servers and the licensing mode.

For the GPO policy (`vmware_rdsh_server.admx`), go to:

Computer Configuration > **Policies** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**



Setting
Use the specified Remote Desktop license servers
Hide notifications about RD Licensing problems that affect the RD Session Host server
Set the Remote Desktop licensing mode

If you are using Windows registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
```

- `LicenseServers` (`REG_MULTI_SZ`)
- `LicensingMode` (`2` = per device, `4` = per user)

It is recommended that you delete the key containing `timebomb` in the following hive of the registry of the RDSH image so that the grace period starts after deployment and not on creation of the image:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\RCM\GracePeriod
```

ESXi Host Sizing Best Practices

To determine the number of ESXi hosts you need, as well as the number of CPUs and the amount of memory on each host, consider how many end users you must serve, how many and what type of applications they use, and how intensive their workloads are.

The steps to follow are

1. Establish a baseline of user requirements.
2. Calculate CPU requirements based on users' workloads.
3. Calculate memory requirements based on users' workloads.
4. Perform a load test.
5. Use a pilot to validate ESXi host requirements.
6. Calculate the number of ESXi hosts required.

Establish a Baseline of User Requirements

Gather the baseline information on the user groups that have been identified as good candidates for an RDSH environment. The purpose of this step is to understand the performance characteristics of the target users' workload. For example:

- Which applications do users need?
- Are the applications CPU- or memory-intensive?
- Does their work generate a large number of storage operations?
- What type of network load is being generated by user activities?

Note: This information is applicable whether you are implementing a new RDSH environment or migrating an existing RDSH or virtual desktop infrastructure (VDI) environment to a Horizon 7 published applications environment.

A performance-monitoring tool, such as VMware vRealize® Operations Manager™, Liquidware Labs Stratusphere FIT, or Lakeside Software SysTrack, can help you gather the baseline information. In addition, Windows includes Performance Monitor (Perfmon), which allows you to capture and graph performance statistics from local and remote computers. See the VMware knowledge base article Collecting the Windows Perfmon log data to diagnose virtual machine performance issues (2010970).

Calculate CPU Requirements Based on Users' Workloads

There are two recommended virtual CPU configurations when deploying Horizon 7 RDSH.

- Four virtual CPUs with a 1:1 virtual-to-physical CPU ratio
- Eight virtual CPUs with a 2:1 virtual-to-physical CPU ratio

Make sure that the ratios do not span CPUs because every RDSH needs to follow NUMA.

Which configuration works best depends on the thread use of the application workload. Always test your configuration with a pilot.

For example, if the hosts used for an RDSH cluster have two Intel Xeon Processor E5-2699 v4 (22 cores), the hosts should run a maximum of:

2 (physical CPUs) * 1 (1:1 ratio) * 20 (physical cores) / 4 (virtual CPUs) = 10 RDSH VMs

This amount is equal for both ratios. The extra cores and hyper-threaded cores are not lost. They are used for virtual networking, storage, and other host tasks.

From the baseline that you previously established, you can estimate the CPU resources required per type of user. With this example, we can determine the number of hosts required for a company:

- Based on Perfmon, the average CPU usage of one type of user found is 260 MHz.
- The Intel Xeon Processor E5-2699 v4 has an all-core turbo. If Turbo Boost is disabled or high temperatures are expected, use the base frequency, which is 2200 MHz.
- With a speed of 2800 MHz and with four physical cores available per RDSH, this processor allows for 11200 MHz to be shared among users.
- When leaving a 40 percent margin for CPU spikes, such as during boot storms, you can have 30 users per RDSH, or 300 per ESXi host.

11200 / (260*1.4) = 30.77

Calculate Memory Requirements Based on Users' Workloads

The amount of memory required for an ESXi host depends on the private memory references for an application workload combined with

- Memory for the host operating system
- Shared application memory
- Memory required for a user session

Start with 4 GB of memory for the operating system, plus 975 MB (750 MB + 30 percent margin) per user, unless the performance monitoring shows high memory usage. In our example, the amount is 32 GB:

4 + (30 users * 0.95) = 32.5 GB

Perform a Load Test

After calculating the CPU and memory requirements, perform a load test with a tool like VMware View Planner before doing a day-to-day operations pilot.

Use a Pilot to Validate ESXi Host Requirements

Now that we have calculated our starting point—10 RDS hosts with 30 users per ESXi host—you want to pilot these numbers on a few ESXi hosts. Have users perform their normal day-to-day operations while monitoring the environment extensively. Adjust the configurations based on the outcome.

Besides validating your calculations, you can determine whether to use a 1:1 or 2:1 virtual-to-physical CPU ratio, based on performance.

Calculate the Number of ESXi Hosts Required

After the numbers are adjusted based on the pilot, calculate the number of hosts required: total number of users divided by the number of users per server, plus the number of servers required for redundancy or other minimums.

For example, if you have 900 users who need to continue working when an ESXi host is down, you need four hosts:

(900 / 300) + 1

If you want to use vSAN 6.5 RAID-6 Erasure Code, you need six hosts, because the supported configuration is 4 + 2. You can also choose smaller CPUs.

With four hosts and 2 GB required for ESXi, you need 384 GB of host memory, which is the closest supported configuration to the required amount of 322 GB to allow enough headroom for vSAN:

2 + (10 * 32) = 322 GB

With six hosts, the closest supported configuration to the required amount of host memory is 256 GB to allow enough headroom for vSAN:

2 + (6 * 32) = 194 GB

Remote Desktop Session Host Configuration Best Practices

After you set up the vSphere infrastructure, you can create an optimized master VM for cloning RDS hosts.

The steps:

1. Create the master RDS host VM.
2. Install common Microsoft runtimes and features.
3. Install Microsoft updates.
4. Tune Windows with the OS Optimization Tool.
5. Trim the image.

Create the Master RDS Host Virtual Machine

To create a master VM image for your RDS hosts, use a version of the VMware vSphere Web Client that is compatible with the ESXi host. Use the following specifications.

- **CPU** – Four or eight sockets (use the number determined from the pilot) with one core per socket.
- **Memory** – We recommend reserving the full amount of memory required (use the amount determined from the pilot) to avoid accidental over-commitment and consumption of disk space with unused swap files.
- **Virtual SCSI controller** – The recommended virtual disk controller for RDSH VMs is LSI Logic SAS.

  For more information about storage controllers, see *SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility* in the vSphere Virtual Machine Administration Guide.

  Note: After you create the image, if you need to adjust the controller, you must boot once with a secondary controller and temporary disk before changing the boot device.
- **Virtual disk format** – Use thin-provisioned virtual disks, unless the VM resides on spinning disk drives. For more information, see *Virtual Disk Thin Provisioning* in the vSphere Storage Guide.
- **Virtual network adapter** – Select **VMXNET3**.
- **OS installation method** – Use a Microsoft-provided ISO file. Supported OS versions include Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016.
- **VMware Tools™** – In the VMware Tools installation wizard, select **Typical** mode.
- **DVD and floppy drives** – After installing the OS and VMware Tools, remove the virtual DVD drive and floppy drive. Also disable the floppy drive controller in the virtual BIOS.
- **COM and LPT** – In the virtual BIOS, disable the LPT and COM ports.

Install Common Microsoft Runtimes and Features

Before updating Windows in the VM, install all required versions of Microsoft runtimes that are patched by Windows Update and that can run side by side in the image. For example:

- NET Frameworks (3.5, 4.5, and so on)
- Visual C Redistributables x86/x64 (2005 SP1, 2008, 2012, and so on)

These items cannot be part of an App Volumes AppStack or VMware ThinApp®. But make sure to install these runtimes on all provisioning VMs.

Install the Desktop Experience feature if scanner redirection or a richer user experience is required. For more information, see *Install Desktop Experience on Windows Server* in Setting Up Published Desktops and Applications in Horizon 7.

Install Microsoft Updates

Install all available updates to Microsoft Windows and other Microsoft products with Windows Update or Windows Server Update Service. You might have to first manually install Windows Update Client for Windows 8.1 and Windows Server 2012 R2: March 2016.

Tune Windows with the OS Optimization Tool

Run the VMware OS Optimization Tool with the default options, but consider disabling the optimization that allows TCP/IP offload in the HKLM settings. Current network cards can do offloading, so by not enabling this optimization, you can achieve better network performance.

Trim the Image

Use the following methods to reclaim empty space and delete unnecessary files:

- **Disk cleanup** – You can use the Windows built-in Disk Cleanup utility to delete unnecessary files.
- **Zero empty space** – Zero out empty space so that it can be reclaimed. You can use the Windows Sysinternals SDelete command, as described in the VMware knowledge base article Storage vMotion to thin disk does not reclaim null blocks (2004155). For example:

  ```
  sdelete64.exe –z c:
  ```

  To monitor the progress, check the volume's free space. The tool inflates the disk to its full size and then releases the free space.
- **Disk space reclamation** – On a VMFS5 volume, you can use `vmkfstools` on the ESXi shell to reclaim the empty space. For example:

  ```
  vmkfstools -K /path/to/disk-name.vmdk
  ```

  On non-VMFS5 volumes you can clone to a thin disk.

Horizon 7 Best Practices

We recommend using Instant Clone Technology when creating RDSH server farms. We also recommend using advanced load balancing if the default method, which bases load-balancing decisions on the current session count, is not adequate for your needs.

Provisioning RDS Hosts Using Instant Clones

Instant clones deploy RDS hosts more rapidly, scale more easily, and perform maintenance up to 85 percent more quickly than was previously possible.

Publishing occurs only when you create a new farm or update an existing farm to incorporate changes. Publishing the master image takes between 7 and 40 minutes, depending on the type of storage and number of hosts that you are using.

After the publishing process is complete, provisioning the servers takes 1 or 2 seconds per server. Provisioning does not require power operations, and the clones are forked from a running parent VM to further expedite the process.

You can delay the provisioning process by not enabling it in the Add Farm wizard. When you scale up the pool, all that needs to be done is provisioning.

RDSH Load Balancing

By default, the Connection Server uses the current session count and limit to balance the placement of new application sessions on RDS hosts. You can override this behavior and control the placement of new application sessions with a load-balancing script. Load balancing on multiple metrics like CPU, memory, disk, and network is recommended. You can write your own load-balancing script or use one of the samples provided with Horizon Agent.

A load-balancing script returns a load value. The load value can be based on any host metric, such as CPU utilization or memory utilization. Horizon Agent maps the load value to a load preference and reports the load preference to the Connection Server. The Connection Server uses the load preference to determine where to place new application sessions.

Important: Include margins for peak loads in the script, just as we did in the CPU and memory calculations. Use the script in conjunction with a reasonable maximum number of connections per host, which is set on the host or farm. Session load balancing addresses load balancing only at connection time and cannot move users after they have been assigned.

You must enable the VMware Horizon View Script Host service on an RDS host before you configure a load-balancing script. The service is disabled by default. Set it to automatic using `services.msc`.

You must configure the same load-balancing script on every RDS host in the farm. Configuring a load-balancing script involves setting a registry key on the RDS host.

```
HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents\RdshLoad
```

```
cscript.exe "C:\Program Files\VMware\VMware View Agent\scripts\cpuutilisation.vbs"
```

If you are using an automated farm, you perform this procedure on the master VM for the automated farm.

For more information, see *Configuring Load Balancing for RDS Hosts* in View Administration.

User Environment Manager Policy Configuration Best Practices

After you have created farms of RDS hosts, you can use VMware User Environment Manager for fine-grained policy management.

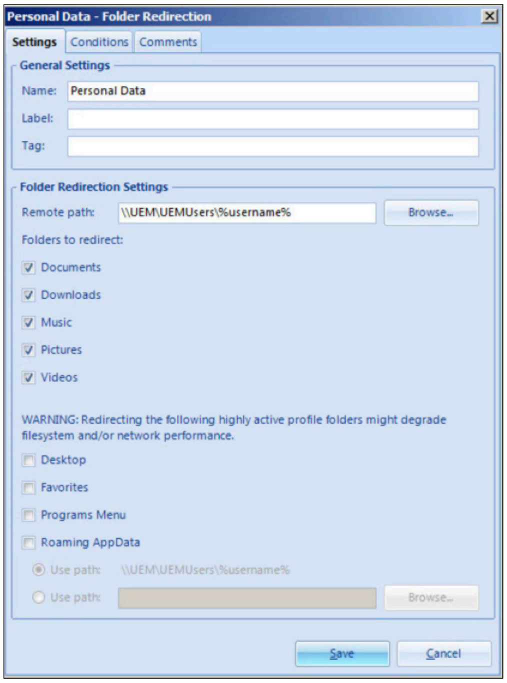
Horizon Smart Policies

By default, Horizon 7 allows pasting from a client system to an RDS host, but not the reverse. If users need to be able to copy text from the session, you can use a Smart Policy, as described in *Configure Horizon Smart Policies* in the VMware User Environment Manager Administration Guide.

Horizon Smart Policies are available for configuring USB redirection, client-drive redirection, bandwidth profiles, and more.

Folder Redirection

To allow user data to persist between sessions, use folder redirection for the Documents folder, at a minimum. We recommend using User Environment Manager to configure folder redirection.



General Settings

Name: Personal Data

Label:

Tag:

Folder Redirection Settings

Remote path: \\UEM\UEMUsers\%username%

Folders to redirect:

☑ Documents
☑ Downloads
☑ Music
☑ Pictures
☑ Videos

WARNING: Redirecting the following highly active profile folders might degrade filesystem and/or network performance.

☐ Desktop
☐ Favorites
☐ Programs Menu
☐ Roaming AppData

● Use path: \\UEM\UEMUsers\%username%
○ Use path:

Figure 2: User Environment Manager Folder Redirection Configuration Dialog Box

For more information, see *Configure Folder Redirection* in the VMware User Environment Manager Administration Guide.

User Profiles

Because users can get a different RDS host each time they log in, we do not recommend keeping profile information on the RDS host. Doing so consumes an excessive amount of disk space. Instead, use folder redirection, and use mandatory user profiles, as described in the VMware blog post VMware User Environment Manager, Part 1: Easier, Faster Windows Logins with Mandatory Profiles.

A mandatory user profile is a special type of preconfigured roaming profile that you can use to specify settings for users. A user can modify a desktop, but the changes are not saved when the user logs out. The next time the user logs in, the mandatory user profile created by the administrator is downloaded.

If you choose not to use mandatory user profiles, remove the cached user profile at logout. See Delete cached copies of roaming profiles.

Printer Configuration

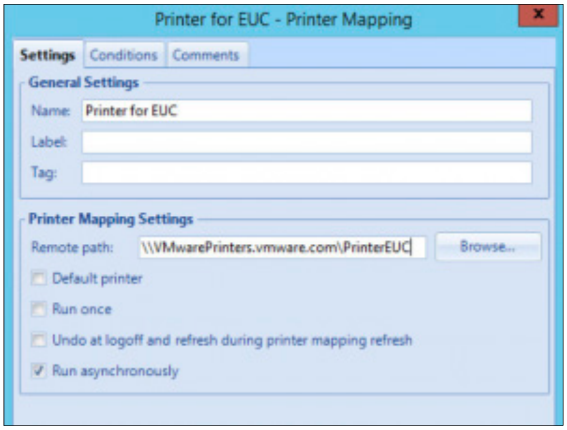
When using locally attached personal printers or specialized printers, such as bar code printers and label printers, users can use local printer redirection (also called the virtual printing feature), which is included with Horizon 7. This feature does not require installing printer drivers in the RDS host because the printer driver is installed on client endpoints.

Keep the following in mind when using local printer redirection with VMware Horizon 7.

- Printer redirection supports many common printer features, such as two-sided printing, but it might not support some unique features of a specific printer.
- Client systems that do not have local printer drivers, such as PCoIP zero clients and mobile clients, are not supported.

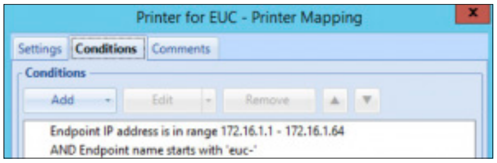
However, local printer redirection is not the right solution for corporate network printers. Network printing is redirected over virtual channels, which can impact overall performance. When using network print servers, we recommend using User Environment Manager to set up printer mappings and to deliver a follow-me printing solution. Printers can be mapped during the user login process. The printer is ready immediately after the login process completes.

For example, you map a particular printer, such as a barcode printer, when a user launches a specific application. The mapping is deleted when the user closes the application. This setup streamlines the login process because the printer is mapped only when the user needs it.



Name: Printer for EUC
Label:
Tag:
Remote path: \\VMwarePrinters.vmware.com\PrinterEUC
□ Default printer
□ Run once
□ Undo at logoff and refresh during printer mapping refresh
☑ Run asynchronously

Figure 3: Printer Mapping Settings Tab Showing the Path to the Printer



Endpoint IP address is in range 172.16.1.1 - 172.16.1.64
AND Endpoint name starts with 'euc-'

Figure 4: Printer Mapping Conditions Based on IP Range and Endpoint Name

For more information, see the VMware blog post Choosing Printing Options for VMware Horizon 7.

Turning Off Hardware Graphics Acceleration in Commonly Used Applications

If the RDSH VMs are not using a physical GPU in the ESXi hosts, you can reduce CPU usage by not emulating hardware graphics in applications. We recommend using User Environment Manager configuration files to control these application settings.

For more information, see the VMware User Environment Manager Application Profiler Administration Guide.

Internet Explorer

To turn off hardware graphics acceleration for Internet Explorer, navigate to **Internet Options** > **Advanced** > **Accelerated graphics** and select **Use software rendering instead of GPU rendering**.

Microsoft Office

To turn off hardware graphics acceleration for Microsoft Office, navigate to **File** > **Options** > **Advanced** and select **Disable hardware graphics acceleration**.

Adobe Reader

To turn off hardware graphics acceleration and disable other CPU-intensive display options for Adobe Reader:

1. Navigate to **Preferences** > **Page Display** > **Rendering** and deselect the following options:
   - **Smooth imaging**
   - **Smooth line art**
   - **Use page cache**
   - **Enhance thin lines**
2. Navigate to **Preferences** > **Page Display** > **Page Content and Information** and select **Disable smooth zooming**.

   For more information, see the Adobe documentation about General Application Settings in the Windows Registry.

Google Chrome

To turn off hardware graphics acceleration for Chrome, navigate to **chrome://settings** > **System** and deselect **Use hardware acceleration when available**.

App Volumes Best Practices

App Volumes stores applications in shared read-only virtual disks (VMDK files) called AppStacks. AppStacks are assigned to RDS hosts rather than to users, as is done with VDI. Because RDS hosts can be deleted and recreated regularly, assign the AppStack to the AD group object that contains the computer objects for the RDS hosts. That way, the AppStack assignment does not depend on specific computer names.

Create dedicated AppStacks for RDS hosts. Do not reuse an AppStack that was originally created for a desktop OS.

Install the applications on the same operating system that is on the deployment RDS host.

Before installing applications on an AppStack, switch the RDSH server to the RD-Install mode. For more information, see Publishing Applications with VMware Horizon 7.

Important: If you are assigning App Volumes AppStacks to OUs, contact Global Support Services for the App Volumes 2.12.3 hot patch. This fix will also be included in general releases of App Volumes later than 2.12.

Antivirus Configuration Best Practices

To increase performance, you can adjust the all-inclusive antivirus scanning. The following recommendations apply to both desktops and applications provided by RDSH.

- Always run a virus scan on master images before putting them into production.
- Stagger scheduled scans on RDS hosts to not scan all hosts at the same time, which would overload the vSphere environment.
- Disable scanning on read operations for RDS hosts that are rebuilt frequently, such as for recurring maintenance.

  Important: This recommendation assumes that the master image has already been scanned and is known to be virus free. Do not disable real-time scanning, and make sure that scanning for write operations is enabled.
- Remove unnecessary antivirus actions or processes from the desktop's startup or login routines.

  Important: Seek guidance from your security team or antivirus vendor if you are unsure what is unnecessary.
- Disable heuristic scanning on RDS hosts that are rebuilt frequently.
- Disable auto-updates of antivirus software on RDS hosts that are rebuilt frequently.

  Important: This recommendation applies to all installed software, not just antivirus software, because updates made when using a nonpersistent VM are lost on refresh. Ensure that you keep master images regularly updated with new antivirus software versions and signature files.
- Exclude low-risk files and folders from real-time scans on RDS hosts. Some locations include:
  - Page files
  - Windows event logs
  - `C:\Program Files\VMware`
  - `%systemroot%\SoftwareDistribution\DataStore`
  - `%allusersprofile%\NTUser.pol`
  - `*.pst`, `*.pstx`, and `*.ost` files
  - `%systemroot%\System32\Spool\Printers`
  - `%ProgramData%\VMware\VDM\Logs`
  - App Volumes: `C:\SnapVolumesTemp`
  - App Volumes: `C:\SVROOT`

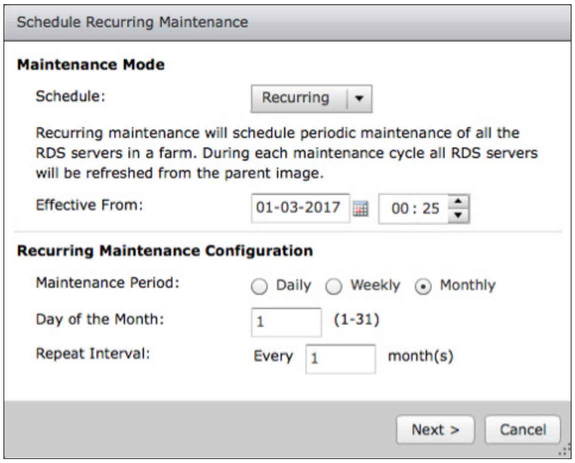
  Important: Continue to scan low-risk files and folders excluded from real-time scans on a regular schedule.

For more information, see Antivirus Considerations in a VMware Horizon 7 Environment.

Maintenance Operations Best Practices

A recurring maintenance schedule ensures that the RDS hosts are periodically regenerated. Potential contamination is removed so that the farm runs optimally. Because the maintenance operation does only provisioning, the operation needs little time to complete, which is one of the many reasons why using instant clones is highly recommended.

We recommend scheduling weekly or daily maintenance outside of business hours to minimize the impact on users. If you have multiple shifts per day of users, weekly maintenance is recommended. Otherwise, daily maintenance is recommended.



Schedule Recurring Maintenance

Maintenance Mode

Schedule: Recurring

Recurring maintenance will schedule periodic maintenance of all the RDS servers in a farm. During each maintenance cycle all RDS servers will be refreshed from the parent image.

Effective From: 01-03-2017 00 : 25

Recurring Maintenance Configuration

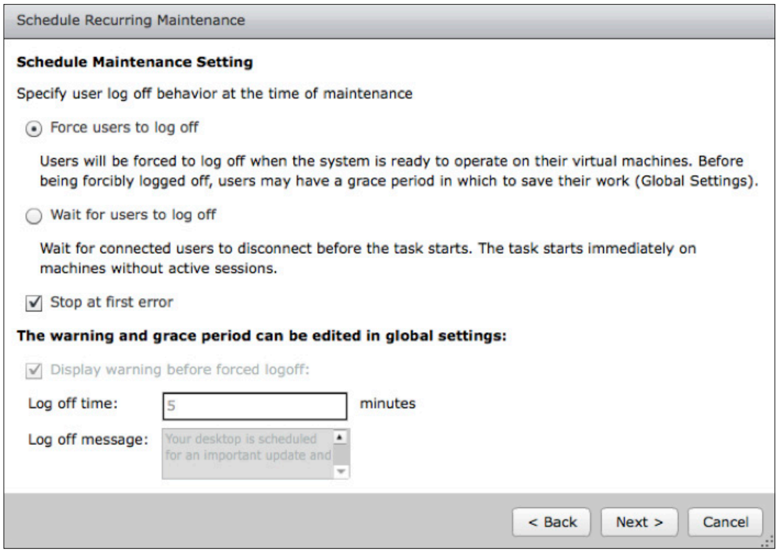
Maintenance Period: ○ Daily ○ Weekly ● Monthly

Day of the Month: 1 (1-31)

Repeat Interval: Every 1 month(s)

Figure 5: Recurring Maintenance Schedule

You can choose whether to log out users or wait for them to log out before performing maintenance.



Schedule Recurring Maintenance

Schedule Maintenance Setting

Specify user log off behavior at the time of maintenance

● Force users to log off

Users will be forced to log off when the system is ready to operate on their virtual machines. Before being forcibly logged off, users may have a grace period in which to save their work (Global Settings).

○ Wait for users to log off

Wait for connected users to disconnect before the task starts. The task starts immediately on machines without active sessions.

☑ Stop at first error

The warning and grace period can be edited in global settings:

☑ Display warning before forced logoff:

Log off time: 5 minutes

Log off message: Your desktop is scheduled for an important update and

Figure 6: Configuring Logout Behavior for Maintenance Operations

Conclusion

Setting up a Horizon 7 RDSH environment is similar to deploying a VDI desktop environment. The main differences involve calculating VM density on vSphere hosts and installing software and features on the RDS host VMs. Adhering to the best practices described in this guide ensures that you get the best performance for your RDSH applications and desktops.

Additional Resources

Choosing Printing Options for VMware Horizon 7 (VMware blog post)

Collecting the Windows Perfmon log data to diagnose virtual machine performance issues
(VMware knowledge base article)

VMware App Volumes User Guide

Horizon 7 Documentation

Just-in-Time Apps with VMware Horizon 7 (VMware blog post)

Publishing Applications with VMware Horizon 7

Storage vMotion to thin disk does not reclaim null blocks (VMware knowledge base article)

Virtualizing Performance Critical Database Applications in VMware vSphere 6.0

VMware Horizon 7 Enterprise Edition Multi-Site Reference Architecture

VMware Horizon 7 Enterprise Edition Reference Architecture

VMware OS Optimization Tool

VMware User Environment Manager Administration Guide

VMware User Environment Manager, Part 1: Easier, Faster Windows Logins with Mandatory Profiles
(VMware blog post)

vSphere 6 Documentation

About the Author

Hilko Lantinga is an End-User-Computing Architect in VMware Technical Marketing with a focus on application and desktop virtualization. Previously, he was a senior consultant in VMware Professional Services, leading large-scale EUC deployments in EMEA, and he has 18 years of experience in end-user computing.

To comment on this paper, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com