VMware vRealize Operations for Horizon Security

vRealize Operations for Horizon 6.1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001738-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

VMware vRealize Operations for Horizon Security

1

VMware vRealize Operations for Horizon Security provides information about security in VMware vRealize™ Operations for Horizon®, including how to modify default ports for RMI services, change the default SSL/TLS configuration for servers and agents, and replace default self-signed certificates.

This information is intended for anyone who wants to implement vRealize Operations for Horizon.

Managing RMI Communication in vRealize Operations for Horizon 2

The vRealize Operations for Horizon components communicate by using Remote Method Invocation (RMI). The View adapter exposes RMI services that can be called by an external client. The View adapter acts as a server and the broker and desktop agents act as clients. You can change the default ports for these RMI services.

For detailed descriptions of the vRealize Operations for Horizon components, see the *VMware vRealize Operations for Horizon Installation* document.

This chapter includes the following topics:

RMI Services

The View adapter exposes the following RMI services.

RMI registry service — The broker and desktop agents initially connect to the RMI registry service and request the address of a specific RMI server. Because the RMI registry service is used only for lookup and no sensitive data is transmitted to it, it does not use an encrypted channel.

Desktop message server — The desktop agents connect to the desktop message server and use it to send desktop performance data to the View adapter. The desktop message server uses an SSL/TLS channel to encrypt the data that is sent from the desktop agents.

Broker message server — The broker agent connects to the broker message server and uses it for sending View inventory information to the View adapter. The broker message server uses an SSL/TLS channel to encrypt the data that is sent from the broker agent.

Certificate management server — The broker agent connects to the certificate management server during the certificate pairing process. The certificate management server does not use an encrypted channel. Certificates are encrypted by using the server key during the certificate pairing process. For information, see "Certificate Pairing," on page 21.

Default Ports for RMI Services

The RMI services use certain default ports. The default ports are left open on the firewall on cluster nodes and remote collector nodes.

Table 2-1. Default Ports for RMI Services

RMI Service	Default Port
RMI registry	3091
Desktop message server	3092
Broker message server	3093
Certificate management server	3094

Changing the Default RMI Service Ports

You can change the default ports for the RMI registry service, desktop message server, broker message server, and certificate management server.

RMI Service Port Properties

The RMI service ports are defined in properties in the `msgserver.properties` file on the server where the View adapter is running.

Table 2-2. RMI Service Port Properties

RMI Service	Property
RMI registry	registry-port
Desktop message server	desktop-port
Broker message server	broker-port
Certificate management server	certificate-port

Change the Default RMI Service Ports

You can change the default RMI service ports by modifying the `msgserver.properties` file on the server where the View adapter is running.

Prerequisites

- Verify that you can connect to the node where the View adapter is running.
- Become familiar with the RMI service port properties. See "RMI Service Port Properties," on page 8.

Procedure

1 Log in to the node where the View adapter is running.

2 In a text editor, open the `msgserver.properties` file.

Platform	File Location
Linux	`/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work/msgserver.properties`
Windows	`C:\vmware\vcenter-operations\user\plugins\inbound\V4V_adapter3\work\msgserver.properties`

3 Modify the properties for the RMI service ports that you want to change.

4 Save your changes and close the `msgserver.properties` file.

What to do next

Open the new RMI service port or ports on the vRealize Operations Manager firewall. See "Update the vRealize Operations Manager Firewall," on page 9.

Update the vRealize Operations Manager Firewall

If you change the default port for an RMI service, you must open the new port on the vRealize Operations Manager firewall.

NOTE If the View adapter is running on a remote collector, see the documentation for the firewall on the remote collector node for information about updating the firewall.

Procedure

1 On the cluster node where the View adapter is running, use a text editor to open the `vmware-vcops-firewall.conf` file.

The `vmware-vcops-firewall.conf` file is in the `/opt/vmware/etc/` directory.

2 Update the appropriate ports in the `vmware-vcops-firewall.conf` file and save the file.

3 Restart the firewall service to make your changes take effect.

```
service vcopsfirewall restart
```

RMI Considerations for View 5.0 and 5.1 Environments

View 5.2 and later releases provide tighter integration with vRealize Operations for Horizon than View 5.1 and earlier releases, including features that enable the broker agent to send configuration data to remote desktops. This configuration enables the broker agent to send information that the desktop agent needs to perform authentication.

If you use vRealize Operations for Horizon to monitor a View 5.0 or 5.1 environment, you must disable RMI authentication in the View adapter. You typically disable RMI authentication for the View adapter when you initially install and configure vRealize Operations for Horizon.

For information about disabling RMI authentication for the View adapter, see the *VMware vRealize Operations for Horizon Installation* document.

RMI Considerations for Remote Collector Use

vRealize Operations Manager can use remote collectors to improve performance and scalability in environments that have multiple data centers. A remote collector can be installed on Windows or Linux and can host one or more adapter instances. This configuration enables data collection to be distributed across multiple datacenters.

The use of remote collectors has several serious security implications.

- To connect the remote collector to vRealize Operations Manager, you must publically expose the RMI interface of vRealize Operations Manager. No authentication is performed on connections to this interface. An attacker can use this interface to retrieve arbitrary data, send rogue data, and potentially take control of vRealize Operations Manager.
- The connection between the remote collector and vRealize Operations Manager is not encrypted. An attacker can sniff the network and gain access to data sent from a View adapter instance to vRealize Operations Manager.
- Configuration data that is sent from vRealize Operations Manager to the adapter instances on the remote collector is not encrypted. An attacker can sniff the network to gain access to the configuration information for any View adapter instance on the remote collector. This vulnerability includes, but is not limited to, the vRealize Operations for Horizon server key as well as vCenter Server credentials that the VMware adapter uses.

Changing the Default SSL/TLS Configuration in vRealize Operations for Horizon

3

The vRealize Operations for Horizon broker message server uses an SSL/TLS channel to communicate with the broker agents. The vRealize Operations for Horizon desktop message server uses an SSL/TLS channel to communicate with the desktop agents. You can change the default SSL/TLS configuration for servers and agents by modifying SSL/TLS configuration properties.

This chapter includes the following topics:

Default SSL/TLS Protocols and Ciphers

When an RMI connection is established between an agent and a server, the agent and server negotiate the protocol and cipher to use.

Each agent and server has a list of protocols and ciphers that it supports. The strongest protocol and cipher that is common to both the agent list and server list is selected for the SSL/TLS channel.

By default, RMI agents and servers are configured to accept only TLSv1 connections with the following ciphers:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA

SSL/TLS Configuration Properties

The SSL/TLS protocols and ciphers for the desktop and broker message servers are specified in properties in the `msgserver.properties` file. The SSL/TLS protocols and ciphers for the desktop and broker agents are specified in properties in the `msgclient.properties` file.

Table 3-1. SSL/TLS Configuration Properties

Property		Default Value
sslProtocols	List of accepted SSL/TLS protocols, separated by commas.	TLSv1
sslCiphers	List of accepted SSL/TLS ciphers, separated by commas.	TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA

Change the Default SSL/TLS Configuration for Servers

You can change the default SSL/TLS configuration that the desktop message server and broker message server use by modifying the `msgserver.properties` file on the server where the View adapter is running.

Prerequisites

- Verify that you can connect to the node where the View adapter is running.
- Become familiar with the SSL/TLS configuration properties. See "SSL/TLS Configuration Properties," on page 12.

Procedure

1 Log in to the node where the View adapter is running.

2 In a text editor, open the `msgserver.properties` file.

Platform	File Location
Linux	`/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work/msgserver.properties`
Windows	`C:\vmware\vcenter-operations\user\plugins\inbound\V4V_adapter3\work\msgserver.properties`

3 Modify the SSL/TLS configuration properties.

4 Save your changes and close the `msgserver.properties` file.

Change the Default SSL/TLS Configuration for Agents

You can change the SSL/TLS configuration that the desktop and broker agents use to connect to the desktop and broker message servers by modifying the `msgclient.properties` file.

For desktop agents, you modify the `msgclient.properties` file on the desktop virtual machine or RDS server where View Agent is running. For a broker agent, you modify the `msgclient.properties` file on the View Connection server host where the broker agent is installed.

Prerequisites

- For the desktop agents, verify that you can connect to the remote desktop virtual machine or RDS host where View Agent is installed.

- For a broker agent, verify that you can connect to the View Connection Server host where the broker agent is installed.
- Become familiar with the SSL/TLS configuration properties. See "SSL/TLS Configuration Properties," on page 12.

Procedure

1 Modify the SSL/TLS configuration properties for a desktop agent.

   a Log in to the remote desktop virtual machine or RDS host where View Agent is running.

   b In a text editor, open the `msgclient.properties` file.

   The `msgclient.properties` file is in the `C:\ProgramData\VMware\vCenter Operations for View\conf` directory.

   c Modify the SSL/TLS configuration properties.

   d Save your changes and close the `msgclient.properties` file.

2 Modify the SSL/TLS configuration properties for a broker agent.

   a Log in to the View Connection Server host where the broker agent is installed.

   b In a text editor, open the `msgclient.properties` file.

   The `msgclient.properties` file is in the `C:\ProgramData\VMware\vCenter Operations for View\conf` directory.

   c Modify the SSL/TLS configuration properties.

   d Save your changes and close the `msgclient.properties` file.

Managing Authentication in vRealize Operations for Horizon 4

RMI servers provide a certificate that the agents use to authenticate the View adapter. Broker agents use SSL/TLS client authentication with a certificate that the View adapter uses to authenticate the broker agents. Desktop agents provide tokens that the View adapter uses to authenticate the desktop agents.

To increase security, you can replace the default self-signed certificates that the View adapter and broker agents use. You can also reissue desktop authentication tokens.

This chapter includes the following topics:

Understanding Authentication for Each Component

Each vRealize Operations for Horizon component handles authentication differently.

View Adapter Authentication

When an RMI connection is established between the desktop message server and a desktop agent, or between the broker message server and a broker agent, the agent requests a certificate from the server to perform authentication. This certificate is validated against the agent's trust store before proceeding with the connection. If the server does not provide a certificate, or the server certificate cannot be validated, the connection is rejected.

When the View adapter is first installed, a self-signed certificate is generated. The desktop message server and broker message server use this self-signed certificate by default to authenticate to their agents. Because this certificate is generated dynamically, you must manually pair the View adapter and broker agent before the agents can communicate with the View adapter. For more information, see "Certificate Pairing," on page 21.

Broker Agent Authentication

When an RMI connection is established to the broker message server, the broker message server requests a certificate from the client to perform client authentication. The certificate is validated against the View adapter's trust store before proceeding with the connection. If the client does not provide a certificate, or the agent's certificate cannot be validated, the connection is rejected.

When the broker agent is first installed, a self-signed certificate is generated. The broker agent uses this self-signed certificate by default to authenticate to the View adapter. Because this certificate is generated dynamically, you must manually pair the View adapter and broker agent before the broker agent can communicate with the View adapter. For more information, see "Certificate Pairing," on page 21.

Desktop Agent Authentication

Connections to the desktop message server require an authentication token to verify that the connection is coming from a valid desktop agent. The broker agent generates a unique authentication token for each remote desktop and RDS host in a View pod.

After the broker agent generates an authentication token, the token is sent to the remote desktop or RDS host by using the View configuration store. The token is sent to the View adapter along with View inventory information.

When a desktop agent attempts to send data to the View adapter, the adapter uses its local cache to verify the authentication token that the remote desktop or RDS host sends. If the token does not match the adapter's local cache, an authentication failure occurs and the connection is rejected.

If an attacker gains access to an authentication token, you can revoke and reissue the token by using the vRealize Operations View Broker Agent Settings wizard. The wizard removes all existing authentication tokens from the adapter, generates new authentication tokens, and distributes the new tokens to all desktops in the View pod. See "Reissue View Desktop Authentication Tokens," on page 21.

Certificate and Trust Store Files

The vRealize Operations for Horizon components use a certificate trust store to store trusted certificates and root certificates for certificate authorities. Certificates and trust stores are stored in Java key store format.

View Adapter Certificate and Trust Store Files

The certificate and trust store files for the View adapter are in the adapter's `work` directory. These files are in Java key store format.

The `work` directory is on the node where the View adapter is installed. On Linux, the path to the `work` directory is `/usr/lib/vmwarevcops/user/plugins/inbound/V4V_adapter3/`. On Windows, the path to the `work` directory is `C:\vmware\vcenteroperations\user\plugins\inbound\V4V_adapter3\`.

You can use the Java `keytool` utility to view and control the certificate store and trust store files.

Table 4-1. Java Key Stores in the `work` Directory

Java Key Store	Description
`v4v-adapter.jks`	Contains the certificate that the adapter uses to authenticate itself to agents.
`v4v-truststore.jks`	Contains the trust store that the adapter uses to authenticate the broker agent certificate.

The names of the key store files and their credentials are defined in the `msgserver.properties` file, which is also in the `work` directory.

Table 4-2. Adapter Key Store Configuration Properties in the `msgserver.properties` File

Property	Default Value	Description
keyfile	`v4v-adapter.jks`	Name of the key store file that contains the adapter certificate.
keypass		Password to the key store file that contains the adapter certificate. The password is dynamically generated.
trustfile	`v4v-truststore.jks`	Name of the key store file that contains the adapter trust store.
trustpass		Password to the key store file that contains the adapter trust store. The password is dynamically generated.

Broker Agent Certificate and Trust Store Files

The broker agent certificate and trust store files are in the `C:\ProgramData\VMware\vCenter Operations for View\conf` directory on the View Connection Server host. These files are Java key store files.

You can use the Java `keytool` utility to view and control the certificate store and trust store files.

Table 4-3. Java Key Stores in the `conf` Directory

Java Key Store	Description
`v4v-brokeragent.jks`	Contains the certificate that the broker agent uses to authenticate itself to the View adapter.
`v4v-truststore.jks`	Contains the trust store that the broker agent uses to authenticate the View adapter certificate.

The names of the key store files and their credentials are defined in the `msgclient.properties` file, which is also in the `conf` directory.

Table 4-4. Broker Agent Key Store Configuration Properties in the `msgclient.properties` File

Property	Default Value	Description
keyfile	`v4v-brokeragent.jks`	The name of the key store file that contains the broker agent's certificate.
keypass		The password to the key store file that contains the broker agent's certificate. The password is dynamically generated.
trustfile	`v4v-truststore.jks`	The name of the key store file that contains the broker agent's trust store.
trustpass		The password to the key store file that contains the broker agent's trust store. The password is dynamically generated.

Replacing the Default Certificates

By default, the View adapter and the broker agent use self-signed certificates for authentication and data encryption. For increased security, you can replace the default self-signed certificates with certificates that are signed by a certificate authority.

Replace the Default Certificate for the View Adapter

A self-signed certificate is generated when you first install the View adapter. The desktop message server and the broker message server use this certificate by default to authenticate to the agents. You can replace the self-signed certificate with a certificate that is signed by a valid certificate authority.

Prerequisites

- Verify that you can connect to the node where the View adapter is running.
- Verify that you have the password for certificate store. You can obtain the password from the `msgserver.properties` file. See "View Adapter Certificate and Trust Store Files," on page 16.
- Become familiar with the Java `keytool` utility. Documentation is available at http://docs.oracle.com.

Procedure

1 Log in to the node where the View adapter is running.

2 Navigate to the View adapter's `work` directory.

Platform	Directory Location
Linux	`/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work`
Windows	`C:\vmware\vcenteroperations\user\plugins\inbound\V4V_adapter3\work`

3 Use the `keytool` utility with the `-selfcert` option to generate a new self-signed certificate for the View adapter.

Because the default self-signed certificate is issued to VMware, you must generate a new self-signed certificate before you can request a signed certificate. The signed certificate must be issued to your organization.

For example:

```
keytool -selfcert -alias v4v-adapter -dname dn-of-org -keystore v4v-adapter.jks
```

dn-of-org is the distinguished name of the organization to which the certificate is issued, for example, "OU=Management Platform, O=VMware, Inc., C=US".

By default, the certificate signature uses the SHA1withRSA algorithm. You can override this default by specifying the name of the algorithm with the `-sigalg` option.

4 Use the `keytool` utility with the `-certreq` option from the adapter `work` directory to generate a certificate signing request.

A certificate signing request is required to request a certificate from a certificate signing authority.

For example:

```
keytool -certreq -alias v4v-adapter -file certificate-request-file -keystore v4v-adapter.jks
```

certificate-request-file is the name of the file that will contain the certificate signing request.

5 Upload the certificate signing request to a certificate authority and request a signed certificate.

If the certificate authority requests a password for the certificate private key, use the password configured for the certificate store.

The certificate authority returns a signed certificate.

6 To import the certificate, copy the certificate file to the View adapter `work` directory and run the `keytool` utility with the `-import` option.

For example:

```
keytool -import -alias v4v-adapter -file certificate-filename -keystore v4v-adapter.jks
```

certificate-filename is the name of the certificate file from the certificate authority.

When the `keytool` utility is finished, the signed certificate is imported to the adapter certificate store.

7 To start using the new certificate, restart the View adapter on the node where the adapter is running.

Platform	Action
Linux	Run the `service vmware-vcops restart` command.
Windows	Use the Windows Services tool (`services.msc`) to restart the vRealize Operations View Adapter service.

What to do next

After you restart the View adapter, you must pair any broker agents that are attached to the View adapter. See "Certificate Pairing," on page 21.

Replace the Default Certificate for the Broker Agent

A self-signed certificate is generated when you first install the broker agent. The broker agent uses this certificate by default to authenticate to the View adapter. You can replace the self-signed certificate with a certificate that is signed by a valid certificate authority.

Prerequisites

- Verify that you can connect to the View Connection Server host where the broker agent is installed.
- Verify that the `keytool` utility is added to the system path on the View Connection Server host where the broker agent is installed.
- Verify that you have the password for the certificate store. You can obtain this password from the `msgserver.properties` file. See "Broker Agent Certificate and Trust Store Files," on page 17.
- Become familiar with the Java `keytool` utility. Documentation is available at http://docs.oracle.com.

Procedure

1 Log in to the View Connection Server host where the broker agent is installed.

2 Use the `keytool` utility with the `–selfcert` to generate a new self-signed certificate.

Because the default self-signed certificate is issued to VMware, you must generate a new self-signed certificate before you request a signed certificate. The signed certificate must be issued to your organization.

For example:

```
keytool -selfcert -alias v4v-brokeragent -dname dn-of-org -keystore v4v-brokeragent.jks
```

dn-of-org is the distinguished name of the organization to which the certificate is issued, for example, "OU=Management Platform, O=VMware, Inc. , C=US".

By default, the certificate signature uses the SHA1withRSA algorithm. You can override this default by specifying the name of the algorithm in the `keytool` utility.

3 Use the `keytool` utility with the `–certreq` option to generate the certificate signing request.

A certificate signing request is required to request a certificate from a certificate signing authority.

For example:

```
keytool -certreq -alias v4v-brokeragent -file certificate-request-file -keystore v4v-brokeragent.jks
```

certificate-request-file is the name of the file that will contain the certificate signing request.

4 Upload the certificate signing request to a certificate authority and request a signed certificate.

If the certificate authority requests a password for the certificate private key, use the password configured for the certificate store.

The certificate authority returns a signed certificate.

5 Copy the certificate file to the `conf` directory and run the `keytool` utility with the `–import` option to import the signed certificate into the certificate store for the broker agent.

You must import the certificate file to the certificate store for the broker agent so that the broker agent can start using the signed certificate.

For example:

```
keytool -import -alias v4v-brokeragent -file certificate-filename -keystore v4v-brokeragent.jks
```

certificate-filename is the name of the certificate file from the certificate authority.

6 Run the `keytool` utility with the `–import` option to import the certificate authority root certificate into the trust store file for the broker agent.

For example:

```
keytool -import -alias aliasname -file root_certificate -keystore v4v-truststore.jks -trustcacerts
```

root_certificate is the name of the certificate authority root certificate.

7 Restart the broker agent to start using the new certificate.

You can restart the broker agent by using the vRealize Operations View Broker Agent Settings wizard, or by restarting the vRealize Operations View Broker Agent Service.

What to do next

After you restart the broker agent, you must pair it with the View adapter. See "Certificate Pairing," on page 21.

Certificate Pairing

Before broker agents can communicate with the View adapter, the adapter certificate must be shared with the agents, and the broker agent certificate must be shared with the adapter. The process of sharing these certificates if referred to as certificate pairing.

The following actions occur during the certificate pairing process:

1 The broker agent's certificate is encrypted with the adapter's server key.

2 A connection is opened to the certificate management server and the encrypted certificate is passed to the adapter instance. The adapter decrypts the broker agent's certificate by using the server key. If decryption fails, an error is returned to the broker agent.

3 The broker agent's certificate is placed in the adapter's trust store.

4 The adapter's certificate is encrypted with the adapter's server key.

5 The encrypted certificate is returned to the broker agent. The broker agent decrypts the adapter's certificate by using the server key. If decryption fails, an error is returned to the user.

6 The adapter's certificate is placed in the broker agent's trust store.

7 The adapter's certificate is sent to all remote desktops and RDS hosts in the View pod by using the View configuration store.

8 When the agent on the remote desktop or RDS host reads the View configuration, it places the adapter's certificate in the agent's trust store.

After the certificates are successfully paired, they are cached in the trust stores for each individual component. If a new remote desktop is provisioned, the adapter's certificate is sent to the desktop by using the View configuration store, and you do not need to pair the certificates again. However, if either the adapter or broker agent certificate changes, you must pair the certificates again.

You use the vRealize Operations View Broker Agent Settings wizard to pair certificates. For more information, see the *VMware vRealize Operations for Horizon Administration* document.

Reissue View Desktop Authentication Tokens

If you believe that the security of your View environment might be compromised, you can issue a new authentication token for each desktop virtual machine and RDS host in your View environment.

Procedure

1 Log in to the View Connection Server host where you installed the broker agent with a domain user account.

Local accounts do not have the necessary privileges to configure broker agent settings.

2 From the **Start** menu, select **VMware > vRealize Operations View Broker Agent Settings**.

3 In the **Security** section of the vRealize Operations View Broker Agent Settings dialog box, click **Re-issue Desktop Tokens**.

4 When the operation is finished, click **Close**.

5 Click **Close** again to exit the vRealize Operations View Broker Agent Settings dialog box.

The configuration change might take several minutes to propagate to the View adapter and all of the desktop agents in your View environment.

SSL/TLS and Authentication-Related Log Messages

The View adapter logs SSL/TLS configuration and authentication-related messages.

Table 4-5. View Adapter Log Message Types

Log Message Type	Description
CONFIGURATION	The SSL/TLS configuration this currently being used.
AUTHENTICATION SUCCESS	A remote desktop has been successfully authenticated.
AUTHENTICATION FAILED	A remote desktop has failed authentication.

Only CONFIGURATION and AUTHENTICATION FAILED events are written to the log by default. To troubleshoot problems, you can raise the logging level to log other types of events.

You can view log messages and modify logging levels in the vRealize Operations Manager user interface. For more information, see the *VMware vRealize Operations for Horizon Administration* document.

Index