VMware® Horizon Workspace™ 1.5 Security Considerations

WHITE PAPER
Table of Contents

Introduction ................................................................. 3
Components ....................................................................... 4
Authentication and Authorization........................................ 5
Auditing ............................................................................ 6
Demilitarized Zone (DMZ) .................................................. 6
Sharing .............................................................................. 7
Access Control ................................................................... 7
Device Control .................................................................... 8
Conclusion ......................................................................... 9
About the Author ............................................................... 9
References .......................................................................... 9
Introduction

VMware® Horizon Workspace™ is a virtual appliance (vApp) deployed in the customer datacenter to provide ease of access to data, virtual desktops, VMware ThinApp® packages, and Software as a Service (SaaS) applications. Horizon Workspace unifies the end-user experience and reduces IT costs by combining applications and data into a single, enterprise-class aggregated workspace, which can be delivered securely on any device.

The goal is to provide control and flexibility without constraints. However, because Horizon Workspace enables external access and facilitates the use of both managed and unmanaged devices for that purpose, security questions require appropriate consideration.

To deploy Horizon Workspace robustly and securely, IT architects, system administrators, and technical personnel should understand the Horizon Workspace architecture and where to apply VMware best practices.

This document gives an overview of some important security considerations and recommendations. For further details on Horizon Workspace features and functionality, refer to the VMware Horizon Workspace Documentation and the References at the end of this document.
Components

The Horizon Workspace vApp consists of five virtual appliances:

- Horizon Gateway (gateway-va) – The entry and endpoint for Horizon Workspace. An external proxy or load balancer forwards all network traffic through Secure Socket Layers (SSL) on port 443 to the Horizon Gateway virtual machine, which then proxies requests to the other virtual appliances.

- Horizon Service (service-va) – Maintains sessions and logic for SaaS-based authentication and authorization, based on the industry-standard Security Association Markup Language (SAML). The VMware Horizon Application Manager™ is part of Horizon Service. The Horizon Service also provides the Administrator Web interface used for managing applications, data, and entitlements for users and groups.

- Horizon Files™ (data-va) – Provides file synchronization functionality and maintains any data files that are transferred between desktop, mobile, or Web clients, and enables data sharing and collaboration.

- Horizon Connector™ (connector-va) – Provides synchronization between Microsoft Active Directory (AD) and Horizon Workspace, plus the configuration for the VMware ThinApp repository, and VMware Horizon View™ pool synchronization.

- Horizon Configurator (configurator-va) – You use the Configurator to install and configure Horizon Workspace. It provides a wizard to help you set up and push configuration settings to the other virtual machines in the vApp.

The Horizon Workspace vApp is distributed on a SUSE Linux virtual machine that has been subjected to initial hardening, such as closing or disabling unused ports, and network tuning. All virtual machines follow the VMware security hardening guidelines detailed in VMware Horizon Workspace Security Features. In addition, all components of the Horizon Workspace vApp undergo routine in-house and external security testing. Depending on your enterprise security requirements, you may need to perform additional hardening, such as encryption on servers and other elements of the physical infrastructure.
Authentication and Authorization

Horizon Workspace integrates into Microsoft Active Directory, using federated identity for single sign-on (SSO). You can apply authentication policies to existing groups as well as to new users and new groups.

The following figure illustrates how users and groups can be imported from AD, mapped to Horizon, and granted entitlements.

Entitled users are authenticated with their desktop credentials (Kerberos) or their AD credentials or, if connecting externally, with an assigned RSA SecurID token. The Horizon Workspace administrator can set session timeouts and other authentication token-related configuration items with the administrative console.
Auditing

Use an external firewall to enable auditing of the external network connection—to help to track, among other events, anomalous connections from potential attackers—as well as an internal firewall with auditing enabled. Horizon Gateway communicates with other Horizon Workspace components only over SSL connections.

Horizon Workspace audits user events, such as login, logout, entitlement, and user provisioning, as well as administrative events concerning new user and group creation and user and group entitlements to applications. Audit reports can be accessed from Horizon Workspace reports.

Demilitarized Zone (DMZ)

Enterprise networks are typically designed to separate external (Internet) and internal (intranet) network traffic. To minimize the risks associated with leakage and intrusion, any component on the internal network that interacts with the Internet or exposes a service to it should be placed in a demilitarized zone (DMZ). The other components remain on the internal network, protected by a firewall.

In the following figure, the Horizon vApp (including the Gateway) is placed behind the DMZ. The DMZ has a load balancer or enterprise proxy that routes traffic to the Gateway. The vApp has both a routed network connection—to facilitate communication outside the enterprise—and an internal connection to all Horizon Workspace components.

To further strengthen security—especially to prevent, or at least mitigate, man-in-the-middle (MITM) attacks against clients connecting from outside the firewall—use trusted certificates as your first line of defense. Horizon Workspace generates self-signed certificates that are sufficient for proof of concept (PoC) or pilot projects but not for production environments. Trusted certificates, however, enable browsers and Horizon applications to detect forged connections and warn users not to connect to suspicious servers. Trusted certificates are widely available from SSL vendors.
Sharing

Horizon Workspace accommodates users’ wishes to share files and folders, both inside and outside the corporate firewall. When setting up or administering a Horizon Workspace implementation, give careful consideration to which aspects of this functionality best suit your environment and security concerns. For instance, you can enable or disable public sharing (with expiration policies for share invitations) and configure selective domains for blacklisting or whitelisting—by user account level or by class of service (CoS) level.

Access Control

Horizon Workspace provides the ability to manage users and their roles, privileges, and entitlements.

To enhance the intrinsic security of a Horizon Workspace implementation, use the least privilege principle to grant the access rights and permissions that users and administrators need to perform their official duties. This restricts opportunities for data leakage, password compromise, or other potential vulnerabilities.

In particular

- Grant users, or classes of users, access only to the tools and information they need.
- Use separate accounts to administer Active Directory, Horizon Workspace, and SaaS provisioning.
- Use separate user accounts for administration and for user functions.
  - Have the IT administrator set up an AD user account for the Horizon Workspace administrator.
    
    The IT administrator should verify that the Horizon Workspace administrator does not have AD domain or local administrator privileges. Limiting the Horizon Workspace administrator’s AD privileges reduces the chance of attack in case that account is compromised.
  
  - Use the Horizon Workspace administrator account only for Horizon administration.

  Never use this account to access Horizon applications, desktops, or files. The person who performs Horizon Workspace administrator functions should always use a separate, non-administrative Horizon user account when performing normal user functions.
  
  - Have the Horizon Workspace administrator explicitly create and entitle a Horizon user account for SaaS administrator tasks, to be used only for SaaS provisioning.

    The SaaS administrator can integrate most SAML applications, such as Google Apps, Salesforce, and Box.net, into Horizon Workspace but should not be able to perform Horizon Workspace administration functions.

    The SaaS administrator account must never be the same account as the Horizon Workspace administrator.

These practices help to reduce potential attack vectors and credential leakage.

Access, roles, and privileges are discussed at greater length in Managing Users and Groups in the Horizon Workspace Administrator’s Guide and vSphere Security in the VMware vSphere® 5.1 Documentation Center.
Device Control

It is important to set access privileges appropriately when users work remotely, especially on their own devices. The Bring Your Own Device (BYOD) phenomenon has now become a fact of life, and Horizon Workspace enables content sharing and file synchronization across a wide range of devices and browsers. However, BYOD also increases the risks associated with intrusion, malware, and theft of data and devices—even more so for unmanaged devices. For enterprises with special security needs, zero clients may offer a better mobility solution than smart phones, tablets, or conventional PCs. In these circumstances, you have to evaluate the trade-offs between convenience and security.

It is important to evaluate the risks and benefits of various device types and to educate your users about minimizing exposure to wireless and Bluetooth snooping.

In case of a breach, Horizon Workspace provides a remote wipe capability. Both administrators and end users can remotely wipe the Horizon Workspace client and all its content from a device. Wiping the client does not clean the entire device, so user files and personal data are neither lost nor protected. This capability should be used judiciously. After a device is wiped, the end user has to enter server information and valid credentials to relink to the Horizon Workspace server.

If a mobile device is rooted or jail-broken, however, any keys in its key chain should be considered compromised.
Conclusion

Long before the invention of the Internet, General Douglas MacArthur observed, “There is no security on this earth.” That does not mean we cannot strive for real security, but achieving it is a lot like approaching a limit: We can always get closer, but we will never quite get there.

With that pleasant thought in mind, it is best to evaluate your security policies thoroughly and often. Just as important, verify that they are fully implemented.

This brief document can never be complete, because security threats are continually evolving, but it can help to steer you in the right direction.

About the Author

Manrat Chobchuen is a Technical Solutions Architect in the VMware End-User Computing Solutions group who specializes in cloud storage and system scaling, as well as security.

To comment on this paper, contact the VMware End-User Computing Solutions Management and Technical Marketing team at twitter.com/vmwareeucsmtm.

References

Horizon Workspace Documentation
BYOD security strategies: Balancing BYOD risks and rewards, by Lisa Phifer
Secure Remote Access for Government Teleworkers
VMware View Security Hardening Guide
VMware vSphere 5.1 Documentation