VMware vRealize Operations for Horizon Security

20 SEP 2018

VMware vRealize Operations for Horizon 6.6

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

https://docs.vmware.com/

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 discusses how to modify the default RMI ports and TLS configuration and how to replace the default self-signed certificates.

Intended Audience

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

RMI Communication in vRealize Operations for Horizon

2

The vRealize Operations for Horizon components communicate by using Remote Method Invocation (RMI). The Horizon Adapter exposes RMI services that can be called by external clients. The adapter acts as a server and the broker and desktop agents act as clients.

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

This chapter includes the following topics:

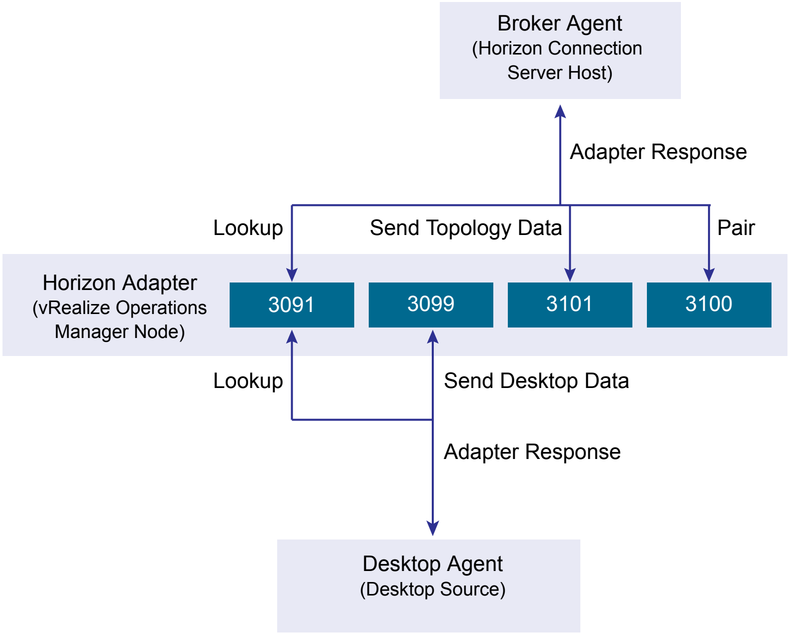
RMI Services

The Horizon Adapter exposes the RMI registry service, desktop and broker message servers, and certificate management server.

Table 2-1. RMI Services

Service	Description	Default Port
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.	3091
Desktop message server	The desktop agents connect to the desktop message server and use it to send desktop performance data to the Horizon Adapter. The desktop message server uses a TLS channel to encrypt the data that is sent from the desktop agents.	3099
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 more information, see Certificate Pairing.	3100
Broker message server	The broker agents connect to the broker message server and use it to send Horizon inventory information to the Horizon Adapter. The broker message server uses a TLS channel to encrypt the data that is sent from the broker agent.	3101

Figure 2-1. Communication Through RMI Service Ports



Note In vRealize Operations for Horizon 6.1 and earlier, the desktop message server, broker message server, and certificate management server use ports 3092, 3093, and 3094, respectively. Ports 3091 through 3101 are open by default in the vRealize Operations Manager firewall to maintain backward compatibility.

RMI Security with Remote Collectors

vRealize Operations Manager can use remote collectors to distribute data collection across multiple data centers. However, the use of remote collectors has several security implications.

To connect the remote collector to vRealize Operations Manager, you must publicly expose the RMI interface of vRealize Operations Manager. No authentication is performed on connections to this interface. An attacker can exploit this interface to retrieve data, send rogue data, and potentially take control of vRealize Operations Manager.

In addition, the connection between the remote collector and vRealize Operations Manager is not encrypted. An attacker can potentially gain access to data sent from a Horizon Adapter instance to vRealize Operations Manager. This data includes configuration information for any Horizon Adapter instance on the collector, the server key, and the vCenter Server that the adapter uses.

Change 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.

The RMI service ports are defined in the `msgserver.properties` file on the vRealize Operations Manager node where the Horizon Adapter instance is running. You can modify the value of the corresponding properties to change the RMI service ports.

Table 2-2. RMI Service Port Properties

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

Procedure

1. Open the `/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work/msgserver.properties` file on the node where the Horizon Adapter instance is running.
2. Modify the values of the properties corresponding to the RMI service ports that you want to change.
3. Open the `/opt/vmware/etc/vmware-vcops-firewall.conf` file and locate the following command:

   ```
   # V4V Adapter specific ports
   TCPPORTS="$TCPPORTS 3091:3101"
   ```

4. Change `3091:3101` to the ports or port range that you specified in the `msgserver.properties` file.
5. Restart the firewall.

   ```
   /etc/init.d/vmware-vcops-firewall restart
   ```

TLS Configuration in vRealize Operations for Horizon

3

The vRealize Operations for Horizon broker message server and desktop message server each use a TLS channel to communicate with agents. You can change the default TLS configuration for servers and agents to meet your security needs.

This chapter includes the following topics:

TLS Configuration Properties

You can change the TLS versions and ciphers used to encrypt communication between servers and agents.

Each agent and server supports a certain set of protocol versions 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 by selecting the strongest protocol and cipher that both ends support.

The supported versions and ciphers for desktop and broker message servers are specified in the `msgserver.properties` file on the vRealize Operations Manager node where the adapter instance is running. The supported versions and ciphers for broker agents are specified in the `msgclient.properties` on the Horizon Connection Server host where the agent is installed. The supported versions and ciphers for desktop agents are specified in the `msgclient.properties` file on the corresponding desktop source or RDS host.

Table 3-1. TLS Configuration Properties

Property	Description	Default Value
`sslProtocols`	List of accepted TLS versions, separated by commas.	`TLSv1.2`

`sslCiphers`	List of accepted TLS ciphers, separated by commas.	`TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,`
		`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,`
		`TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,`
		`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`

Change the Default TLS Configuration

You can change the default TLS configuration that vRealize Operations for Horizon components use by modifying the `msgserver.properties` and `msgclient.properties` files.

Procedure

1 Log in to the vRealize Operations Manager node where the Horizon Adapter instance is running and open the `/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work/msgserver.properties` file.

2 Modify the value of the `sslProtocols` and `sslCiphers` properties as desired.

3 Log in to the Horizon Connection Server host where the broker agent is running and open the `C:\ProgramData\VMware\vRealize Operations for Horizon\Broker Agent\conf\msgclient.properties` file.

4 Modify the value of the `sslProtocols` and `sslCiphers` properties to match the Horizon Adapter.

5 Log in to the desktop source where the desktop agent is running and open the `C:\ProgramData\VMware\vRealize Operations for Horizon\Desktop Agent\conf\msgclient.properties` file.

6 Modify the value of the `sslProtocols` and `sslCiphers` properties to match the Horizon Adapter.

Authentication in vRealize Operations for Horizon 4

The broker and desktop message servers on the Horizon Adapter use certificates to authenticate themselves to agents. The broker agent uses a certificate to authenticate itself to the broker message server, and the desktop agent uses authentication tokens to authenticate itself to the desktop message server.

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

This chapter includes the following topics:

Certificate Pairing

Horizon Adapter instances and broker agents must share certificates with each other before they can communicate. This process is called pairing.

Upon installation, Horizon Adapter instances and broker agents generate self-signed certificates that are used by default for authentication. Because these certificates are generated dynamically, you must manually pair the Horizon Adapter instance and broker agent.

The certificate pairing process is as follows:

1. The broker agent encrypts its certificate with the server key configured for the adapter instance.
2. The broker agent opens a connection to the certificate management server, and the encrypted certificate is sent to the adapter instance.
3. The adapter decrypts the broker agent certificate by using the server key. If decryption fails, an error is returned to the broker agent and the process is discontinued.
4. The adapter instance places the valid broker agent certificate in its trust store.

5 The adapter instance encrypts its own certificate with the server key configured for the instance.

6 The adapter instance sends the encrypted certificate to the broker agent.

7 The broker agent decrypts the adapter instance certificate by using the server key. If decryption fails, an error is returned to the user and the process is discontinued.

8 The broker agent places the adapter instance certificate in its trust store.

9 The adapter instance certificate is sent to all desktop sources and RDS hosts in the Horizon pod.

10 The desktop agents on those desktop sources place the adapter instance certificate in their trust stores.

Note If the certificate used by the adapter instance or broker agent changes, you must pair the adapter instance and broker agent again.

Component Authentication

The various components of vRealize Operations for Horizon use certificates and tokens to perform authentication.

When an RMI connection is established between a message server and an agent, the agent requests a certificate from the server to perform authentication. The agent validates this certificate against its trust store before proceeding with the connection. If the server does not provide a certificate, or the server certificate cannot be validated, the agent rejects the connection.

The broker message server also requests a certificate from broker agents that it validates against its trust store. If the agent does not provide a certificate, or the agent certificate cannot be validated, the server rejects the connection.

Desktop agents generate a unique authentication token for each remote desktop and a server ID for the local Horizon server. They then send the server ID to vRealize Operations Manager.

Desktop agents include the authentication token and server ID when they attempt to send data to the Horizon Adapter. The adapter instance compares the authentication token with the one stored in its memory and rejects the communication attempt if they do not match. If the token does not exist on the adapter instance, it caches the token in memory. It then checks whether a virtual machine with the specified server ID exists in vRealize Operations Manager and adds the virtual machine to the topology if so.

Certificate and Trust Store Files

The vRealize Operations for Horizon components store certificates in Java keystore format.

You can use the Java `keytool` utility to view and control these files.

Horizon Adapter

Certificate and trust store files for the Horizon Adapter are located in the /usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work directory on the vRealize Operations Manager node where the adapter instance is running. The names and passwords of these files are defined in the msgserver.properties file in the same directory.

Table 4-1. Adapter Certificate Properties

Property	Default Value	Description
keyfile	v4v-adapter.jks	Certificate that the adapter uses to authenticate itself to agents.
keypass		Password to the keystore file specified in the keyfile property. The password is dynamically generated.
trustfile	v4v-truststore.jks	Trust store that the adapter uses to authenticate broker agent certificates.
trustpass		Password to the keystore file specified in the trustfile property. The password is dynamically generated.

Broker Agent

Certificate and trust store files for the broker agent are located in the C:\ProgramData\VMware\vRealize Operations for Horizon\Broker Agent\conf directory on the Horizon Connection Server host where the agent is running. The names and passwords of these files are defined in the msgclient.properties file in the same directory.

Table 4-2. Broker Agent Certificate Properties

Property	Default Value	Description
keyfile	v4v-brokeragent.jks	Certificate that the broker agent uses to authenticate itself to the Horizon Adapter.
keypass		Password to the keystore file specified in the keyfile property. The password is dynamically generated.
trustfile	v4v-truststore.jks	Trust store that the broker agent uses to authenticate adapter instance certificates.
trustpass		Password to the keystore file specified in the trustfile property. The password is dynamically generated.

Replacing the Default Certificates

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

Replace the Default Certificate for the Horizon Adapter

Broker and desktop message servers use a self-signed certificate generated by the Horizon Adapter for authentication with agents. You can replace this self-signed certificate with a certificate that is signed by a valid certificate authority.

Prerequisites

- Obtain the keystore passwords from the `msgserver.properties` file on the vRealize Operations Manager node where the adapter instance is running.
- Become familiar with the Java `keytool` utility. For related documentation, visit the Oracle Help Center at http://docs.oracle.com.

Procedure

1 Log in to the vRealize Operations Manager node where the adapter instance is running and open the `/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work` directory.

2 Run the `keytool` utility with the `-genkeypair` option to generate a new self-signed certificate for the Horizon 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.

```
keytool -genkeypair -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".

3 Run the `keytool` utility with the `-certreq` option to generate a certificate signing request.

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

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.

5 After the certificate authority returns a signed certificate, copy the certificate file to the `/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work` directory.

6 Run the `keytool` utility with the `-import` option to import the new certificate.

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

7 Restart the Horizon Adapter service.

```
service vmware-vcops restart
```

The broker and desktop message servers on the adapter instance now use the signed certificate that you imported.

8 Pair broker agents with the adapter instance again.

a Log in to the Horizon Connection Server host where the broker agent is installed using a domain account that is part of the local administrators group.

b Select **Start > VMware > vRealize Operations for Horizon Broker Agent Settings**.

c Confirm the port and server key and click **Pair**.

d Click **Next** until the **Ready To Complete** page is displayed and click **Finish**.

Replace the Default Certificate for the Broker Agent

Broker agents use a self-signed certificate by default for authentication with the Horizon Adapter. You can replace this self-signed certificate with a certificate that is signed by a valid certificate authority.

Prerequisites

- Obtain the keystore passwords from the `msgclient.properties` file on the vRealize Operations Manager node where the adapter instance is running.
- Become familiar with the Java `keytool` utility. For related documentation, visit the Oracle Help Center at http://docs.oracle.com.
- Add the `keytool` utility to the system path on the host where the broker agent is installed.

Procedure

1 Log in to the Horizon Connection Server host where the broker agent is installed and open the `C:\ProgramData\VMware\vRealize Operations for Horizon\Broker Agent\conf` directory.

2 Run the `keytool` utility with the `-genkeypair` option to generate a new self-signed certificate for the broker agent.

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.

```
keytool -genkeypair -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".

3 Run the `keytool` utility with the `-certreq` option to generate a certificate signing request.

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

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.

5. After the certificate authority returns a signed certificate, copy the certificate file to the `C:\ProgramData\VMware\vRealize Operations for Horizon\Broker Agent\conf` directory.

6. Run the `keytool` utility with the `-import` option to import the new certificate.

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

7. Run the `keytool` utility with the `-import` option again to import the root certificate of the certificate authority.

   ```
   keytool -import -alias alias-name -file root-cert-name -keystore v4v-truststore.jks -trustcacerts
   ```

8. Restart the broker agent service.

   a. Select **Start > VMware > vRealize Operations for Horizon Broker Agent Settings**.

   b. Click **Next** until the **Broker Agent Service** page is displayed and then click **Restart**.

   The broker agent now uses the signed certificate that you imported.

9. Pair the broker agent with the adapter instance again.

   a. Click **Back** until the **Pair Adapter** page is displayed.

   b. Confirm the port and server key and click **Pair**.

   c. Click **Next** until the **Ready To Complete** page is displayed and click **Finish**.

Reissue Horizon Desktop Authentication Tokens

If you believe that the security of your Horizon environment might be compromised, you can issue a new authentication token for each desktop virtual machine and RDS host in your Horizon environment by restarting the broker agent service. By default, a new authentication token for each desktop virtual machine and RDS host is issued every hour.

TLS and Authentication-Related Log Messages

The Horizon Adapter logs various messages related to TLS configuration and authentication.

Table 4-3. Log Message Types

Log Message Type	Description
`CONFIGURATION`	TLS configuration in use
`AUTHENTICATION SUCCESS`	Successful authentication of a remote desktop
`AUTHENTICATION FAILED`	Failed authentication of a remote desktop

Only `CONFIGURATION` and `AUTHENTICATION FAILED` events are written to the log by default. If you want to log other types of events, you can change the logging level.

For more information, see "Viewing Horizon Adapter Log Files" and "Modify the Logging Level for the Horizon Adapter" in *VMware vRealize Operations for Horizon Administration*.