



# Anti-Virus Practices for VMware® View™

TECHNICAL NOTES

**Table of Contents**

Introduction ..... 3  
System Resource Usage ..... 4  
Common Anti-Virus Practices ..... 4  
Conclusion..... 12  
About the Author ..... 12

## Introduction

Desktop virtualization is a transformative platform technology that can deliver cost-effective, manageable network and desktop access to workers with diverse computing needs.

However, with security threats becoming more sophisticated, more frequent, more targeted, and potentially more profitable to those who seek to inflict damage, virtualization is not exempted from increasing regulation and compliance requirements.

Anti-virus software is one of the largest segments in today's computer security market. Nearly every enterprise deploys anti-virus software on every desktop. In the virtual endpoint ecosystem, common computing practices have not vanished. Rather, solutions such as log analysis, host-based IPS, firewalls, and anti-virus need to evolve and adapt to desktop virtualization.

The typical top-down virus scanning model usually involves desktop pattern recognition and signature file updates, with access to an auto-update server. So during the virus or agent update, it is not uncommon to see system resource usage spike or become overly committed.

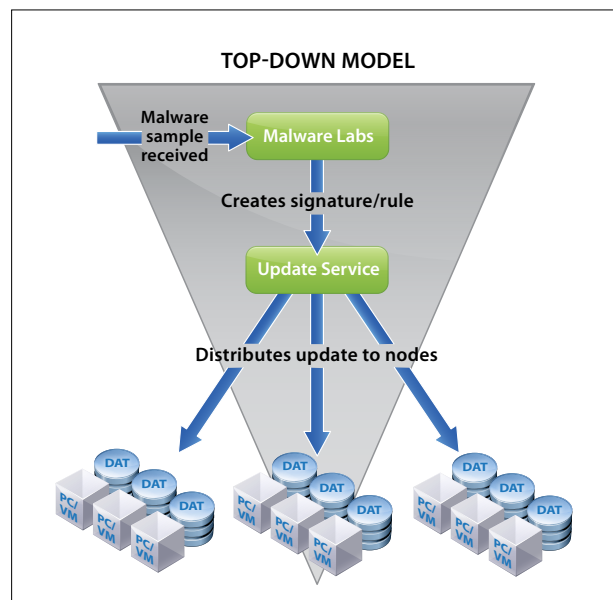


Figure 1: Top-down model

In desktop virtualization, hosting, managing applications, and provisioning services to end-users are performed in ways similar to traditional PC methods. As services such as security, mobility, access control, and line-of-business applications are all rolled up into the datacenter or cloud, anti-virus practices need to be rolled up as well.

Most organizations have acceptable use policies applicable to corporate internet, intranet, and network access usage. The corporation—including management, IT, and legal—needs to update its application installation and user data policy for virtual desktop configuration.

In VMware® View™, IT professionals can control application installation by setting up persistent or non-persistent desktops. In the event of a security outbreak or breach, with proper configuration with refresh on logoff or reboot, a non-persistent desktop can resume its original state after reboot. Although some may argue that some virus attacks can traverse through memory or network, it is the quick alternative to deploy stateless desktop and simply restart to get a clean OS environment. However, for persistent desktops, an anti-virus protection agent should be installed before the virtual machine is converted into a parent virtual machine for VMware View Composer-linked clone creation, although the feasibility of including the anti-virus agent in the parent virtual machine is determined by the choice of the anti-virus protection suite.

## System Resource Usage

Virtualization offers unprecedented visibility benefits for machine resources such as CPU, memory, network utilization, and storage partitioning. It empowers you to manage the utilization and virtual resource pooling because virtualization separates hardware resource allocation and management from application interfaces in a small and trustable code base. This also makes it easier for you to see the system bottleneck when virus scanners are running at the same time, causing an I/O storm and system usage spike on the host.

AV storms” can cause 100% saturation in shared compute (CPU) and SAN/NAS (storage I/O) environments. Traditional anti-virus agents are resource intensive and not optimized for high utilization, efficient clouds 100MB footprint can add up to 6 GB in deployments with high consolidation ratios such as VMware View.

## Common Anti-Virus Practices

You can consider the following practices when deploying anti-virus solutions for virtual systems.

**1. Install the core virus scanner, not the bells-and-whistles packages.**

Top anti-virus vendors have broadened their appeal to enterprises by cross-selling personal firewalls, combined security centers with anti-spyware, and host intrusion-prevention technologies. Such bundles may be appropriate for a freestanding PC but are less so for virtual machines in a contained datacenter. Installing only the core scanner helps to reduce the desktop agent memory and CPU footprint.

**2. Include Network Access Control (NAC) management agent in the parent virtual machine prior to cloning to make sure the anti-virus signature file is up to date.**

NAC creates a security posture checking system for clients with enforcement at the network level. Use the NAC agent to ensure the signature pattern file in the persistent desktop or pool is up-to-date by disallowing network access. All View Composer based linked clones are deployed from a snapshot of the parent virtual machine. For non-persistent linked-clone desktops, roll up the virus signature file with a virus-free snapshot in the VMware View Administration console. This ensures compliance with government regulations.

**3. Use virtual desktops to manage user access.**

The use of virtual desktops helps IT professionals to view and manage user access—for instance by forbidding certain application installations, controlling USB device access, or assigning non-persistent desktops to a particular profile group. VMware View entitlements are tightly integrated with Active Directory, so you can restrict access to persistent and non-persistent desktops based on user ID or Active Directory security group.

**4. Use random or staggered scan scheduling.**

There are two common types of anti-virus scans: On Demand Scanning (ODS) and On Access Scanning (OAS). In most organizations, customers enable OAS for inbound (write operations) and outbound (read operations) file access scenarios. In organizations that are very sensitive about security, customers may additionally prefer to perform frequent on-demand scans. With most anti-virus solutions, you can perform ODS on a scheduled basis and always have OAS enabled. Our recommendation is to consider the impact to the storage and hypervisor resources, and randomize the ODS scan times based on the hypervisor or storage LUN.

Randomizing or staggering the scan schedule can help to reduce the number of same-host virtual machines that are running their updates simultaneously. Most of anti-virus software has default set to

update immediately when there is a new signature file available. Check into the settings on random or stagger the update process can also help reduce the host resource loads. Physical PCs have their own individual resources to handle virus scanning. With virtualization visibility, you can gather I/O load data by comparing the increased ratio between a clean virtual machine and a virtual machine with anti-virus installed. Prevent virus scanning activities from saturating the I/O, and make sure that host CPU utilization is lower than 80 percent at your host capacity planning.

#### 5. Update your virtualization software and apply security patches.

As with any software, desktop virtualization software on guest or local systems can be exploited, so it is important to keep all your known virtualization software and applications updated with appropriate security patches. The common reasons to update software are to resolve functional bugs and leverage optimized/improved code, and to close vulnerabilities opened by security bugs.

#### 6. Virus scanning and VMware ThinApp™ packages.

Although virus scanners cannot scan within the ThinApp executables, you can protect ThinApp by updating the virus signature file and hardening the “packaging” computer. Some useful virus scanning practices for ThinApp are as follows:

- Scan against the project directory on a scheduled basis only (no on-demand scanning unless required by rules, regulations, or laws).
- Where on-demand scanning is necessary, reconfigure the ThinApp packages to utilize a separate Primary Data Container File (e.g., a DAT file) and small EXE entry point files to enhance the user experience.
- If at all possible, do not install anti-virus on the capture-and-build system. If anti-virus is required or necessary on the capture-and-build system, remember the following:
  - ThinApp works on the tried-and-true Delta Snapshot technology; therefore, anything the anti-virus program installs, that may also be used by the application being packaged, will likely not be captured due to the application’s installer already seeing it installed.
  - Almost all application manufacturers will recommend disabling or shutting down all anti-virus solutions (as well as Firewall and other “security” technologies) during the installation of their application to ensure it is properly installed without conflicts caused by the anti-virus software.

The thing to note here is that it is entirely environment-specific and we can only suggest some courses of action. If the application doesn’t need to be on the network in order to be captured, then disable the network connection to the virtual machine or use HOST only mode.

As for a ThinApp packaged application being “infected,” this can only happen if the “capture-and-build” system was already infected. A ThinApp packaged app cannot become infected once packaged, except for through the action of the application (e.g., a packaged browser used to browse to an infected web site). Once this occurs, the malware cannot escape from the virtual bubble (ThinApp packaged application) as the virtual bubble does not allow the application (including the malware) to adjust system settings—these modifications are virtualized within the bubble and dumped to the ThinApp sandbox.

Once the malware makes a modification, the modification is dumped to the sandbox, and once the modification hits the sandbox, it hits the hard drive—where any “on-demand” anti-virus solution will detect and remove the malware.

Conversely, if the host is infected and the packaged application isn’t, the host cannot infect the packaged application since the nature of application virtualization prohibits the host or anything in native memory from seeing into the virtual bubble. As for the sandbox, infection from the host to the application through the

sandbox is not possible, as ThinApp tracks all changes the packaged application makes to the sandbox and ignores outside changes made to the sandbox from the host.

For example, if you unknowingly package a Trojan horse virus inside of one of your ThinApp packages, the virus signature behaves as described in:

[http://www.symantec.com/business/security\\_response/attacksignatures/detail.jsp?asid=22990](http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=22990)

Once executed, the Trojan horse drops the following file: %System%\drivers\runtime.sys

It then creates the following registry subkey:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Runtime or overwriting system32 files

Self-contained ThinApp packages sandbox those changes. Once the system is rebooted, the Trojan horse will not run again because those changes never occurred. One possible exception is that if your sandbox application writes to network shares, you will expose writable network shares to the virus and allow it to traverse into an outbreak.

If the packaged application tries to copy files from inside the package to the system or makes a network connection and tries to download new content (usually EXE files), ThinApp will write these files to the sandbox. The sandbox is just a collection of files on the system, and your anti-virus software will definitely scan and quarantine anything detected as a malicious activity.

Run and scan the application prior to the packaging step to make sure there are no network file shares or unexpected file execution.

For up-to-date information on combating viruses on ThinApp, see:

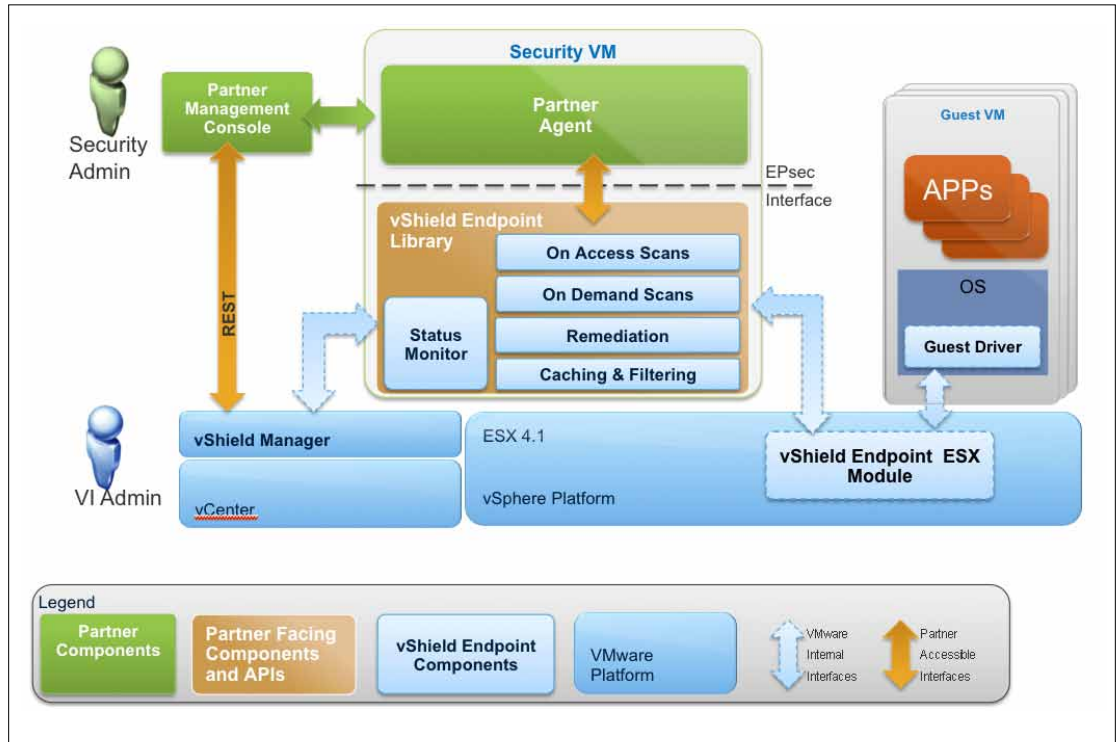
<http://blogs.vmware.com/thinapp/2008/10/anti-virus-ques.html>

## 7. Make sure there is a unique entry in Active Directory for each VMware View desktop.

Traditional virus scanners operate based on either a computer's security ID or MAC address to generate unique GUID. However, that's not entirely true; for example, McAfee does not directly require a unique SID for its agents. McAfee generates its own GUID for identification but the customer's DNS should be able to resolve the host properly; sometimes you will not be able to do that if you don't have a unique SID. Make sure each View desktop has a unique host name entry in DNS. This entry should be created by default during desktop provisioning by VMware View. With View Composer, VMware View 4.5 leverages the linked clone technology to create persistent or non-persistent desktop pools by using Sysprep or Quickprep to add VMs to specific Organizational Units (OUs). This enhancement helps create a new SID for each desktop provisioned.

**8. Consider Anti-Virus products integrated with vShield Endpoint.**

The concept of vShield endpoint is to leverage hypervisor to offload AV functions from agents into a dedicated security VM. It helps deploy security in a more agile, service-driven manner to both private and public cloud environments. Instead of deploying a scanning agent in individual virtual machines, VMware vShield provides a security framework and API's.



**Figure 2:** vShield Endpoint Components

Keeping a signature file in each individual virtual desktop has become inefficient and unsustainable. Since virtual desktops reside in a shared environment with multiple virtual machines per core and limited SAN bandwidth (as well as a shared network configuration), it is hard to apply physical anti-virus or other security solutions to a virtual desktop.

However, using vShield endpoint-compatible products allows you to retain the same consolidation ratio and provide security deduplication. VMware provides the vShield Endpoint Security API (EPsec) so that anti-malware security vendors can provide agent-less, real-time scanning and scheduled or manual scans.

For more information on VMware vShield products, please visit the product site at <http://www.vmware.com/products/vshield/overview.html>.

## 9. Resolve virus scanner deployment issues in linked clones.

Traditional AntiVirus server periodically communicates with all of the clients that it manages. It directly contacts the client and queries for the Globally Unique Identifier (GUID) value data stored in the client's registry. If you deploy the VMs using quickprep, all desktop VMs will share the same SID as the parent image. If you choose to use SysPrep, all cloned VMs will have unique SIDs.

During desktop refresh, if you would prefer to store the previous GUID, you can save the GUID by using Power Off script to save the GUID.

**A possible workaround** is to preserve GUID before shutting down the virtual machine: Use the Power Off script, for example saveGUID.bat, to a network share. The following function is provided in VMware View Administration Console where you can provide a custom script to interact with the VMware View Composer. For more information on how to configure View Composer in VMware View, please refer to the VMware View Administration Guide.

The screenshot shows the 'QuickPrep Settings' dialog box. On the left is a navigation pane with the following items: Type, Desktop Persistence, vCenter Server, Unique ID, DesktopPool Settings, Provisioning Settings, Parent VM, Default Image, Virtual Machine Folder, Host or Cluster, Resource Pool, Detectors, and QuickPrep Settings (which is selected and marked 'Ready to Complete').

The main area is titled 'QuickPrep Settings' and contains the following text:
   
QuickPrep is used to configure desktops after they have been created
   
⚠️ If the QuickPrep settings are changed, spare virtual machines using the previous settings will continue to be used until a sufficient number of new spares can be created. If this is not desired, the old spare virtual machines can be deleted from the Desktop Sources tab.
   
In order to join desktops to a domain, QuickPrep requires sufficient domain credentials for the target domain. Select the desired domain/account entry from the QuickPrep domain drop down menu. QuickPrep can also execute scripts on power-off and after creating new desktops or after a recomposition or refresh event. Enter paths (located on the Parent VM) to the scripts.

The configuration fields are:
   
QuickPrep domain: vmware-vdi.com (administrator) [dropdown menu]
   
Power-off script: c:\save\_guid.bat [text input]
   
Post synchronization script: c:\restore\_guid.bat [text input]
   
The AD container relative distinguished name (e.g., CN=Computers or OU=Marketing): CN=Computers [text input]

At the bottom right are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Figure 3. Quickprep settings

This suggestion depends entirely on how the third-party AV software handles the scan policy if SID, MAC, or DNS is used to generate the GUID. Some vendors do not directly require unique SID for their AV agents. They can generate their own GUID for identification if the DNS can resolve the host properly. Some require a MAC address for licensing tracking and scan validation.

**If the Master image is infected**, perform the virus scanning and cleaning on the master image, and then a recompose could be performed. This is the best option for scanning the master image, since it is not really in use and is essentially a template.

**If Master image is good, but the clone desktop is infected**, the best course of action is to refresh if it cannot be refreshed for whatever reason then the in-guest, anti-virus solution should be able to clean up the malware.

- If the anti-virus software relies on GUID, see the possible workaround below.
- If the anti-virus software relies on DNS entry, the VMware View desktop behavior is the same as the regular desktop. Every VMware View desktop has an entry in the DNS.
- If the anti-virus software relies on MAC, the use of a MAC address for traditional hosted anti-virus is to track desktop licensing. However, this measure is not so effective in virtual desktops.
- If the anti-virus software relies on SID, you might experience some issues. VMware View 4.5 deploys Sysprep to compose the virtual machine and it now creates the SID for each Replica.

#### **User Data Disk (UDD)**

- With user data disk, while composing the linked clone, you have the option to create a separate user data disk (UDD) to the same storage where the virtual machine resides or some other preferred storage. User data disk—specifically for the “My Documents” type data and not the operating system UDD in this case—will rely on the on-access scanning done using the anti-virus real-time agent which runs in the guest operating system.

**Note:** This depends completely on what your virus scanner uses to associate the desktop. VMware has not conducted testing with all virus scanners.

After virus clean up and recompose of the virtual machine, use the Post Synchronization script, for example, restoreGUID.bat, to restore the previous GUID back to the virtual machine.

The Ideal solution would be to have the anti-virus software vendor track the installation and scan policy by associating the virtual machine UUID and hostname for better identification.

#### **10. Configure corporate virus scanner configuration and scanning exclusion lists.**

Almost all enterprise-grade virus scanners allow you to set up whitelist/inclusion and blacklist/exclusion for scanning.

##### **Exclude certain types of files from scanning.**

Database and encrypted type files should generally be excluded from scanning to avoid performance and functionality issues. The following are sample exclusions to consider, depending on the type of machine you are installing the virus scanner client on.

**General Exclusions for All Windows Platforms**

- Pagefile.sys
- \*.pst
- %systemroot%\System32\Spool (replace %systemroot% with actual directory)
- %systemroot%\SoftwareDistribution\Datastore (replace %systemroot% with actual directory)
- %allusersprofile%\NTUser.pol
- %systemroot%\system32\GroupPolicy\registry.pol

**Microsoft Active Directory Domain Controller**

- <drive>: \ WINNT \ SYSVOL
- <drive>: \ WINNT \ NTDS
- <drive>: \ WINNT \ ntfrs
- <drive>: \ WINNT \ system32 \ dhcp
- <drive> : \ WINNT \ system32 \ dns

**Microsoft IIS Server**

- Web Server log files should be excluded from scanning. By default, IIS logs are saved in
- <drive>: \ WINNT \ system32 \ LogFiles
- <drive>: \ WINNT \ system32 \ IIS Temporary Compressed Files

**Cisco CallManager**

- Drive:\Program Files\Call Manager
- Drive:\Program Files\Call Manager Serviceability
- Drive:\Program Files\Call Manager Attendant

**Microsoft SQL Server**

Because scanning may hinder performance, large databases should not be scanned. Since Microsoft SQL Server databases are dynamic, exclude the directory and backup folders from the scan list. If it is necessary to scan database files, a scheduled task can be created to scan them during off-peak hours.

- <drive>: \ Program Files \ Microsoft SQL Server \ MSSQL \ Data
- <drive: \ WINNT \ Cluster (if using SQL Clustering)
- Q:\ (if using SQL Clustering)

**Cluster Servers**

- Q:\ (Quorum drive)
- C:\Windows\Cluster

**Microsoft Sharepoint Portal Server**

- <drive>: \ Program Files \ SharePoint Portal Server
- <drive>: \ Program Files \ Common Files \ Microsoft Shared \ Web Storage System
- <drive>: \ Windows \ Temp \ Frontpagetempdir
- M:\

**Microsoft Systems Management Server (SMS)**

- SMS \ Inboxes \ SMS\_Executive Thread Name
- SMS\_CCM \ ServiceData
- Microsoft Operations Manager Server (MOM)
- <drive>: \ Documents and Settings \ All Users \ Application Data \ Microsoft \ Microsoft
- Operations Manager
- <drive>: \ Program Files \ Microsoft Operations Manager 2005

**Microsoft Internet Security and Acceleration Server (ISA)**

- <drive>: \ Program Files \ Microsoft ISA Server \ ISALogs
- <drive>: \ Program Files \ Microsoft SQL Server \ MSSQL\$MSFW \ Data

**Microsoft Windows System Update Server (WSUS)**

- <drive:> \ WSUS
- <drive:> \ WsusDatabase

**VMware**

Other file extension types that should be added to the exclusion list include large flat and designed files, such as VMware disk partitions. Scanning VMware partitions while attempting to access them can affect session loading performance and the ability to interact with the virtual machine.

- Exclusions can be configured for the directories that contain the Virtual Machines, or by excluding \*.vmdk and \*.vmem files.
- VMware View Connection Server—Java Message Bus

**Mapped Drives/Shared Folders**

The mapped drives/shared folders option is best disabled. If it is enabled, it may create unnecessary network traffic when end-users access remote paths or mapped network drives. It can severely impact the user's experience. Consider disabling this function if all workstations have the OfficeScan client installed and updated to the latest virus signature.

**Volume Shadow Copies**

The backup process takes longer to finish when real-time scanning is enabled. There are also instances when real-time scan detects an infected file in the volume shadow copy but cannot enforce the scan action because volume shadow copies have read-only access.

It is also advisable to apply the latest Microsoft patches for the Volume Shadow Copies service:  
<http://support.microsoft.com/kb/833167>

## Conclusion

Virus and malware prevention in virtual desktops depends upon the IT architecture and the controls you have put in around the network perimeter. Some might think virus protection is not a big problem in pooled, non-persistent desktops since you can get a clean desktop after logout. However, rebooting cannot solve virus infection issues on individual and persistent desktops with separate user disk allocation. Although the practices suggested in this document apply to VMware View deployment scenarios in particular, IT professionals can consider examining their corporate virtualization and system deployment strategy and to recommend a subset of best practices for your organization.

## About the Author

Cynthia Hsieh is responsible for solution management at End User Computing Group at VMware. She focuses on application integration, proof of concepts, and security subjects. Hsieh's previous background includes product management positions at Wyse, Trend Micro, Oracle, and Yahoo.

Collectively, special thanks to Dean Flaming, John Dodge, Marios Leventopoulos, and Mason Uyeda for their in-depth desktop virtualization expertise and diligent review.

