TECHNICAL WHITE PAPER – **FEBRUARY 2017**

ANTIVIRUS CONSIDERATIONS IN A VMWARE HORIZON 7 ENVIRONMENT

VMware Horizon 7

This document is for informational purposes only and is intended solely to assist you in considering your security needs. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon as the primary source for making security decisions.

vmware®

Table of Contents

Introduction

Using antivirus software in any computing environment is a very important security consideration. Unless your operating system is protected from malware, you leave it open to negative and potentially destructive software infection. However, one of the consequences of running antivirus software is that operating system performance can suffer. There is a balance between an acceptable level of security and an acceptable level of performance, and this varies from one environment to the next.

This article discusses the use of antivirus software in a VMware Horizon® 7 environment, and changes that can be made to improve performance without unduly compromising system security.

If you are looking for information about a specific third-party antivirus vendor solution, see Additional Resources.

Caution: Before restricting your antivirus software settings in any way, seek guidance from your security team and your antivirus vendor to ensure that the restrictions are appropriate for you.

What Is Horizon 7?

One component of VMware Horizon 7 is View, the VMware virtual desktop infrastructure (VDI) software that delivers a Windows desktop experience remotely to a user's thin client, zero client, PC, or mobile device, from centralized enterprise servers. Within View, you can set up shared desktops or applications running on Remote Desktop Session Hosts (RDSH). VMware Horizon 7 editions can also include VMware App Volumes™, VMware User Environment Manager™, VMware ThinApp®, and other components such as the VMware Access Point™ virtual appliance.

Areas of Consideration

When looking to adjustments to all-inclusive antivirus scanning in order to increase performance, there are several areas to consider. These apply to both single-user virtual desktops and session-based desktops and applications provided by RDSH.

Virtual Machines

There are several general considerations to take into account with virtual machines.

- Set real-time scanning to scan local drives only.

  Important: So long as you are using antivirus solutions to monitor all other remote locations that host file shares, user profiles, redirected folders, and remote peripherals, there is no need for end-user desktops to also scan these locations.

- Always run a virus scan on master images before putting them into production.
- Use nonpersistent desktops. This mitigates risk by ensuring each user session is refreshed to a known clean state on logout.
- Disable scan on read for nonpersistent desktop pools.

  Important: This assumes that the master image has already been scanned and is known to be virus free. It also does not mean to disable real-time scanning. Scan on write should still be enabled.

- Remove any 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 nonpersistent virtual machines, according to the article Phase 5 - Antivirus Impact and Best Practices on VDI v1.0.
- Make frequent software updates to your master images as needed. This ensures that if an end user needs their desktop refreshed or recomposed in order to clean a virus, they will lose as little software as possible.
- Disable auto-updates of antivirus software for nonpersistent desktop pools.

  Important: This actually applies to any installed software, not just antivirus software, as updates made during use of a nonpersistent desktop will be lost on logout and refresh anyway. Ensure that you keep master images regularly updated with new antivirus software versions and signature files.

- Scan VMware View® Composer™ persistent disks—formerly called user data disks (UDD)—for viruses on a regular basis. Because this type of disk is persistent, a refresh or recompose operation will not remove any viruses.

- Exclude low-risk files and folders from real-time scans on single-user View virtual machines or RDSH machines. Some locations include:
  - Page files
  - IIS log files
  - Windows event logs
  - `C:\SnapVolumesTemp`
  - `C:\SVROOT`
  - `C:\Program Files\VMware\`
  - `%systemroot%\SoftwareDistribution\DataStore`
  - `%allusersprofile%\NTUser.pol`
  - `*.pst, *.pstx,` and `*.ost` files
  - `%systemroot%\System32\Spool\Printers`
  - `%ProgramData%\VMware\VDM\Logs`

  Important: Any low-risk files and folders excluded from real-time scans should still be scanned on a regular schedule.

Services

Review the Microsoft support article, Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows, for general guidance on service exclusions.

Caution: Exclusions can present a security risk. Seek guidance from your security team and your antivirus vendor to ensure that any restrictions are appropriate for you.

Horizon 7 Management Servers

There are several Horizon 7 management servers that play a role in a VDI environment.

- View Connection Servers broker the connections from users to their allocated resources.
- Enrollment servers are deployed to support the implementation of True SSO.
- View Composer delivers advanced virtual image management to conserve disk space and streamline virtual desktop provisioning and deployment.
- Access Point is a hardened Linux virtual appliance that resides in the DMZ. Access Point ensures that the only remote desktop and application traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user.

  Caution: The design of Access Point ensures no weaknesses that a virus can exploit. The installation of antivirus software to Access Point will stop it from functioning.

Consider excluding the following server folders from real-time scanning:

- View Connection Servers:
  - `%programData%\VMware\VDM\Logs`
  - `%AllUsersProfiles%\Application Data\VMware\VDM\Backups`
  - `C:\Documents and Settings\All Users\Application Data\VMware\VDM\backups`
- For enrollment servers, `%programData%\VMware\VDM\Logs`
- For View Composer, `%ProgramData%\Vmware\View Composer\Logs`

  Important: These server folders should still be scanned on a regular schedule.

App Volumes

VMware App Volumes makes it easy to deliver, update, manage, and monitor applications, and users of those applications, across virtual desktop and published application environments.

When working with App Volumes, consider the following when planning antivirus scanning:

- The App Volumes provisioning machine is used to create AppStacks.
  - The provisioning machine should use a snapshot that is known to be virus free but also has no antivirus software installed. The presence of antivirus software can interfere with the proper creation of an AppStack. You can make sure it is virus free by installing the required operating system and base software without it being on the network, and taking the snapshot. Alternatively, you can install antivirus software to it, scan it, uninstall the antivirus software, and take the snapshot.

    If possible, disconnect the provisioning machine from the network when creating an AppStack.
- Consider excluding certain files and folders from real-time scanning on the App Volumes Manager.

  Important: These files and folders should still be scanned on a regular schedule:

  - `C:\Program Files (x86)\CloudVolumes`
  - `C:\Program Files\VMware\`
  - `pagefile.sys`
  - `LDF files`
  - `MDF files`
  - `NDF files`
- The App Volumes client is a machine that can have AppStacks attached; that is, View single-user and session-based RDSH virtual desktops, Citrix XenApp servers, Citrix XenDesktops, and physical Windows desktops.
  - On the App Volumes client, exclude `C:\Program Files (x86)\CloudVolumes\Agent\svservice.exe` from real-time scans.

User Environment Manager Scan Exclusions

VMware User Environment Manager delivers personalization and centrally managed policy configurations across virtual, physical, and cloud-based Windows desktop environments. User Environment Manager allows IT to control which settings users are allowed to personalize, and also maps environmental settings such as networks and location-specific printers.

On servers, exclude the FlexEngine log path from real-time scans. For example:
`\\server\FlexArchiveShare\%username%\Logs`

On clients, as with other network paths, exclude the following paths from real-time scans:

- VMware User Environment Manager configuration share path
  For example: `\\server\FlexConfigShare\general`
- Profile archive path
  For example: `\\server\FlexArchiveShare\%username%\Archives`
- Profile archive backup path
  For example: `\\server\FlexArchiveShare\%username%\Backups`

Additionally, in nonpersistent desktop pools that have a clean master image, you can exclude these User Environment Manager executables from real-time scans because they are known to be virus free:

- `FlexEngine.exe`
- `FlexSyncTool.exe`
- `Flex+ Helpdesk Support Tool.exe`
- `Flex+ Self-Support.exe`

ThinApp

VMware ThinApp is a virtualization technology that isolates and encapsulates pre-installed applications. Virtualized applications are isolated from all other applications as well as from the underlying operating system. These packages can run on virtual or physical desktops, stream from a file share, or be placed on VMware App Volumes AppStacks.

When working with ThinApp, consider the following when planning antivirus scanning:

- Your ThinApp capture machine should use a snapshot that is known to be virus free but also has no antivirus software installed. The presence of antivirus software can interfere with the proper creation of a ThinApp package. You can make sure it is virus free by installing the required operating system and base software without it being on the network, and taking the snapshot. Alternatively, you can install antivirus software to it, scan it, uninstall the antivirus software, and take the snapshot.

  If possible, do not have the capture machine connected to the network when capturing applications.
- When using a network share to store ThinApp packages, exclude all of the files known to be virus free from real-time scans. Do not exclude the directory itself, as it is possible that an unknown file can be accidentally written to the share by an administrator.
- Antivirus software has on occasion generated false-positives because of the signature used by ThinApp packages to store data. If the file actually is a ThinApp package, this is not an indication that the ThinApp package contains a virus.

About the Author and Contributors

Author

Alex Birch, End-User-Computing Architect, EUC Technical Marketing, VMware, wrote this paper. In his role as an EUC Architect in the VMware End-User-Computing Business Unit, Alex creates deep-dive content and produces technical content for specialist staff and partners. Alex has more than 20 years of IT experience, which includes working within the EUC space for more than 15 years and specializing in virtual desktop design and implementation since 2007.

Contributors

The following individuals contributed content and review to this paper:

- Graeme Gordon, Senior End-User-Computing Architect, EUC Technical Marketing, VMware
- Stephane Asselin, Senior End-User-Computing Architect, EUC Technical Marketing, VMware
- Hilko Lantinga, End-User-Computing Architect, EUC Technical Marketing, VMware
- Prasanna Sankar, Technical Support Director, VMware

This document contains some material from a prior version of this paper. Authors of the previous version are

- Tina de Benedictis, End-User-Computing Senior Manager, Public Content, EUC Technical Marketing, VMware
- Cynthia Hsieh, VMware alumna
- Jeff Birnbaum, VMware alumnus

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

Additional Resources

This section lists third-party antivirus software vendors and Microsoft guides, and provides other links.

Antivirus Software Vendors

There are several antivirus software vendor articles that might be useful.

Note: VMware does not endorse or recommend any particular third-party antivirus software vendor, nor is this list meant to be exhaustive.

- Trend Micro
  - Best Practice for Setting Up Virtual Desktop Infrastructure (VDI) in OfficeScan
  - OfficeScan VDI Pre-Scan Template Generation Tool
  - Frequently Asked Questions (FAQs) about Virtual Desktop Infrastructure/Support In OfficeScan
- McAfee – McAfee MOVE AntiVirus: Optimized Security for Virtualized Environments
- Sophos
  - Best Practice for Running Sophos on Virtual Systems
  - Sophos Anti-Virus for Windows 2000+: Incorporating Current Versions in a Disk Image, Including for Use With Cloned Virtual Machines
- Symantec
  - Virtualization Best Practices for Endpoint Protection 12.1.1 (RU1) and Earlier
  - Symantec Endpoint Protection 12.1 - Non-persistent Virtualization Best Practices
  - How to Prepare a Symantec Endpoint Protection 12.1.x Client for Cloning

Microsoft Guides

Microsoft provides the following guide on antivirus protection.

Virus Scanning Recommendations for Enterprise Computers That Are Running Currently Supported Versions of Windows

Other Links

This paper referenced some third-party articles.

- Phase 5: Antivirus Impact and Best Practices on VDI v1.0
- Kaspersky: Virus Scan Exclusions for Microsoft Products

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

2/17