Security Guide

vCenter Operations Manager for Horizon View 1.5

TECHNICAL WHITE PAPER

Contents

Introduction

The *VMware vCenter Operations Manager for Horizon View Security Guide* provides information about security in VMware® vCenter™ Operations Manager for Horizon View™. Topics include the product surface area, authentication mechanisms, and options for configuration and management of security features.

This information is intended for anyone who wants to implement vCenter Operations Manager for Horizon View.

Surface Area

vCenter Operations Manager for Horizon View consists of three major components:

- An adapter, which is installed on the vCenter Operations Manager vApp or on a remote collector. The adapter is responsible for collecting data from the agents and sending it to vCenter Operations Manager.
- A broker agent, which is installed on a Horizon View Connection server. The broker agent is responsible for collecting Horizon View™ inventory information and sending it to the adapter.
- Desktop agents, which are installed on each Horizon View desktop. The desktop agent is responsible for collecting desktop performance data and sending it to the adapter.

Both the desktop and broker agents establish outbound connections to the adapter. There are no inbound connections made to either the broker or desktop agent. The adapter listens for inbound connections from the agents. There are no outbound connections made by the adapter.

All components of vCenter Operations Manager for Horizon View communicate by using RMI. The adapter acts as a server and the agents act as clients. The adapter exposes the following RMI services that can be called by an external client:

- *RMI registry* (port 3091 by default). The agents initially connect to the RMI registry and request the address of a specific RMI server.
- *Desktop message server* (port 3092 by default). The desktop agents connect to this RMI server and uses it for sending desktop performance data to the adapter.
- *Broker message server* (port 3093 by default). The broker agent connects to this RMI server and uses it for sending Horizon View inventory information to the adapter.
- *Certificate management server* (port 3094 by default). The broker agent connects to this RMI server during the certificate pairing process. Certificate pairing is described in the *Certificate Management* section.

The *desktop message server* and *broker message server* both use an SSL channel to encrypt the data that is sent from the agents. The *RMI registry* does not use an encrypted channel, as it is only used for lookup and no sensitive data is transmitted to it. The *certificate management server* does not use an encrypted channel; however, certificates are encrypted using the server key during the certificate pairing process. Certificate pairing is described in the *Certificate Management* section.

The default ports used by these RMI services can be changed by modifying the *msgserver.properties* file on the server that the adapter is running on. Table 1 shows the location of this file for different versions of vCenter Operations Manager, and Table 2 shows the properties that correspond to the ports for each service.

Table 1: Location of msgserver.properties

Adapter Location	File Location
vCenter Operations Manager vApp	/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work on the Analytics VM
Windows Remote Collector	c:\vmware\vcenter-operations\user\plugins\inbound\V4V_adapter3\work
Linux Remote Collector	/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work

Table 2: Service port properties

Service	Property	Default Port
RMI Registry	registry-port	3091
Desktop message server	desktop-port	3092
Broker message server	broker-port	3093
Certificate Management Server	certificate-port	3094

If you change one or more of these ports, you might have to open the new ports through the firewall. To update the firewall on the vCenter Operations Manager vApp:

1. Open *vcopsfirewall.conf*, located in /usr/lib/vmware-vcops/user/conf/install on the Analytics VM.
2. Locate the section titled *v4v RMI* and update the ports that are specified.
3. Restart the firewall by running *service vcopsfirewall restart*.

To update the firewall on a remote collector, refer to the documentation for the specific firewall that is installed on the remote collector server.

SSL Configuration

The broker message server and desktop message server both use an SSL channel for communication with the agents. When an RMI connection is established between an agent and one of the servers, a negotiation of the protocol and cipher that will be used for the connection takes place. Both the agent and the server have a list of protocols and ciphers that they support, and between those lists, the strongest protocol and cipher will be chosen.

By default, the RMI servers and agents are configured to only accept SSLv3 or TLSv1 connections with the following ciphers:

- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- 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

The SSL configuration used by the RMI servers can be changed by modifying the *msgserver.properties* file on the server that the adapter is running on. See Table 1 for the location of this file.

The SSL configuration used by the agents to connect to the RMI servers can be changed by modifying the *msgclient.properties* file on the Horizon View server and desktop. This file is located in C:\ProgramData\VMware\vCenter Operations for View\conf. Table 3 contains descriptions of the SSL configuration properties.

Table 3: SSL configuration properties

Property	Description	Default Value
sslProtocols	List of accepted SSL protocols, separated by commas.	SSLv3,TLSv1
sslCiphers	List of accepted SSL ciphers, separated by commas.	SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, 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

Authentication

Authentication is handled differently for each component in vCenter Operations Manager for Horizon View. The RMI servers provide a certificate that the agents use to authenticate the adapter. The broker agent uses SSL client authentication with a certificate that the adapter uses to authenticate broker agents. The desktop agent provides a token that the adapter uses to authenticate desktop agents.

Adapter

When a connection is established to the *desktop message server* or *broker message server*, the agent requests a certificate from the server in order to perform authentication. The certificate is validated against the agent's trust store before proceeding with the connection. If a certificate is not provided by the server, or if the server's certificate cannot be validated, then the connection is rejected. See the *Certificate Management* section for information regarding how to manage the certificate and trust store used during authentication.

When the adapter is first installed, a self-signed certificate is generated that the *desktop message server* and *broker message server* use by default to authenticate to the agents. Because this certificate is generated dynamically, the adapter and broker agent must be "paired" before the agents can communicate with the adapter. Refer to the *Certificate Pairing* section below for a description of the pairing process.

Broker Agent

When a connection is established to the *broker message server*, the server requests a certificate from the client in order to perform client authentication. The certificate is validated against the adapter's trust store before proceeding with the connection. If a certificate is not provided by the client, or if the agent's certificate cannot be validated, then the connection is rejected. See the *Certificate Management* section for information regarding how to manage the certificate and trust store used during authentication.

When the broker agent is first installed, a self-signed certificate is generated that the broker agent uses by default to authenticate to the adapter. Because this certificate is generated dynamically, the adapter and broker agent must be "paired" before the broker agent can communicate with the adapter.

Certificate Pairing

Before the agents can communicate with the adapter, the adapter certificate must be shared with the agents, and the broker agent certificate must be shared with the adapter. This process is referred to as certificate pairing. Certificate pairing is initiated by clicking "Pair with View Adapter" in the "vCenter Operations for View Broker Agent Settings" tool. The user that initiates the pair must be a local Administrator on the Horizon View server, and must also be able to provide the adapter's server key.

Certificate pairing consists of the following steps:

1. The broker agent's certificate is encrypted using the server key given by the user during the adapter instance configuration.
2. A connection to the *certificate management server* is opened, and the encrypted certificate is passed to the adapter using this service.
3. The adapter decrypts the broker agent's certificate using the configured server key. If decryption fails, an error is returned to the broker agent.
4. The broker agent's certificate is placed into the adapter's trust store.
5. The adapter's certificate is encrypted using the configured server key.
6. The encrypted certificate is returned to the broker agent.

7. The broker agent decrypts the adapter’s certificate using the server key given by the user. If decryption fails, an error is returned to the user.
8. The adapter’s certificate is placed into the broker agent’s trust store.
9. The adapter’s certificate is sent to all desktops in the Horizon View pod using the Horizon View configuration store.
10. When the desktop agent reads the Horizon View configuration, it places the adapter’s certificate into the desktop agent’s trust store.

Once *certificate pairing* is complete, certificates are cached in the trust stores for each individual component, so there is no need to pair again. Additionally, if a new desktop is provisioned, the adapter’s certificate will automatically be sent to the desktop using the Horizon View configuration store. However, if either the adapter or broker agent certificate changes, it is necessary to pair again.

Desktop Agent

All connections to the *desktop message server* require an authentication token in order to authenticate that the connection is coming from a valid desktop agent. Unique authentication tokens are automatically generated by the broker agent for each desktop in the Horizon View pod. When the broker agent generates an authentication token, the token is sent to the desktop using the Horizon View configuration store, and is also sent to the adapter with other Horizon View inventory information.

When the desktop agent attempts to send data to the adapter, the adapter verifies the authentication token sent by that desktop with its local cache. If the token doesn’t match, then an authentication failure occurs and the connection is rejected.

In the event that an attacker gains access to an authentication token, tokens can be revoked and re-issued. To reissue tokens, click “Re-issue Desktop Authentication Tokens” in the “vCenter Operations for View Broker Agent Settings” tool. All existing authentication tokens will be removed from the adapter, and new authentication tokens will be generated and distributed to all desktops in the Horizon View pod.

Audit Log

The adapter writes out an audit log while it is running. To view the audit log:

1. Log on to the *vCenter Operations Manager Web Console*, located at https://<UI-VM>/vcops-custom/.
2. Open Admin->Support, and click Logs.
3. In the Logs list, expand the folder for the collector where the adapter instance is configured.
4. Expand adapters and V4VAdapter.
5. Click audit.log.

The following types of events can be found in the audit log:

- CONFIGURATION: The SSL configuration that is currently being used.
- AUTHENTICATION SUCCESS: A desktop has been successfully authenticated.
- AUTHENTICATION FAILED: A desktop has failed authentication.

By default, only CONFIGURATION and AUTHENTICATION FAILED events are written to the audit log. Other event types can be logged by raising the log level. To raise the log level, add the following line to *msgserver.properties*:

```
audit-log-level = INFO
```

Raising the log level greatly increases the number of events that are written to the audit log, which reduces the time that events are stored before being rolled over. Leaving the log level at INFO is not recommended.

Audit log files are automatically rolled over when they reach 10 MB in size. By default, 20 log files are kept at a time before the oldest log file is overwritten. To change the number of log files to keep, add the following line to *msgserver.properties*:

```
audit-log-maxbackups = <number of log files to keep>
```

Certificate Management

Both the adapter and the broker agent have certificates that are used for authentication and data encryption. Additionally, all components have a certificate trust store that is used for storing certificates that are trusted, as well as the root certificates for certificate authorities. Certificates and trust stores are stored in Java key store format.

Adapter

The adapter's certificate and trust store are located in the adapter's work directory. Table 4 shows the location of this directory for different versions of vCenter Operations Manager.

Table 4: Location of the adapter work directory

Adapter Location	Certificate Location
vCenter Operations Manager vApp	/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work on the Analytics VM
Windows Remote Collector	c:\vmware\vcenter-operations\user\plugins\inbound\V4V_adapter3\work
Linux Remote Collector	/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work

The work directory contains two Java key stores:

- *v4v-adapter.jks*, which contains the certificate used by the adapter to authenticate itself to agents.
- *v4v-truststore.jks*, which contains the trust store used by the adapter to authenticate the broker agent's certificate.

The credentials for these key store files are stored in the *msgserver.properties* file, also located in the work directory. Table 5 shows a list of the key store properties.

Table 5: Adapter key store configuration properties

Property	Description	Default Value
keyfile	The name of the key store file that contains the adapter's certificate.	v4v-adapter.jks
keypass	The password to the key store file that contains the adapter's certificate.	Dynamically generated
trustfile	The name of the key store file that contains the adapter's trust store.	v4v-truststore.jks
trustpass	The password to the key store file that contains the adapter's trust store.	Dynamically generated

Both the certificate store and trust store can be viewed and controlled using the Java `keytool` application. For information regarding using this tool, refer to http://docs.oracle.com/javase/1.4.2/docs/tooldocs/windows/keytool.html.

When the adapter is first installed, a self-signed certificate is generated that the *desktop message server* and *broker message server* use by default to authenticate to the agents. For increased security, a certificate signed by a valid certificate authority can be used instead. The process for generating and importing a signed certificate is as follows:

1. Create a new self-signed certificate for your organization.
2. Generate a certificate signing request.
3. Send the request to a certificate signing authority.
4. Import the certificate from the certificate signing authority into the certificate store.

These steps should be performed on the server that the adapter is running on. If the adapter is running on the vCenter Operations Manager vApp, this server will be the Analytics VM. If the adapter is running on a remote collector, this server will be the server where the remote collector is installed.

Important: If the certificate authority requests a password for the certificate's private key, the password configured for the certificate store must be used.

Creating a New Self-Signed Certificate

The default self-signed certificate is issued to VMware. If a new signed certificate is being requested, it is recommended that the new certificate be issued to the individual organization. As a result, a new self-signed certificate should be generated first.

A new self-signed certificate can be generated by using keytool (from the adapter's work directory) with the `–selfcert` option, as follows:

```
keytool –selfcert –alias v4v-adapter –dname “<DN of Organization>” –keystore
v4v-adapter.jks
```

<DN of Organization> is the distinguished name of the organization that the certificate will be issued to. For example, “OU=Management Platform, O=”VMware, Inc.”, C=US”.

This command will prompt for the password to the certificate store, which can be found in the *msgserver.properties* file as described above. Once complete, a new certificate issued to the given organization will be generated for the adapter.

By default, the certificate's signature will use the SHA1withRSA algorithm. This can be overridden by also specifying the name of the algorithm in the keytool command, as follows:

```
keytool –selfcert –alias v4v-adapter –dname “<DN of Organization>” –sigalg
SHA256withRSA –keystore v4v-adapter.jks
```

Generating a Certificate Signing Request

A certificate signing request is required in order to request a certificate from a certificate signing authority. This request can be generated by using keytool (from the adapter's work directory) with the `–certreq` option, as follows:

```
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.

This command will prompt for the password to the certificate store, which can be found in the *msgserver.properties* file as described above. Once complete, a certificate signing request will be generated for the adapter's certificate. This request can then be uploaded to a certificate authority in order to request a signed certificate.

Importing a Certificate

Once the adapter's certificate is signed by a certificate authority, it needs to be imported into the certificate store in order for the adapter to start using it. First, the certificate file needs to be copied to the adapter's work directory. Then the certificate can be imported by using keytool (from the adapter's work directory) with the `–import` option, as follows:

```
keytool –import –alias v4v-adapter –file <Certificate File> -keystore v4v-adapter.jks
```

`<Certificate File>` is the name of the certificate file from the certificate authority.

This command will prompt for the password to the certificate store, which can be found in the *msgserver.properties* file as described above. Once complete, the signed certificate will be imported into the adapter's certificate store.

After importing a new certificate, you must restart the adapter to start using the new certificate. To restart the adapter:

- On the Analytics VM of the vCenter Operations Manager vApp, run the following command:

  ```
  service vcops restart collector
  ```

- On Windows Remote Collectors, use the Stop and Start shortcuts on the Start Menu to restart the collector.
- On Linux Remote Collectors, run the following command:

  ```
  service vcops restart collector
  ```

Once the adapter has been restarted, any broker agents that are attached to the adapter will need to be paired again.

Broker Agent

The broker agent's certificate and trust store are located in the configuration directory on the Horizon View server:

```
C:\ProgramData\VMware\vCenter Operations for View\conf
```

This directory contains two Java key stores:

- *v4v-brokeragent.jks*, which contains the certificate used by the broker agent to authenticate itself to the adapter.
- *v4v-truststore.jks*, which contains the trust store used by the broker agent to authenticate the adapter's certificate.

The credentials for these key store files are stored in the *msgclient.properties* file, also located in the configuration directory. Table 6 shows a list of the key store properties.

Table 6: Broker Agent key store configuration properties

Property	Description	Default Value
keyfile	The name of the key store file that contains the broker agent's certificate.	v4v-brokeragent.jks
keypass	The password to the key store file that contains the broker agent's certificate.	Dynamically generated

Property	Description	Default Value
trustfile	The name of the key store file that contains the broker agent's trust store.	v4v-truststore.jks
trustpass	The password to the key store file that contains the broker agent's trust store.	Dynamically generated

Both the certificate store and trust store can be viewed and controlled using the Java `keytool` application. For information regarding using this tool, refer to http://docs.oracle.com/javase/1.4.2/docs/tooldocs/windows/keytool.html.

When the broker agent is first installed, a self-signed certificate is generated that the broker agent uses by default to authenticate to the adapter. For increased security, a certificate signed by a valid certificate authority can be used instead. The process for generating and importing a signed certificate is as follows:

1. Create a new self-signed certificate for your organization.
2. Generate a certificate signing request.
3. Send the request to a certificate signing authority.
4. Import the certificate from the certificate signing authority into the certificate store.

These steps should be performed on the Horizon View Connection server where the broker agent is installed.

Important: If the certificate authority requests a password for the certificate's private key, the password configured for the certificate store must be used.

Creating a New Self-Signed Certificate

The default self-signed certificate is issued to VMware. If a new signed certificate is being requested, it is recommended that the new certificate be issued to the individual organization. As a result, a new self-signed certificate should be generated first.

A new self-signed certificate can be generated by using keytool (from the configuration directory) with the `–selfcert` option, as follows:

```
keytool –selfcert –alias v4v-brokeragent –dname “<DN of Organization>” –
keystore v4v-brokeragent.jks
```

`<DN of Organization>` is the distinguished name of the organization that the certificate will be issued to. For example, “OU=Management Platform, O=”VMware, Inc.”, C=US”.

This command will prompt for the password to the certificate store, which can be found in the *msgclient.properties* file as described above. Once complete, a new certificate issued to the given organization will be generated for the broker agent.

By default, the certificate's signature will use the SHA1withRSA algorithm. This can be overridden by also specifying the name of the algorithm in the keytool command, as follows:

```
keytool –selfcert –alias v4v-brokeragent –dname “<DN of Organization>” –sigalg
SHA256withRSA –keystore v4v-brokeragent.jks
```

Generating a Certificate Signing Request

A certificate signing request is required in order to request a certificate from a certificate signing authority. This request can be generated by using keytool (from the configuration directory) with the `–certreq` option, as follows:

```
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.

This command will prompt for the password to the certificate store, which can be found in the *msgclient.properties* file as described above. Once complete, a certificate signing request will be generated for the broker agent's certificate. This request can then be uploaded to a certificate authority in order to request a signed certificate.

Importing a Certificate

Once the broker agent's certificate is signed by a certificate authority, it needs to be imported into the certificate store in order for the broker agent to start using it. First, the certificate file needs to be copied to the configuration directory. Then the certificate can be imported by using keytool (from the configuration directory) with the `–import` option, as follows:

```
keytool –import –alias v4v-brokeragent –file <Certificate File> -keystore v4v-
brokeragent.jks
```

`<Certificate File>` is the name of the certificate file from the certificate authority.

This command will prompt for the password to the certificate store, which can be found in the *msgclient.properties* file as described above. Once complete, the signed certificate will be imported into the broker agent's certificate store.

After importing a new certificate, the broker agent must be restarted before it will start using the new certificate. The broker agent service can be restarted either by using the "vCenter Operations for View Broker Agent Settings" tool, or by restarting the *vCenter Operations for Horizon View Broker Agent* service.

Once the broker agent has been restarted, you must pair the broker agent to the adapter again.

Security in VMware View 5.0 and 5.1

Horizon View 5.2 contains tighter integration with vCenter Operations Manager for Horizon View, including features that enable the broker agent to send configuration data to the Horizon View desktops. This allows the broker agent to send information needed by the desktop agent for performing authentication.

View 5.0 and 5.1 do not include these features. In order to use vCenter Operations Manager for Horizon View to monitor either a View 5.0 or View 5.1 environment, it is necessary to disable authentication in the adapter. To disable authentication, add the following line to *msgserver.properties* on the server where the adapter is running:

```
disable-authentication = true
```

The collector needs to be restarted before changes to this setting will take effect.

- On the Analytics VM of the vCenter Operations Manager vApp, run the following command:

  ```
  service vcops restart collector
  ```

- On Windows Remote Collectors, use the Stop and Start shortcuts on the Start Menu to restart the collector.
- On Linux Remote Collectors, run the following command:

  ```
  service vcops restart collector
  ```

Disabling authentication has the following security implications:

- The adapter will not authenticate desktops, so an attacker could potentially send rogue data for a desktop to vCenter Operations Manager.
- All data that is transmitted will still be encrypted. However, a default self-signed certificate is used. If an attacker gains access to this certificate, it would be possible to decrypt the data sent from the agents to the adapter. This includes the Horizon View inventory, Horizon View events, machine names, IP addresses, user names, and general desktop performance data.

Remote Collector Security

In order to improve performance and scalability in environments that have multiple data centers, vCenter Operations Manager can use *remote collectors*. A remote collector is installed on either a Windows or Linux server, and can host one or more adapter instances. This allows data collection to be distributed across multiple data centers.

Use of remote collectors has several serious security implications:

- In order to connect the remote collector to the vCenter Operations Manager vApp, it is necessary to expose the RMI interface of the vApp publically. However, there is no authentication performed on connections to this interface. An attacker could use this interface to retrieve arbitrary data, send rogue data, and potentially take control of vCenter Operations Manager.
- The connection between the remote collector and the vApp is not encrypted. An attacker could gain access to any data sent from an adapter instance to the vApp by sniffing the network.
- Configuration data that is sent from the vApp to the adapter instances on the remote collector is not encrypted. An attacker could gain access to the configuration information for any adapter instance on the remote collector by sniffing the network. This includes, but is not limited to, the vCenter Operations Manager for Horizon View server key as well as vCenter credentials used by the VMware adapter.

To configure a remote collector, contact VMware Global Support Services for assistance.

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