# Integrating VMware Horizon Workspace and VMware Horizon View

## Table of Contents

1. Introduction ............................................................. 3
   - Requirements ......................................................... 3
   - Horizon Workspace Components .................................. 3
   - SAML 2.0 Standard .................................................. 3

2. Authentication Flow Sequence ...................................... 4

3. Configuring Horizon Workspace and Horizon View ............... 5
   - Initial Horizon View Setup ........................................ 6
   - Initial Horizon Workspace Setup ................................. 6
   - Configuring Horizon Workspace .................................. 6
     - Directory Synchronization ...................................... 9
     - Join Horizon View Active Directory Domain ................. 11
     - Configure and Synchronize Horizon View Pools ............. 12
     - Validate User and Group Entitlements to Horizon View Pools 14
   - Configuring Horizon View ......................................... 15
   - Verify Desktop Launch Capability ................................ 16
   - Horizon View Pool Protocol Selection .......................... 17

4. Configuring SAML 2.0 Authentication ............................ 18
   - Authentication in Horizon View .................................. 18
   - Enable a SAML 2.0 Authenticator ............................... 19
   - Add a SAML 2.0 Authenticator .................................... 20
   - Manage Authenticators ............................................. 21
   - Select an Existing SAML 2.0 Authenticator ..................... 21
   - Dashboard ......................................................... 21
   - Authentication in Horizon Workspace ............................ 22

5. Extended Functionality ............................................... 23

6. Troubleshooting and Tips ........................................... 25

7. Conclusion ............................................................. 27

8. References ............................................................. 28

9. About the Authors .................................................... 28
Introduction

This paper describes how to integrate VMware® Horizon View™ with VMware Horizon Workspace™, using the Security Assertion Markup Language (SAML) 2.0 standard to establish mutual trust, which is essential for single sign-on (SSO) functionality. With SSO enabled, users who have logged in to Horizon Workspace with Active Directory (AD) credentials can launch Horizon View desktops without having to go through a second login procedure.

Requirements

Integration of Horizon View with Horizon Workspace requires Horizon View Client 1.6 or later with Horizon View 5.2 or later and Horizon Workspace 1.0.

After Horizon Workspace and Horizon View are installed, you need to perform the following tasks:

• Configure Horizon Workspace with Horizon View information.
• Configure Horizon View to delegate responsibility for authentication to Horizon Workspace. To do this, you create a SAML 2.0 Authenticator in Horizon View to contain the trust and metadata exchange between Horizon View and Horizon Workspace.

These tasks are independent of one another and can be performed in any sequence. However, after you add SAML Authenticator information in Horizon View, use VMware Horizon Connector™ to make sure this information is saved and synchronized.

Horizon Workspace Components

Horizon Workspace includes five components, which are deployed as separate virtual appliances in a vApp and described in Installing Horizon Workspace:

• VMware Horizon Configurator (configurator-va)
• VMware Horizon Manager (service-va), also known informally as Horizon Service
• VMware Horizon Connector (connector-va)
• VMware Horizon Data™ (data-va)
• VMware Horizon Gateway (gateway-va)

SAML 2.0 Standard

SAML is an XML-based standard used to describe and exchange authentication and authorization information between different security domains. It passes information about users between identity providers and service providers in XML documents called SAML assertions.

Integrated Horizon Workspace deployments use SAML 2.0 Authenticators to provide single sign-on (SSO) functionality.
Authentication Flow Sequence

Figure 1 illustrates the authentication flow sequence, from user login to the launch of a Horizon View desktop, after Horizon View and Horizon Workspace are integrated.

URI: vmware-view://connection-server/desktop?SAMLart=XXXXXXXXXXXX

1. A user logs in to Horizon Gateway and clicks a Horizon View pool icon. Horizon Manager (Service) generates a unique SAML 2.0 artifact and uses it to create a Universal Resource Identifier (URI), which launches the View Client through Horizon Gateway. The URI, which is based on the vmware-view:// scheme, contains information about the View Connection Server where the pool resides, which desktop to launch, and the SAML 2.0 artifact.

2. The Horizon Manager sends the SAML 2.0 artifact to the View Client through Horizon Gateway, which, in turn, sends it to the View Connection Server.

3. The View Connection Server validates the SAML 2.0 artifact and verifies that it has not been used before. The View Connection Server stores previously used artifacts (the default is 10,000).

4. Using the SAML 2.0 artifact, the View Connection Server retrieves the SAML 2.0 assertion from the Horizon Manager through Horizon Gateway.

5. As in step 3, the View Connection Server then validates the SAML 2.0 assertion and decrypts the user’s password.

6. Using the decrypted password from the SAML 2.0 assertion, the View Connection Server launches the Horizon View desktop.
Configuring Horizon Workspace and Horizon View

The Horizon Workspace and Horizon View components need to establish trust and set up common configuration features before desktops can be discovered and presented to users.

- Use Horizon Workspace Configurator to perform initial configuration. You need to configure Horizon View to delegate responsibility for authentication to Horizon Workspace, which provides SAML 2.0 authentication.
- Use the Horizon Connector Web Interface to perform all other administration tasks.
- Users go through Horizon Gateway to access Horizon Workspace and Horizon View desktops.

Figure 2: User Login and Administrator Tasks
Initial Horizon View Setup

View Connection Servers and View Security Servers must be configured only on the default HTTPS port (443). Non-default ports for Horizon View servers and intermediate devices, such as load balancers between Horizon Workspace and Horizon View pods, are not supported with Horizon Workspace 1.0.

1. Deploy VMware Horizon View.
   For instructions, see VMware Horizon View Installation.
2. Verify that the Horizon View environment is configured and that Horizon View pools are created.
3. Entitle Active Directory users and groups to the appropriate Horizon View pools.
4. Verify that all Horizon View users have email address assigned in Active Directory. Horizon Workspace does not sync users who have null email addresses.

Initial Horizon Workspace Setup

You can integrate Horizon View with Horizon Workspace through either the Horizon Configurator Web interface or the Horizon Connector Web interface. This paper, however, provides instructions only on how to perform integration from the Horizon Connector Web interface.

If Horizon Workspace is not yet installed and configured, see Installing Horizon Workspace for instructions.

Configuring Horizon Workspace

Perform the following steps after Horizon Workspace and Horizon View are installed:

1. Point Horizon Workspace and the Horizon View pod to the same Network Time Protocol (NTP) server.
   For domain-joined servers, the Active Directory often acts as the NTP server. Horizon Workspace components sync with their respective hosts, which should sync with the same NTP server as the Active Directory server.
2. Verify that the Horizon View deployment, as well as each virtual appliance in the Horizon Workspace vApp, has both its own DNS entry and static IP address with reverse lookup.
   If reverse lookup is not properly configured, the Horizon Workspace integration with Horizon View fails.
3. Log in to the Horizon Workspace Connector Web interface at:
   https://<HorizonConnectorFQDN>:8443/hc/admin/
4. Navigate to the **Directory** page, and provide details about the domain controller server host name.

![Figure 3: Enter Details in Directory Window](image)

If your deployment uses a multidomain Active Directory Domain Service (AD DS) forest, see **Extended Functionality** and **Configuring a Multi-domain Active Directory Domain Service Forest**.

5. Navigate to the **User Attributes** page, then select **userPrincipalName** as the required attribute, and click **Save**.
6. The userPrincipalName (UPN) field is required so that information about the user can be passed in SAML assertions.
Directory Synchronization
To allow Horizon Workspace to get information about Active Directory users and groups, you need to synchronize users and groups that have Horizon View pool entitlements with Horizon Workspace.

1. Navigate to the Directory Sync page, where you can schedule sync jobs and save sync rules.
2. Click Edit Directory Sync Rules, enter the Active Directory DN for Users, and click Next.

3. On the Select Users page, click View Results or View Errors to display more detailed information about the sync status. Click Next to select specific groups.
4. On the Select Groups Page, add specific Active Directory groups to sync, and click **Next**. 
   **Note:** Select groups explicitly to make sure they get synchronized.

   ![Select Specific Groups](image)

   **Figure 7:** Select Specific Groups

   5. Click **Next** to perform a dry run. This step provides information about the users and groups to be added to or removed from the Horizon database.

   ![Push to Horizon](image)

   **Figure 8:** Directory Sync Status Displaying Users and Groups to Be Synched

   6. Click the **Users** or **Groups** link to display the list of users or groups to be synchronized.

   7. Click **Save and Continue** to synchronize the selected users and groups.
Join Horizon View Active Directory Domain
To allow Horizon Workspace to authenticate with Horizon View and get configuration information from the View Connection Server, you have to join Horizon Connector to the same domain as the View Connection Server.

- Provide the required domain information and credentials on the Horizon Connector Join Domain page, as shown below.

Figure 9: Horizon Connector Join Domain Page
Configure and Synchronize Horizon View Pools

After you perform a directory sync operation, to synchronize all required domain users, and join Horizon Connector to the same domain as the Horizon View pod, you need to provide Horizon View pod details to Horizon Workspace.

Horizon Workspace establishes trust with each of the View Connection Servers in the Horizon View pod. During the sync operation, Horizon Connector fetches information about all the Horizon View pools and their entitlements from View LDAP and stores it in the Horizon database. If the primary View Connection Server is not available during a sync operation, Horizon Connector continues to perform the sync operation, whether scheduled or manual, from the next replicated View Connection Server available.
Use the following steps to configure Horizon View pools:

1. Navigate to the **View Pools** page, click **Enable View Pools**, and provide information about the Horizon View environment.

2. Provide the Fully Qualified Domain Name (FQDN) of the primary View Connection Server in the **Connection Server** field.

3. Enter an account with at least read-only administrator privileges from the View Connection Server domain in the **Username** field. Horizon Connector fails to bind with View LDAP if this View Administrator user account is not from the same domain as the View Connection Server.

4. The **FQDN for Client Access** field is the end user’s entry point when a Horizon View desktop is launched. This is the same URL that you provide for a View Client.

5. Select **Enable SSO** to enable single sign-on to the Horizon View desktop.
   
   If this feature is disabled, users have to re-authenticate when a Horizon View desktop is launched from Horizon Workspace.

6. Click **Save** to enable Horizon Workspace to fetch information about all the View Connection Servers in the Horizon View pod, Horizon View SSL certificates, and the status of the SAML 2.0 Authenticator on the View Connection Servers.

7. Click the **Update SSL Cert** link next to each View Connection Server, and click **Accept** on the **Certificate Information** page.

8. Click **Save** on the **View Pools** page to save the updated certificates from View Connection Servers.

SSL certificates are not accepted by default. You must accept a SSL certificate explicitly, by clicking Invalid/Update SSL cert. If any SSL certificate fails to get validated during the sync operation, the sync operation fails.
9. Click **Sync Now** to sync Horizon View pool information.

   This process gathers Horizon View pool information from all the View Connection Servers in the Horizon View pod and stores it in the Horizon Workspace Database.

![Figure 12: Window Displaying Horizon View Pool Details to Be Synched](image)

The Sync operation synchronizes the following items:

- Number of View Connection Servers in a pod
- Horizon View pool entitlements
- Pool display names
- Protocols supported
- Pool state

**Sync Now** also performs a dry run and reports information about which pools are to be synchronized.

10. Click **Continue** on the dry sync action and complete the sync job.

11. You can schedule recurring sync operations. The frequency of the sync operation typically depends upon how often your Horizon View deployment is updated.

   Horizon does not synchronize information about the number of desktops in a pool, so you do not need to run a sync operation when you add or remove a desktop from a pool. Adding or removing a pool, however, does require a sync operation.

12. To check sync operation status, click **Check Alerts** under **Last Sync Status Summary**.

### Validate User and Group Entitlements to Horizon View Pools

The Horizon View pool sync operation stores Horizon View environment details in the Horizon database.

1. To verify that sync operation has succeeded, log in to the Horizon Workspace Administrator Web interface at:

   `https://<HORIZONGATEWAYFQDN>/SAAS/

2. Select **Catalog** > **View Pools**, and click a Horizon View pool.

   The **Entitlements** option displays information about group and user entitlements for that Horizon View pool.

   The **Details** tab displays the connection information, which consists of attributes retrieved from the View Connection Server instance.

This completes the preliminary configuration from Horizon Workspace.
Configuring Horizon View

When the preliminary procedures are complete, perform the following steps:

1. Configure the View Connection Server to delegate responsibility for authentication to Horizon Workspace.

   See Authentication in Horizon View for more information on Horizon View SAML 2.0 authentication settings and options.

2. After SAML is enabled and updated from the View Connection Server, verify that this information is correctly displayed on the Horizon Connector View Pools page.

   Click Save to get updated SAML information from View Connection Servers.

   ![View Pools](image)

   Figure 13: Verify Information on View Pools Window

This completes the Horizon Workspace and Horizon View integration process.
Verify Desktop Launch Capability

To verify that the preceding procedures have succeeded, launch a Horizon View desktop from Horizon Workspace, using SSO:

1. Log in to Horizon Workspace as a Horizon View pool user from a Horizon View Client on any supported device. The URL is:
   https://<HorizonGatewayFQDN>/web
2. Navigate to the Computers tab.

   ![Figure 14: Horizon Workspace Computers Window](image)

3. Click a pool icon to launch a Horizon View desktop from that pool.

   If your pool supports Horizon View HTML Access, you can right-click the pool icon to select a protocol. This selection is retained for the next desktop launch.
   - **Open with VMware View** uses the Horizon View Client.
   - **Open with web browser** uses an HTML browser to launch a desktop.

   If the Horizon View Client is not installed, selecting **Install View Client** redirects you to an appropriate download link.
Horizon View Pool Protocol Selection

When you create or edit Horizon View pools from the View Administrator console, you can choose which protocol, PCoIP or RDP, to use by default when users launch Horizon View desktops. With the Open with VMware View option, Horizon View desktops launched from Horizon Workspace use whichever protocol is selected as Default display protocol.

The Allow users to choose protocol setting does not apply when users launch their Horizon View desktops from Horizon Workspace.
Configuring SAML 2.0 Authentication

Further details about authentication procedures and options for Horizon View and Horizon Workspace are described in the following sections.

Authentication in Horizon View

To launch Horizon View desktops from Horizon Workspace, you need to configure SAML 2.0 Authentication in Horizon View.

1. Log in to the Horizon View Administrator Web interface with an administrative user account.
2. Select View Configuration > Servers from the navigation panel to access the SAML 2.0 settings described in the following sections.
3. On the Connection Servers tab, select a Connection Server from the list and then select Edit > Authentication.
4. Configure each Connection Server that you want to use SAML 2.0 for authentication to Horizon.

Figure 16: Configuring SAML Authenticator Information
Enable a SAML 2.0 Authenticator

Use the Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator) drop-down menu to enable and disable the SAML 2.0 Authenticator.

![SAML 2.0 Authenticator Drop-Down Options](image)

The menu options are described in the table below:

<table>
<thead>
<tr>
<th>MENU OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Required    | • SAML 2.0 Authentication is enabled.  
• You can launch Horizon View desktops only from Horizon Workspace. You cannot launch Horizon View desktops from the View Client manually.  
• You can use SSO to access the Horizon View desktop. Smart card and two-factor authentication options are disabled. |
| Allowed     | • SAML 2.0 Authentication is enabled.  
• You can launch Horizon View desktops from both the View Client and Horizon Workspace.  
• You can use SSO to access the Horizon View desktop. Smart card and two-factor authentication options are enabled and can be selected.  
Smart card and two-factor authentication are used only by the View Client and are ignored by the Horizon Portal. |
| Disabled    | • SAML 2.0 Authentication is disabled.  
• You can launch Horizon View desktops from both the View Client and the Horizon Workspace if SAML was configured before changing it to disabled state.  
• You cannot use SSO to access the Horizon View desktop from Horizon Workspace.  
• Smart card and two-factor authentication options are enabled and can be selected. |

Table 1: SAML 2.0 Authenticator Options
Add a SAML 2.0 Authenticator
There are two ways to add a new SAML 2.0 Authenticator:

1. On the SAML Authenticator drop-down menu, select Create New Authenticator.
2. Use the Manage Authenticators option, and click Add (see Manage Authenticators).

Both options display the Add SAML 2.0 Authenticator window.

![Add SAML 2.0 Authenticator Window](image)

The fields are described in the table below:

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>This is a required field that must contain a unique name for the SAML 2.0 Authenticator you are creating.</td>
</tr>
<tr>
<td>Description</td>
<td>This is an optional field that can contain the description of the SAML 2.0 Authenticator to make the label more informative.</td>
</tr>
</tbody>
</table>
| Metadata URL     | • This is a required field and the URL must be HTTPS. The full URL is: https://<YOUR HORIZON SERVER NAME>/SAAS/API/1.0/GET/metadata/idp.xml  
• Instead of typing in the full URL, you can select the Metadata URL field.  
• The section <YOUR HORIZON SERVER NAME> is highlighted where you can provide the FQDN or IP address of your Horizon Gateway or the load balancer. |
| Administration URL | This should point to the Horizon Connector Web interface. It is an optional field. |

Table 2: Add SAML 2.0 Authenticator Fields

After you enter valid details, you must either accept the self-signed certificate (self-signed certificates are not recommended) or use a trusted certificate for Horizon View and Horizon Workspace.

After this, the SAML 2.0 Authenticator drop-down menu displays the newly created authenticator, which is now set as the selected authenticator.
Manage Authenticators
Use the Manage Authenticators options to add, edit, or remove SAML 2.0 Authenticators. Removing the last authenticator used by a View Connection Server in the Horizon View pod sets the SAML 2.0 Authenticator to Disabled. You cannot remove an authenticator if it is being used by any View Connection Server in the Horizon View pod.

Select an Existing SAML 2.0 Authenticator
Select a SAML 2.0 Authenticator from the SAML Authenticator drop-down menu on each View Connection Server, and click OK.

Dashboard
When you create a valid SAML 2.0 Authenticator, the dashboard on the View Administrator displays the authenticator’s health. You can select Dashboard on the Inventory or select System Health > Other components > SAML 2.0 Authenticators.

![System Health Directory]

Selecting the SAML 2.0 Authenticator from the Dashboard displays a health authenticator panel. If there are no problems, the authenticator’s health is green, as shown in the following window:

![Health Authenticator Window Displays Green – No Problems Detected]
If there are issues, the health is shown as red. In the next window, the Status field indicates that there is an untrusted certificate. When you validate and accept the certificate, the health status becomes green.

An authenticator’s health can also display red if Horizon Gateway is not available or if there is an error in the metadata URL.

**Authentication in Horizon Workspace**

SAML 2.0 enables SSO from Horizon Workspace to a Horizon View desktop without requiring re-authentication from users who have logged in using their AD credentials.

If a user authenticates to Horizon Workspace without presenting AD credentials—for instance, by using SecurID or Kerberos—SSO is not possible, and the user must provide credentials on the Horizon View desktop.

Horizon Workspace supports Horizon View desktops on desktops, laptops and iPads; however, it does not support SSO on iPads.
Extended Functionality

Horizon Workspace supports Horizon View deployments that use View Security Servers and load balancing. Make sure that every View Connection Server in the Horizon View pod that requires SAML 2.0 authentication has an authenticator configured.

Both self-signed and third-party-signed SSL certificates are supported, but self-signed certificates are not recommended.

To set up separate distribution for Intranet and Internet traffic, you can add a relevant FQDN for client access information for each Horizon Connector on its View Pool Details page.

Horizon Workspace supports multiple Horizon Connectors. When you integrate Horizon Workspace with Horizon View in a multiconnector environment, configure Horizon View pool information on all Horizon Connectors. To avoid redundant write operations to the Horizon database, perform a Horizon View pool sync operation on any one Horizon Connector but not on all of them.

Horizon Workspace supports Horizon View users from multiple domains if there is trust among the domains.

Figure 22: Traffic Distribution Overview
For Horizon View integration to work in a multidomain environment, verify the following items:

- Horizon Workspace and all the View Connection Servers must be joined to the same domain.

- Directory Server host information on the Horizon Connector Directory page must match the Active Directory server host information for the View Connection Servers. This Directory Server should also be a Global Catalog Server in your domain. Do not specify parent or sibling domain controller information.

- Global Catalog information on the Horizon Connector Directory page allows users from sub-domains and sibling domains to access Horizon Workspace and Horizon View desktops. Specify the Global Catalog port in the Server Port field (the default is 3268), and leave the Base DN field blank to allow searching across multiple trusted domains.

- Users and groups from other trusted domains must be synchronized.

Figure 23: Specify Global Catalog Server and Port on the Directory Page
Troubleshooting and Tips

The following information can be useful for debugging and resolving various issues:

- Configure all View Connection Servers, including load balancers, on the default HTTPS port (443).
- Create Horizon View pools as a user with administrator permissions on the root folder in the View Administrator Console. If you try to create pools without administrator permissions on the root folder, Horizon Workspace cannot recognize the SAML 2.0 Authenticator you configured in View Administrator, and you cannot sync the Horizon View pool in Horizon Workspace.
- You must install a View Client on the user device that launches Horizon Workspace if you want to use RDP/PCoIP to launch Horizon View desktops.
- Horizon Workspace does not support View Connection Server tags or Terminal Services pools.
- Whenever a Horizon View pool sync operation is performed, the Horizon Connector fetches Horizon View deployment-related information, including updates from the View Active Directory Application Module (ADAM), and stores it in the Horizon database.
- Horizon Workspace cannot make changes to Horizon View pools or the Horizon View environment. If a View administrator makes changes to Horizon View pool, a Horizon administrator must implement a Horizon View pool sync operation from Horizon Workspace to propagate the changes to Horizon Workspace. If a new user or group is added to Horizon View entitlements, the Horizon administrator must sync those users and groups before the Horizon View pools information can be synchronized.
- All View Connection Servers that are in a disabled state are removed from Horizon Workspace on the next sync operation. The sync completes successfully if there is at least one View Connection Server available in the Horizon View environment. Newly added replicated Connection Servers are registered with Horizon Workspace on the next sync.
- Accept Horizon View SSL certificates explicitly to validate that they have been fetched successfully. Horizon View pool synchronization fails if any of the SSL certificates fail to get validated during a sync operation.
- Maintain SSL trust between the Horizon Workspace and the View Connection Servers at all times. If you change an SSL certificate on the View Connection Server after integration, you must return to the Horizon Connector and re-accept the SSL certificate. If the Horizon Workspace certificate changes after the initial configuration, you must re-accept the SAML 2.0 Authenticator information from Horizon View.
- Horizon does not sync pools that are in maintenance mode or that have no entitlements. If a Horizon View pool has user or group entitlements, and the Horizon View pool does not sync, ensure that the user or group is synchronized (directory sync) before performing the Horizon View pool sync operation.
- Horizon performs sync operations from the primary View Connection Server specified under Initial Connection Server on the View Pools page on the Horizon Workspace Connector. If this server is not available, Horizon continues to perform the sync operation from the next available replicated View Connection Server.
- Horizon does not sync information about the number of Horizon View desktops in a pool, so addition or removal of Horizon View desktops from pools does not require a sync operation. Addition or removal of a pool, however, does require a sync operation.
- In Horizon Connector, the FQDN for Client Access should point to the View Connection Server where the SAML 2.0 Authenticator is set. If a load balancer is being used, the FQDN for Client Access should point to the load balancer. All View Connection Servers behind this load balancer should be configured to the same SAML 2.0 Authenticator.
- If SSO to Horizon View desktops is not working, verify that the SSO option is enabled on the Horizon Workspace Connector Web interface View Pools page and that you have logged into Horizon Workspace using AD credentials.
• Horizon Workspace and Horizon View must sync time from the same NTP server. Differences in time can lead to rejection of SAML requests when you try to launch a Horizon View desktop. Check the Horizon vApp current time and relative drift information from:

https://<Configurator FQDN>/cfg/system

• For log file locations, see:

  - Horizon Connector log
    /opt/vmware/c2/c2instance/logs/connector.log
    Look at this log file if you cannot save a Horizon View configuration in Horizon Workspace. The log contains a record of each request received from the Horizon Workspace client interface, including the request URL, timestamp, and exceptions. No sync actions are recorded.

  - Horizon Manager (Service) log
    /opt/vmware/horizon/horizoninstance/logs/horizon.log
    Check this log for details if Horizon Workspace saves Horizon View pool information but cannot sync or store Horizon View information in the Horizon database. This log also provides information about unsuccessful Horizon View desktop launches and activity on the Horizon Manager virtual appliance, such as entitlements, users, and groups.

  - View Connection Server log
    Application Data\VMware\VDM\logs
    Look at this log file to check detailed error messages and for information about Horizon View desktop launch failures.

• For failed Horizon View desktop launches from the Horizon Portal, check the View Connection Server log. Use the debug log level for more detailed information. For user login issues, search the logs for SamlAuthFilter or ProperoAuthFilter. For other integration issues, search the log for SamlSOAP, SamlUtil, SamlIdentity, and SamlHttpUtil. Common issues include:

  - Clocks must be synched between View Connection Servers and Horizon Workspace vApp.
    Example log errors include:
    
    **Assertion XXX is not valid before ...**
    
    **Assertion XXX is no longer valid.**
    
    **... Too late by x milliseconds ...**

  - Horizon Workspace cannot retrieve Horizon View metadata.
    Ensure that Horizon Connector has accepted and saved the View Connection Server certificates.
    The following is an example log error:
    
    **Error sending artifact resolve SOAP message to ...**

  - Horizon View cannot connect to Horizon Service.
    Ensure the View Administration dashboard shows a healthy SAML 2.0 Authenticator.
The following is an example log error:

Error sending artifact resolve SOAP message to ...

- Using HTTP instead of HTTPS to log in to the Horizon Workspace end-user client.

Access the Horizon Workspace end-user client from:

https://<your horizon gateway>/

The following is an example log error:

Source ID hash from artifact does not match hash of entityId

• Microsoft does not recommend the use of disjoint namespaces in the domain, and their use may prevent working with Kerberos. Horizon Workspace uses Kerberos to launch Horizon View desktops.

Conclusion

As is often the case, improving user experience requires some extra setup and verification. This paper provides Horizon administrators with detailed instructions for implementing single sign-on functionality so that end users can launch Horizon View desktops directly from Horizon Workspace.
References

OASIS Security Assertion Markup Language (SAML) V2.0 Technical Overview
Security Assertion Markup Language (SAML2.0) – Code Project article
VMware Horizon View Installation
VMware Horizon Workspace Documentation
VMware Horizon Workspace URLs
VMware Horizon View Documentation
VMware Horizon Workspace Reviewer’s Guide
Disjoint Namespace – Microsoft TechNet article

About the Authors

Neena K. Razdan is a Senior Member of the Technical Staff in End-User Computing specializing in Horizon Manager quality engineering.

Dalbir Sehmbi is a Senior Member of the Technical Staff specializing in Horizon View quality engineering.

The authors wish to thank Peter Brown, Raviteg Sistla, David Snowdon, and Karen Zelenko for their help and encouragement.