VMware Horizon with View Security Hardening Overview

Horizon 6 with View

TECHNICAL WHITE PAPER

vmware®

Table of Contents

Introduction

Administrators and security officials need to keep their organization's data both safe and accessible. With that goal in mind, this document presents an overview of measures they can take for secure deployment and administration of VMware® Horizon™ with View™.

It is always desirable to be aware of possible vulnerabilities and to monitor new threats as they emerge; however, some fears about virtualization security are unwarranted. Because the threat landscape changes continually, those responsible for security—whether at a small- to medium-sized business, a global enterprise, or a major government agency—should implement a multi-level defense-in-depth strategy and monitor activity and access to their infrastructures based on a realistic evaluation of their particular requirements. Many industries and organizations have their own standards, regulations, and compliance requirements, the details of which are beyond the scope of this document. Familiarity with these details, however, should be considered essential for anybody responsible for virtual infrastructure security. Also beyond the scope of this document are the descriptions and security practices that apply to underlying technologies, such as VMware vSphere®. For this information, see the vSphere Hardening Guide and the Security of the VMware vSphere Hypervisor white paper.

For a description of how the various parts of a View implementation interact, see *How the Components Fit Together* in View Architecture Planning.

Clients and Endpoints

The VMware Horizon Client™ enables remote access to centrally managed View desktops and applications from a wide range of endpoint devices. The Horizon Client runs on the operating systems of endpoint devices—Windows, Mac OS, or Linux for conventional desktop and laptop computers or iOS or Android for smartphones and tablets. The Horizon HTML Access client provides access to View desktops from a Web browser, using built-in Secure Socket Layer (SSL) and Transport Layer Security (TLS) functionality.

Any vulnerability in the operating system can be a vector to compromise of the services that run on it, so it is important to take measures to harden the operating system.

Client Hardening

Recommendations for supporting Horizon Clients include the following:

- Use standard hardening practices for the guest operating system, such as those published by Microsoft and the Center for Internet Security.
- Create, deploy, and maintain password-protection policies.
- Keep software and security patching up to date.
- Verify firewall requirements.
- Install an antivirus solution on all hypervisors that support View virtual machines.
- Use RADIUS, RSA SecurID, or smart card authentication in addition to Active Directory, which is always required on Windows guest operating systems. Although a single authentication method might be sufficient under certain conditions, such as company-owned devices running on an internal network, two-factor authentication is usually preferable and should be considered mandatory for all remote devices, regardless of ownership. See *Choosing an Authentication Method* in View Architecture Planning and *Using Two-Factor Authentication* in View Administration.
- Consider developing group policies, based on Windows hardening guidelines and industry best practices, to apply and update security policies on clients uniformly on non-BYOD endpoints.
- Consider automating the installation of Horizon Client to streamline deployment and reduce manual errors. See *Horizon Client Command Line Usage* in View Administration for a listing of most properties available for deployment and execution of Horizon components.
- Deploy View Group Policy Administrative (ADM) templates for tasks, such as
  - Enabling the list of brokers trusted for delegation
  - Disabling third-party Terminal Services plug-ins
  - Disabling single sign-on (SSO) to View
  - Determining whether users can enter their credentials from the command line
  - Controlling the level of credential checking performed by the Horizon Client

These tasks are described under *Configuring Policies for Desktop and Application Pools* in View Administration and *View Security Settings* in View Security.

Endpoint Hardening

Portable personal devices are stateful: they store both user data and identifying information that are vulnerable to snooping and other attacks. Thin clients and zero clients are stateless hardware devices that connect to a View Connection Server without the need to run local operating systems or client software. Stateless devices are less vulnerable because they do not store user data or identifying information. Horizon Clients simulate the behavior of hardware clients. They do not store data or identifying information, and are also less vulnerable to attack than personal devices, desktop computers, or laptop computers.

Regardless of which endpoint devices you support, it is always best to keep them up to date with the latest software, firmware, security fixes, and Horizon Clients.

The following practices are recommended if you support mobile device users who access View desktops or applications from remote locations:

- Implement a mobile device management (MDM) solution from AirWatch® by VMware.
- Decide whether to issue organization-owned mobile devices. This decision is typically made at a corporate or agency level and is not controlled by Horizon software, but it does have implications for remediation when mobile devices are lost or compromised.
- Regardless of ownership, it is advisable to check any device's health before granting user access, especially to internal networks. Require devices used in Network Admission Control (NAC) and Network Access Protection (NAP) solutions to produce a clean bill of health.
- Establish clear policies, in advance if possible, on wiping data from endpoint devices in the event of loss, theft, termination, or other potentially compromising events.
- Enable and enforce 256-bit AES encryption at the endpoint.
- Consider using Suite B ciphers for relatively secure wireless communication.

If you do not support users who access View virtual desktops from mobile devices, consider imposing limits on wireless access to internal networks. If the main concern of your organization is security rather than productivity or convenience, consider limiting copy-and-paste functionality and disabling USB connections (see *View PCoIP General Session Variables* and *Using USB Devices with Remote Desktops* in Setting Up Desktop and Application Pools in View). These measures are recommended for situations where the highest level of security is required, but not for most business environments.

Connection Servers and Security Servers

View Connection Server, View security server, and other co-hosted services that run on Windows Server platforms are vulnerable to attacks on the Windows operating system. Use the same hardening techniques as for common Windows Server infrastructures.

Additional recommended practices include the following:

- Replace default self-signed certificates with those from a trusted certificate authority, either a commercial CA or an organizational CA.
- Make sure all communications between Horizon Clients and security servers or View Connection Servers use TLS 1.0 (the default) or later. Consider upgrading to TLS 1.1 or 1.2 on clients and servers.
- Isolate View security servers in their own domain in a demilitarized zone (DMZ), as described in Security Server Deployment. Make sure that neither the virtual nor physical Windows systems are members of the same domain as the security servers.

Also consider the following global security measures:

- Determine which authentication method or methods best suit the needs of your organization. Security servers provide the best overall solution for secure access; however, a virtual private network (VPN) can be used when required by corporate or agency policy.
- Use the principle of least privilege.
  - Limit the root administrator role to a small number of individuals.
  - Work with restrictive built-in roles whenever possible.
  - Use custom roles for specific needs.

  See *Configuring Role-Based Delegated Administration* in View Administration.

For large deployments, consider organizing desktop pools into folders. You can then use role-based access control (RBAC) to delegate administrative roles to the folders by geographical location, business unit, function, or compliance criteria, such as

- User entitlements
- Zoning virtual machines and user data
- Multi-tenancy

For more hardening recommendations for VMware vCenter Server™ and VMware ESXi™ Server, see the vSphere 5.5 Security Hardening Guide and Security of the VMware vSphere Hypervisor. For a fuller discussion of multi-tenancy considerations, see Horizon DaaS.

Event Database

To track the health of a secure View environment, configure, use, and monitor an event database. An event database stores information about View events as database records rather than log file entries, which makes it easier to examine events. See *Configuring Event Reporting* in View Installation.

Parameter Settings

You can set (or not set) parameters such as View Connection Server authentication methods, security server SSL settings, and idle timeouts for both client activity and user activity. New SSO and LDAP settings can detect when a client has crashed or lost connectivity and when a user might have left a device while the client is still running.

For example, a long View Connection session timeout value can increase the risk of exposing the session to malicious users through neglected session hijacking, man-in-the-middle attacks, and other forms of masquerade. On the other hand, end users typically find re-authentication inconvenient. In fact, a session is never more susceptible to attack than during the authentication process. Give some consideration to which settings are optimal for your organization.

- The default View Connection Server session timeout is 10 hours. Increasing this value involves less risk than requiring frequent re-authentication.
- The default View Administrator session timeout is 30 minutes. Increasing this value can increase the risk of unauthorized use of View Administrator.
- The default idle session timeout for clients that support applications is **Never**. As a best practice, set a short timeout value, such as 15 minutes, after which the session is disconnected and the SSO credentials are discarded.
- The default connection ticket timeout is 120 seconds.
- See View Security for further details.

Time Synchronization

Every View server should synchronize its time clock from a time synchronization server. Having an incorrect time clock on a security server makes SSL server certificate validation periods inaccurate and log analysis difficult. Configure all View security servers to use the same secure and trusted internal or external time synchronization server. Use the date and time setting on the Windows operating system to specify the name of an external time synchronization server. To test, verify on each security server that the clock is accurate and that it is set to synchronize from an external time source.

Security Server Hardening

View security servers ensure that only authenticated users gain access from one network to another. They function as SSL offloads that handle external HTTPS processing and virtual machine protocol traffic that would otherwise traverse an internal network.

With the correct firewall rules in place, only authenticated users on an allowed protocol can access virtual desktops. In addition, View security servers ensure that users can access only the virtual desktop resources to which they are entitled or authorized.

For large-deployment scalability and high availability, see View Architecture Planning. In cases where the networks must remain isolated from one another, see the illustrations in VMware Federal Secure Desktop and BYOD.

Security Server Hosts

View security servers can run on Windows Server 2008 R2, which is nearing its end of support, and on Windows Server 2012 R2, which is preferable. It is critical to protect security server hosts against normal operating system vulnerabilities and attacks. The following basic recommendations always apply:

- Install antivirus software (preferably a VMware vShield Endpoint™ security virtual appliance from a VMware partner), spyware filters, intrusion detection systems, and other security measures according to your organization's policies.
- Keep all security measures up to date, including the application of OS patches.

In addition

- Restrict administrative Windows login access. Create specific administrative login accounts for individuals, and make those accounts members of the local administrators' group. If an unauthorized administrator gains access to a security server, the server becomes vulnerable to inadvertent modification as well as to deliberate attack. For password policies
  - Follow corporate or organizational security guidelines. In cases where none are defined, consider implementing an administrative password policy for every View security server and, in some cases, separate password policies for each View security server.
  - Include restrictions on minimum length and character types, and requirements to periodically change passwords.
- Remove unnecessary network protocols. If unnecessary protocols are enabled, a View security server can expose a larger vector to network attack. View security servers use only IPv4 communication.
  - Remove other protocols, such as file and printer sharing for Microsoft Networks and Novell IPX.
  - In the Control Panel on each View security server, look at the properties of each network adapter, and remove or uninstall protocols that are not required.
- Disable unnecessary services. View security servers require only a small number of network services. Disabling unnecessary network services prevents them from starting automatically at boot time and exposing a security server to network attacks.
- Ensure that no server roles are enabled.

Security Server Deployment

View security servers should be deployed in a demilitarized zone (DMZ)—between an external and an internal firewall—especially in environments that include distinct, separate networks. The purpose of a DMZ is to control client access over a hostile network, such as the Internet. However, in spite of the external firewall, the DMZ should still be considered an untrusted environment. To protect the DMZ, it is essential to configure the View security servers, hosts, and any user devices correctly. The following suggestions can be considered best practices:

- Set up a DMZ by configuring firewalls on both sides of the View security servers. This is the most effective way to restrict protocols and network ports to only those required for communication between Horizon Clients and the security servers.
- For communication between security servers and the data center, limit the protocols and network ports from the security servers. View security servers automatically handle TCP forwarding to virtual desktops in a data center and ensure that traffic is forwarded only on behalf of authenticated users.
- Limit the scope of frame broadcasts by deploying View security servers on an isolated network. This topology can help prevent a malicious user on the internal network from monitoring communication between the security servers and View Connection Servers.
- Use advanced security features on your network switches to prevent malicious monitoring of communication between View security servers and View Connection Servers, and to guard against monitoring attacks, such as ARP cache spoofing. For more information, see the administration documentation for your networking equipment.

For illustrations of different DMZ topologies, see *Security Server Topologies* and *Firewalls for DMZ-Based Security Servers* in View Architecture Planning. For topologies suitable for high-security implementations, see VMware Federal Secure Desktop and BYOD.

Security Server Configuration

When a View security server is first installed, the SSL server defaults to self-signed certificates. *Do not use the default self-signed server certificates on a View security server in a production environment*. Replace them with SSL server certificates signed by a commercial or organizational Certificate Authority (CA). Although it is possible to use self-signed certificates securely under some circumstances, such as for testing purposes, most experts agree that default certificates leave the SSL connection vulnerable to man-in-the-middle attacks.

For information on how to replace View security server SSL certificates, see *Understanding SSL Certificates for View Servers* and *Configuring SSL Certificates for View Servers* in View Installation.

To verify that the certificates are valid

- Use a Web browser to make an HTTPS connection to the View security server and inspect the server SSL certificate. Verify that the certificate is signed by the appropriate CA.
- Use the Online Certificate Status Protocol (OCSP) to manage certificate revocation when using smart card authentication.
- Restrict the allowable ports and services to those necessary for the display protocol, such as PCoIP.
- For large deployments, consider organizing resources into access groups. Delegate administrative roles to the groups by geographic location, business unit, function, or compliance.

Guest Operating System Hardening

To automate the desktop and server deployment of a Windows OS, you can use the Microsoft Deployment Toolkit (MDT). For more information, see the VMware Horizon with View Optimization Guide for Windows 7 and Windows 8.

You can determine which features to make available to your users. As a guideline, consider the following items when hardening the parent virtual machine:

- Base operating-system hardening
- Refresh and recompose intervals
- Antivirus solutions
- Patch base operating system
- View Agent
- USB devices and redirection
- Drive redirection
- Clipboard redirection
- Printer redirection
- Multimedia redirection
- Single sign-on (SSO)
- Available display protocols
- Smart cards

Some settings are managed by the View Agent (see, for example, *View Agent Custom Setup Options* in Setting Up Desktop Application Pools in View). Other settings, such as those for Horizon Clients on Windows guest operating systems, are managed by Active Directory Group Policy Objects (GPOs).

Use the master VDI templates updated for your target operating system to know what you can manage in each level.

Use VMware View Administrator to control guest and host cut-and-paste and USB access. These features are useful for productivity in most settings, but they can open significant security holes in sensitive settings. Review which functionalities to enable or disable. For example

- USB functionality can enable features such as Follow Me Printing, but it can also allow large amounts of data to be copied to a thumb drive.
- USB functionality can open a large vector for the introduction of malware, such as the Stuxnet virus or later variants.
- Cut-and-paste and copy-and-paste are also useful but should not be enabled by default or without due consideration.

Define a patch management strategy based on the following considerations:

- Apply patches to the parent virtual machine, and recompose all virtual desktops periodically—monthly, weekly, or more often, if necessary.
- Decide in advance how to handle critical updates.
- Decide whether to include a combination of recompose and standard patch management tools, such as Windows Service Update Service (WSUS), System Center Configuration Manager (SCCM), and Altiris.

PowerShell Execution Policy

Windows PowerShell provides flexibility for automations and administrative tasks, but using it also means that you need to consider a safe way to prevent users from running untrusted scripts. When Windows PowerShell is first installed, it can be used interactively, but it cannot run scripts because the execution policy is set to the default setting of **Restricted**. View PowerCLI provides an easy-to-use PowerShell interface to View. See *Using View PowerCLI* in View Integration.

Some people consider the `AllSigned` execution policy to be a safe option, although it is not difficult to bypass. `AllSigned` requires that all scripts and configuration files, including scripts that you write on the local computer, be signed by a trusted publisher. If the execution policy is set to `AllSigned`, nontechnical users can run a subset of safe scripts that you have signed for them.

To view the execution policy, use the `Get-ExecutionPolicy` cmdlet. Accounts with administrator privileges can modify the policy with the following command:

```
code:Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
```

This command allows local scripts to run, but it blocks scripts from the Internet or UNC-mapped drives unless they are signed with a code-signing certificate that the system can accept.

For more information about PowerShell execution policy settings, see the Microsoft Press *Windows PowerShell Best Practices*.

Kiosk Mode Hardening

Kiosk Mode is designed to enable anonymous use of public endpoints, usually thin clients, zero clients, or locked-down PCs, at airline check-in stations, libraries, or similar self-service points. Client ID or MAC addresses are used to associate virtual machines with devices rather than with users, so that anyone can use a kiosk for a restricted set of functionalities without having to log in. View virtual desktops that are set to run in Kiosk Mode use nonpersistent images because user data does not need to be preserved on the OS disk.

In general, Kiosk Mode should not be used for transactions that require sensitive information, such as credit card numbers or user email accounts and passwords. Kiosks are public by definition and are intended to be anonymous. However, if your organization needs to use Kiosk Mode in a semi-private location, such as a corporate cafeteria, users might be required to provide authentication credentials for some applications. In such cases, make sure that

- The application implements authentication mechanisms for secure transactions.
- The physical network is secure against tampering and snooping.
- All devices connected to the network are trusted.

As a best practice, use dedicated View Connection Server instances to handle clients in Kiosk Mode, and create dedicated organizational units and groups in Active Directory for the accounts of these clients. This practice partitions these systems against unwarranted intrusion and also makes it easier to configure and administer the clients.

Additional Security Practices

For general security hardening practices, keep the number of open ports to a minimum, and establish a policy to manage ports.

For applications running in a base virtual machine, the following practices are recommended:

- Remove unneeded default applications.
- Restrict access to administrative applications.
- Restrict access to deployed applications.

Network Security

Consider using stateful inspection network firewalls, such as VMware NSX™ distributed firewall or VMware NSX Edge™ gateway with a default-deny rule set and exceptions to restrict access or unauthorized communication between virtual machines. This solution provides an extra layer of protection against the spread of malware.

Whether you use these firewalls or others that might already be in place, remember to place View security servers and any Internet-facing servers in a DMZ with strong default-deny rules on the firewall to prevent data exfiltration. For similar reasons, a security server should run in its own domain inside the DMZ. You can use a network intrusion detection or intrusion prevention system (IDS/IPS) to monitor and prevent known attacks. If an SQL Server is configured for event monitoring or VMware View Composer™, put the database on an internal network, not in the DMZ.

In vSphere environments, NSX is recommended for securing the edge of the virtual data center and protecting virtual applications from network-based threats. The preferred solution for antivirus protection is to use one of the dedicated security virtual appliances enabled by vShield Endpoint. For more information on vSphere hardening, see Security of the VMware vSphere Hypervisor.

Security Scanning

Consider running security scanning software against Horizon infrastructure components before and after implementation to identify possible security vulnerabilities or further hardening steps to take. Software options include Nessus, Qualys, and Retina. If you do run a security scanner, check occasionally for VMware Knowledge Base articles about the possibility of false positives, such as SSL certificate error when scanning PCoIP secure gateway port 4172.

Summary

This document provides an overview of major security concerns and hardening techniques for Horizon with View and is meant to remind administrators and security officials to be guided by the following principles:

- Adopt a defense-in-depth strategy to reduce the likelihood of attacks breaking through multiple barriers.
- Remain alert to new threats. There is no such thing as a complete security solution.
- Secure all devices and communication channels. Remember, the endpoint is the weak point.
- Use firewalls, preferably security servers in demilitarized zones, to secure your organization's perimeter.
- Use antivirus appliances to protect every hypervisor.
- Apply the principle of least privilege to limit unauthorized access within your organization.
- Make sure that security policies are enforced, otherwise they cannot be effective.

References

Enabling VMware vShield Endpoint in a VMware Horizon View Environment

Framework for Improving Critical Infrastructure Cybersecurity

Inadequate Security Practices Expose Key NASA Network to Cyber Attack

Securing VMware Horizon View Deployments

Security Configuration Benchmark For Microsoft Windows 7

Security Configuration Guidance Support

Security Considerations for VMware Horizon View 5.2

Security of the VMware vSphere Hypervisor

Security Solution Architecture for VDI

View Documentation

View Installation

VMware Horizon with View Optimization Guide for Windows 7 and Windows 8

View Security

VMware Federal Secure Desktop and BYOD

VMware Horizon Clients Documentation

VMware vSphere 5.5 Security Hardening Guide

VMware vSphere Blog

Windows PowerShell Best Practices

About the Author and Contributors

This paper was revised and updated by Gary Sloane, a consultant for VMware End-User Computing, based in part on an unpublished paper by Rob Baesman, Mark Benson, Andre Leibovici, Cynthia Hsieh, and Gargi Mitra Keeling.

The following people supplied additional material and review comments:

- Kofi Ahulu
- Stephane Asselin
- Mark Benson
- Yee Chin
- Greg Christopher
- Mike Foley
- Paul Green
- Andrew Johnson
- Narasimha Krishnakumar
- Robert Pinkoske
- Sean McGuire
- Eric Oo
- Mike Pryor
- Rob Randell
- Neena Razdan
- Peng “Terry” Wang
- Chris White

vmware®

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